Alessia Bartoli è nata a Roma il 5 Giugno 1974.
Ha conseguito la maturità scientifica presso il Liceo scientifico statale "G. Peano" di Roma nel luglio 1993.
Si è immatricolata al Corso di Laurea in Matematica presso l'Università degli Studi "Roma Tre" nell'anno accademico 1993-1994.
Ha presentato per la prova di qualificazione all'esame di laurea le seguenti tesine orali :
"Il Teorema di Lamé" e "Punti razionali su curve ellittiche piane".
Ha vinto negli anni accademici 1995-1996, 1996-1997 la borsa di collaborazione studenti per il laboratorio di calcolo del Dipartimento di Matematica.

Indice

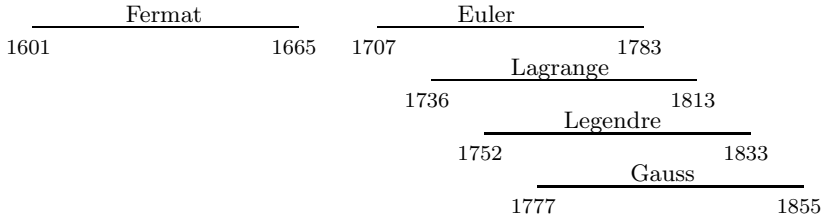
Mathematics il the queen of the sciences,
and Number Theory the queen of mathematics.

La matematica è la regina delle scienze,
e la Teoria dei Numeri è la regina della matematica.

Karl Friedrich Gauss (1777-1855)

Introduzione

Argomento del nostro lavoro è quella parte della Teoria dei Numeri che tratta le proprietà di divisibilità dei numeri interi.
I principali fondatori della Teoria moderna dei Numeri sono stati Fermat, Euler, Lagrange, Legendre e Gauss. Dal 1630, iniziando con i lavori di Fermat, fino alla pubblicazione del volume di Gauss *Disquisitiones Arithmeticae* nel 1801, questi matematici hanno dato contributi fondamentali allo sviluppo successivo della teoria.
Per avere un'idea cronologica di tale periodo diamo il seguente schema:



È opinione condivisa che Gauss sia uno dei massimi matematici dell'era moderna.
La Teoria dei Numeri era la sua grande passione e il suo lavoro: *Disquisitiones Arithmeticae* [G], ne è considerato la base.
Leopold Kronecker, commentando il lavoro di Gauss, disse:
"È veramente incredibile pensare come un singolo uomo, così giovane, sia stato capace di pensare a tali risultati ed, in più, li abbia presentati in maniera precisa e ben organizzata."

Molti dei risultati che verranno presentati nel nostro lavoro, sono frutto dello studio di Gauss, soprattutto quelli riguardanti la Legge di Reciprocità Quadratica e le radici primitive.
Dopo Gauss, molti matematici hanno cercato di estendere la Legge di Reciprocità a congruenze di grado superiore a 2, riassunte tutte nella Legge di Reciprocità di Artin.
Il lavoro di Gauss inizia con la definizione di congruenza:

se m divide $a - b$, allora a è congruo a b modulo m.

Tra l'altro egli ideò l'attuale notazione di congruenza ($\equiv$) che permise un più facile sviluppo di questa teoria, ma anche di molte altre (come ad esempio la Teoria dei Gruppi).
Da Gauss in poi, lo studio della Teoria dei Numeri si è concentrato sulla risolubilità di congruenze polinomiali per poi "arrivare" al concetto di reciprocità già introdotto da Gauss.

Abbiamo suddiviso il nostro lavoro in due parti; nella prima si è presentata la Teoria delle Congruenze dando le definizioni base, studiando in modo approfondito le congruenze lineari, descrivendo metodi applicativi per la soluzione dei vari problemi e, per concludere, studiando il caso delle congruenze quadratiche, approfondendo la Legge di Reciprocità Quadratica dimostrata già da Gauss nel suo lavoro [G]. Facciamo presente che per quanto riguarda questa parte sono stati rielaborati gli appunti distribuiti a lezione dal Prof. Fontana.

Il nostro lavoro si è concentrato nella seconda parte dove sono stati riportati approfondimenti alla teoria descritta nella prima parte, e applicazioni pratiche con il software *Mathematica* .

Più precisamente, abbiamo abbiamo raccolto ed esaminato le funzioni built-in di *Mathematica* che hanno attinenza con la parte della Teoria delle Congruenze sviluppata nella prima parte della tesi. A partire da queste funzioni, abbiamo studiato nuovi algoritmi e sviluppato nuove funzioni (implementate con *Mathematica*) che permettono di risolvere molti dei problemi presi in esame. Questo studio mostra l'efficacia e la duttilità di *Mathematica* , come strumento di ausilio computazionale, nell'ambito della Teoria dei Numeri.

0. Il software *Mathematica*

Mathematica è un *Computer Algebra System* ovvero un sistema di "manipolazione simbolica", cioè un sistema in grado di manipolare espressioni algebriche in quanto tali.

Il nucleo di *Mathematica* (*kernel*) è realizzato in Linguaggio C. Gli utenti dialogano con esso tramite un'interfaccia.
Gli interfaccia più semplici (ad esempio quello per i sistemi UNIX e Linux) si limitano a gestire linee di comando, mentre le immagini vengono prodotte in apposite finestre che si aprono sullo schermo.
Altri interfacce (ad esempio quello per il sistema MS-Windows) consentono l'utilizzo di *notebooks*, cioè files integrati contenenti linee di comando, immagini, suoni e testi di commento.
Al testo viene allegato un dischetto riportante gli approfondimenti svolti con *Mathematica* che utilizza questo ultimo tipo di interfaccia.

Principali convenzioni utilizzate.

Mathematica è un software *case sensitive*, cioè distingue tra maiuscole e minuscole. Tutte le funzioni e le costanti contenute nel sistema (funzioni *built-in*) sono indicate con nomi che iniziano per maiuscola e quindi, nelle definizioni delle funzioni da noi create, abbiamo scelto di utilizzare tutti nomi con la minuscola.
Nella definizione delle funzioni e dei comandi, abbiamo fatto uso delle parentesi secondo i criteri propri del software, che andiamo qui di seguito a descrivere:

- Le parentesi tonde **( )** vengono utilizzate per determinare la priorità del calcolo.
- Le parentesi quadre [ ] vengono utilizzate per indicare gli argomenti delle varie funzioni.
- Le parentesi graffe **{ }** vengono utilizzate per indicare liste e matrici.
- Le doppie parentesi quadre [[ ]] vengono utilizzate per indicare un determinato elemento di una lista o di una matrice.

Analizziamo ora con qualche dettaglio i singoli paragrafi della seconda parte della Tesi.

1. Proprietà elementari delle congruenze

Per quanto riguarda gli approfondimenti teorici viene presentato tra l'altro un algoritmo tramite il quale è possibile determinare a che giorno della settimana corrisponde una determinata data (calendario universale).
Si è fatta questa scelta per dare un'idea di come una teoria, a prima vista tanto astratta, possa in realtà avere applicazioni concrete.

In più si sono aggiunte caratterizzazioni delle congruenze analizzando ulteriori criteri di divisibilità ed esercizi con soluzioni.

Nella parte dedicata al software si è studiato l'Algoritmo Euclideo osservando anche graficamente l'andamento dei resti.
Si è passato quindi ad uno studio dettagliato del software applicandolo alla teoria sviluppata nel paragrafo della prima parte a cui si fa riferimento, sviluppando anche una funzione per una visualizzazione immediata delle classi di congruenza ed utilizzandola successivamente per verificare alcune proprietà delle congruenze.

mostracongruenza[14]

2. Congruenze lineari ed equazioni diofantee lineari

Nella prima parte si sono trattate le equazioni diofantee; qui abbiamo descritto un altro metodo per la risoluzione di tali equazioni utilizzando le **frazioni continue**, dando quindi definizioni e caratterizzazioni necessarie successivamente nella descrizione del metodo pratico per la soluzione di equazioni diofantee.

Avendo definito nella prima parte la funzione di Euler, abbiamo ritenuto opportuno darne alcune proprietà significative, come ad esempio, dimostrare che si tratta di una funzione moltiplicativa e varie formule per calcolarla esplicitamente:
preso comunque $n > 0$ con $n = p_1^{e_1} \cdots p_r^{e_r}$ (come nella Proposizione 13), allora

$$\varphi(n) = p_1^{e_1-1}(p_1 - 1) \cdots p_r^{e_r-1}(p_r - 1).$$

Nella parte dedicata a *Mathematica* si sono studiate graficamente le soluzioni delle equazioni diofantee lineari, dandone vari esempi significativi. Riportiamo qui di seguito la funzione che grafica $3X - 4Y = 2$ con x che varia tra -6 e 6 segnando le sue soluzioni (intere).

linearPlot[3, -4, 2, -6, 6]

Per le equazioni diofantee lineari in tre indeterminate, si è creata una funzione che elenca le soluzioni per una determinata regione di visibilità.

Abbiamo quindi definito due funzioni per determinare le soluzioni delle congruenze lineari in una indeterminata: una funzione grafica che visualizza le soluzioni per i primi 100 interi:

visualizzaSol[3, 6, 7]

ed una funzione che determina le soluzioni per un determinato intervallo. Per quanto riguarda la funzione grafica, nel dischetto allegato al nostro lavoro, si è inserito un comando che permette, facendo variare un dato, di visualizzare un filmato che descriva i vari comportamenti delle soluzioni.

3. Il "piccolo" Teorema di Fermat

Alla Definizione 3.6 della prima parte, si sono definiti i Numeri di Carmichael. Dopo un primo tentativo con *Mathematica* per calcolarne alcuni, si

sono trovati dei risultati (cfr. [LN]) con stime sul tempo necessario per il calcolo di tali valori.
Si è quindi riportata la descrizione dell'algoritmo utilizzato dagli autori del lavoro, con accenni alla teoria che permettessero la completa comprensione dei passaggi, ed in più, si sono riportati alcuni risultati rilevanti descritti in tale nell'articolo.

Nella parte dedicata al software si è definita un'altra funzione per la soluzione delle congruenze lineari, diversa dalla funzione definita nel paragrafo precedente, che permettesse la definizione di una funzione per la soluzione di un generico sistema di congruenze lineari in una indeterminata.

m={{3, 5, 5, 7}, {3, 7, 21, 5}, {3, 7, 8, 13}}

{{3, 5, 5, 7}, {3, 7, 21, 5}, {3, 7, 8, 13}}

sistemaCong[m];

Le soluzioni del sistema dato in input $m = \begin{pmatrix} 3 & 3 & 3 \\ 5 & 7 & 7 \\ 5 & 21 & 8 \\ 7 & 5 & 13 \end{pmatrix}$

e cioè $\begin{cases} 3X \equiv 3 \pmod 3 \\ 5X \equiv 7 \pmod 7 \\ 5X \equiv 21 \pmod 8 \\ 7X \equiv 5 \pmod{13} \end{cases}$

sono: {49, 777, 1505}
Modulo 2184

4. Generalità sulle congruenze polinomiali, Teorema di Lagrange e Teorema di Chevalley

Nella prima parte è stato enunciato il Teorema di Wilson; nella seconda parte ne abbiamo dato una dimostrazione alternativa partendo dalle proprietà del polinomio $X^p - X$ e di conseguenza abbiamo enunciato e dimostrato il

Teorema di Wolstenholme. Sia p un primo maggiore di 3. Allora

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2}$$

dove con $\frac{1}{i}$ si intende l'inverso aritmetico di $i \pmod{p^2}$.

Per la soluzione delle congruenze polinomiali *Mathematica* ha una funzione built-in che, però, non è basata sull'algoritmo descritto nella parte teorica. Abbiamo quindi definito noi una funzione basata su tale algoritmo confrontandola con quella propria del software verificando così che la "nostra" funzione è più lenta nel calcolare le soluzioni base da cui partire.

Una soluzione migliore è stata successivamente presentata nell'ultimo paragrafo.

Solve[xˆ2 + x + 7 == 0 && Modulus == 9]//Timing

{0. Second, {{Modulus → 9, x→ 1}, {Modulus → 9, x→ 4}, {Modulus → 9, x→ 7}}}

congruenzaPolinomiale[xˆ2 + x + 7, 3, 2]//Timing

{0.02 Second, {1, 4, 7}}

Per concludere si è verificato graficamente il Teorema di Lagrange 4.18 su polinomi generati in modo casuale.

5. Radici primitive dell'unità e congruenze del tipo $\mathbf{X^m \equiv a}$ (mod **n**)

Nella parte teorica si è enunciato il Teorema di Gauss sull'esistenza delle radici primitive senza darne dimostrazione.

Teorema Gauss (1801). Sia n un intero positivo. Esiste una radice primitiva (mod n) se, e soltanto se, n è uno dei seguenti interi:

$$2, 4, p^k, 2p^k$$

con $k \geqslant 1$ e p primo dispari.

Nella parte seconda abbiamo, quindi, dimostrato il teorema.

Nella sezione dedicata al software abbiamo definito delle funzioni per il calcolo dell'ordine di un elemento:

ordine[2, 7]

3

una per il calcolo della radice primitiva con due metodi diversi (uno a test, l'altro secondo l'algoritmo di Gauss):

radicePrimitiva[61]

{2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59}

primitivaGauss[61]

2

ed una per il calcolo dell'indice di un elemento:

indice[6, 18, 61]

19

Infine è stata definita una funzione che ci permetta di determinare i valori di a per cui la congruenza

$$\text{coefficiente} \cdot X^{\text{esponente}} \equiv \text{a} \pmod{\text{modulo}}.$$

ammetta soluzione.

soluzioni[2, 4, 14]

La congruenza ha soluzione per i seguenti valori di a:
{1, 2, 4, 7, 8, 9, 11}

6. Congruenze quadratiche e legge di reciprocità

Applicando i Simboli di Legendre e Jacobi, abbiamo descritto un algoritmo teorico per il calcolo della radice modulo un primo.
L'algoritmo è stato utilizzato per definire una funzione per il calcolo della radice (se esiste) modulo un intero n qualsiasi

radiceN[9, 12]

{3, 9}

A questo punto si è migliorata la funzione descritta nel paragrafo quattro per il calcolo della congruenza polinomiale modulo un primo utilizzando un algoritmo, descritto in dettaglio, basato sul calcolo della radice quadrata. Confrontando questo algoritmo con quello precedentemente descritto abbiamo verificato che, effettivamente, il secondo risulta più veloce.

congruPoli[x^4 - 3, 73]//Timing

{0.05 Second, La congruenza non ha soluzione}

congPolinomiale[x^4 - 3, 73]//Timing

{0.01 Second, { }}

Parte I

La teoria delle congruenze

1 Proprietà elementari delle congruenze

Un altro metodo di approccio alla teoria della divisibilità in $\mathbb{Z}$ consiste nello studiare le proprietà aritmetiche del resto della divisione euclidea, o, come si dice abitualmente, la teoria delle congruenze. Tale teoria è stata iniziata da Gauss nel suo celebre *Disquisitiones Arithmeticae* [G], apparso nel 1801 (quando Gauss aveva soltanto ventiquattro anni).

Definizione 1.1. Sia n un intero fissato. Si dice che $a, b \in \mathbb{Z}$ sono *congruenti* $\pmod n$ e si scrive:

$$a \equiv b \pmod n$$

se risulta che $a - b \in n\mathbb{Z}$ (cioè, se n *divide* $a - b$, in altri termini, se esiste un intero $k \in \mathbb{Z}$ tale che $kn = a - b$; in simboli, scriveremo $n|(a - b)$).

Osservazione 1.2. Siano $a, b, n \in \mathbb{Z}$. Dalla definizione precedente segue subito che:
(a) se $n = 1$, allora $a \equiv b \pmod 1$, presi comunque $a, b \in \mathbb{Z}$;
(b) se $n = 0$, allora $a \equiv b \pmod 0 \iff a = b$;
(c) $a \equiv b \pmod n \iff a \equiv b \pmod{-n} \iff a \equiv b \pmod{|n|}$.

Per evitare casi banali, è quindi evidente che ci si può limitare a considerare congruenze modulo $n \geq 2$. In particolare, due interi sono congruenti (modulo 2) se, e soltanto se, hanno la stessa parità.
È evidente che "la congruenza $\pmod n$" stabilisce una relazione (binaria) tra gli elementi di $\mathbb{Z}$. Le prime proprietà di tale relazione sono raccolte nella seguente:

Proposizione 1.3. *Siano n, m due interi positivi fissati e siano a, b, c, $d \in \mathbb{Z}$. Allora:*
(1) *Proprietà riflessiva della "congruenza $\pmod n$":*
$a \equiv a \pmod n$, per ogni $a \in \mathbb{Z}$;
(2) *Proprietà simmetrica della "congruenza $\pmod n$":*
$a \equiv b \pmod n \iff b \equiv a \pmod n$;
(3) *Proprietà transitiva della "congruenza $\pmod n$":*
$a \equiv b \pmod n, b \equiv c \pmod n \Rightarrow a \equiv c \pmod n$;
(4) *Proprietà di compatibilità con la somma della "congruenza $\pmod n$":*
$a \equiv b \pmod n, c \equiv d \pmod n \Rightarrow a + c \equiv b + d \pmod n$;
(5) *Proprietà di compatibilità con il prodotto della "congruenza $\pmod n$":*
$a \equiv b \pmod n$, $c \equiv d \pmod n$, $\Rightarrow ac \equiv bd \pmod n$;
(6) $a \equiv b \pmod n \iff a + c \equiv b + c \pmod n$ *per ogni* $c \in \mathbb{Z}$;
(7) $a \equiv b \pmod n \iff ac \equiv bc \pmod n$ *per ogni* $c \in \mathbb{Z}$;
(8) $a \equiv b \pmod n \iff a^k \equiv b^k \pmod n$ *per ogni intero* $k \geq 0$;
(9) $a \equiv b \pmod n$, $m \mid n \Rightarrow a \equiv b \pmod m$;
(10) $a \equiv b \pmod n$, $m \neq 0 \Rightarrow am \equiv bm \pmod{nm}$;

(11) *Se* $a \equiv b \pmod{n}$, $d \neq 0$, $d \mid a$, $d \mid b$, $d \mid n$ *allora*

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

Dimostrazione. Le semplici verifiche sono lasciate come esercizio. □

Corollario 1.4. *Siano* n *ed* m *due interi positivi fissati.*

(1) *Siano* $a_1, ..., a_m, b_1, ..., b_m, c_1, ..., c_m \in \mathbb{Z}$ *tali che* $a_i \equiv b_i \pmod{n}$ $(1 \leqslant i \leqslant m)$. *Allora:*

$$\sum_{i=1}^{m} a_i c_i \equiv \sum_{i=1}^{m} b_i c_i \pmod{n}$$

(2) *Siano* $a, b \in \mathbb{Z}$ *ed* $f(X) \in \mathbb{Z}[X]$. *Se* $a \equiv b \pmod{n}$, *allora:*

$$f(a) \equiv f(b) \pmod{n}$$

Dimostrazione. Basta utilizzare alcune proprietà della proposizione precedente. □

Osservazione 1.5. Le proprietà (4) e (5) della Proposizione 1.3 permettono di definire sull'insieme quoziente $\mathbb{Z}/n\mathbb{Z}$ delle operazioni di somma e prodotto che determinano su $\mathbb{Z}/n\mathbb{Z}$ una struttura canonica di anello.
La relazione di congruenza (modulo n) corrisponde alla relazione di uguaglianza nell'anello quoziente $\mathbb{Z}/n\mathbb{Z}$. Se infatti, $a, b \in \mathbb{Z}$ e se

$$\bar{a} := a + n\mathbb{Z},\ \bar{b} := b + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z},$$

allora:

$$a \equiv b \pmod{n} \quad \Longleftrightarrow \quad \bar{a} = \bar{b}.$$

Proposizione 1.6. *Siano* $a, b \in \mathbb{Z}, n > 0$. *Allora,* $a \equiv b \pmod{n}$ *se, e soltanto se,* a, b *hanno lo stesso resto nella divisione per* n.

Dimostrazione. Se $a \equiv b \pmod{n}$, allora esiste $k \in \mathbb{Z}$ in modo tale che $a = kn + b$. Dividendo b per n, si ottiene $b = qn + r$, con $0 \leqslant r < n$ e, sostituendo, $a = (k + q)n + r$. Viceversa, se $a = qn + r, b = q'n + r$ con $0 \leqslant r < n$, allora $a - b = (q - q')n$ e dunque $a \equiv b \pmod{n}$. □

Corollario 1.7. *Ogni intero è congruente (modulo* n*) ad uno ed uno soltanto tra gli interi* $0, 1, ..., n - 1$. □

Tale fatto giustifica la seguente definizione:

Definizione 1.8. Si chiama *sistema completo di residui (modulo* n*)* ogni insieme $S \subset \mathbb{Z}$ (formato da n interi) tale che ogni $a \in \mathbb{Z}$ è congruente (modulo n) ad uno ed un solo elemento di S.

Ad esempio $S := \{0, 1, ..., n-1\}$ è un sistema completo di residui (modulo n), detto *sistema completo minimo* $(\text{mod } n)$.
Se n è dispari, allora $S := \{-\frac{n-1}{2}, -\frac{n-3}{2}, ..., -1, 0, 1, ..., \frac{n-3}{2}, \frac{n-1}{2}\}$ è anch'esso un *sistema completo di residui*, detto *minimo in valore assoluto*, $(\text{mod } n)$.
Se n è pari, ci sono due sistemi completi di residui che hanno una proprietà di minimalità rispetto al valore assoluto e sono:
$S_1 := \{-\frac{n-2}{2}, ..., -1, 0, 1, ..., \frac{n-2}{2}, \frac{n}{2}\}$ e $S_2 := \{-\frac{n}{2}, -\frac{n-2}{2}, ..., -1, 0, 1, ..., \frac{n-2}{2}\}$

È subito visto che n interi formano un sistema completo di residui (modulo n), se, e soltanto se, sono a due a due incongruenti modulo n. Torneremo in seguito sui sistemi completi di residui (cfr. Esercizi 1.4 e 1.5); vogliamo tuttavia dimostrare subito alcune regole di cancellazione.

Proposizione 1.9. *Siano $a, b, c, n \in \mathbb{Z}, n > 0$. Se $d := \text{MCD}(c, n)$, allora:*

$$ac \equiv bc \pmod{n} \Rightarrow a \equiv b \pmod{\frac{n}{d}}.$$

Dimostrazione. Per ipotesi, esiste $k \in \mathbb{Z}$ tale che $c(a-b) = kn$. Inoltre, esistono $x, y \in \mathbb{Z}$ tali che $c = dx$, $n = dy$ e $\text{MCD}(x, y) = 1$. Da ciò segue che $x(a-b) = ky$ e dunque $y \mid x\,(a-b)$. In base al Lemma di Euclide, $y \mid (a-b)$ e cioè $a \equiv b \pmod{y}$. $\square$

Osservazione 1.10. Si noti che vale anche il viceversa nella precedente Proposizione. Precisamente, se $a - b = h(\frac{n}{d})$ per qualche $h \in \mathbb{Z}$ allora $ac \equiv bc \pmod{n}$. Infatti, se come sopra $c = dx, n = dy$, allora $(a-b)d = hn$, quindi $(a-b)dx = hnx$ cioè $(a-b)c = hnx$. Pertanto, $ac - bc \equiv 0 \pmod{n}$.

Corollario 1.11. *Siano $a, b, c, n, p \in \mathbb{Z}$, con $n > 0$ e p numero primo. Si ha:*

(a) *se $ac \equiv bc \pmod{n}$ e $\text{MCD}(n, c) = 1 \Rightarrow a \equiv b \pmod{n}$;*

(b) *se $ac \equiv bc \pmod{p}$ e $p \nmid c \Rightarrow a \equiv b \pmod{p}$.* $\square$

Osservazione 1.12. **(a)** Per la validità delle proprietà di cancellazione, le ipotesi nel corollario relative al massimo comun divisore sono essenziali. Ad esempio:
$2 * 4 \equiv 2 * 1 \pmod{6}$ mentre $4 \not\equiv 1 \pmod{6}$ (in tal caso $\text{MCD}(2, 6) = 2$).
(b) L'impossibilità di cancellare (in generale) un fattore di una congruenza è strettamente connessa col fatto che (in generale) $\mathbb{Z}/n\mathbb{Z}$ non è un anello integro. A questo proposito, è opportuno ricordare il seguente fatto ben noto:
Sia $n \in \mathbb{Z}$, $n > 0$. Le seguenti condizioni sono equivalenti:

(i) *$\mathbb{Z}/n\mathbb{Z}$ è un anello integro;*

(ii) *$\mathbb{Z}/n\mathbb{Z}$ è un campo;*

(iii) *n è un numero primo.*

Definizione 1.13. Siano $a, n \in \mathbb{Z}, n > 0$. Si chiama *inverso aritmetico di a (modulo n)* un elemento $a^* \in \mathbb{Z}$ tale che:

$$aa^* \equiv 1 \pmod{n}.$$

Si noti che un siffatto elemento non sempre esiste (ad esempio, 2 non ammette inverso aritmetico (modulo 4)), e, se esiste, non è necessariamente unico (ad esempio, 3, 7, 11, ... sono inversi aritmetici di 3 (modulo 4)). Il seguente risultato precisa tali questioni:

Proposizione 1.14. *Siano $a, n \in \mathbb{Z}, n > 0$. Risulta:*

(a) *a ammette inverso aritmetico (modulo n) se e soltanto se $MCD(a, n) = 1$;*

(b) *se a_1^*, a_2^* sono due inversi aritmetici di a (modulo n), allora $a_1^* \equiv a_2^* \pmod{n}$.*

Dimostrazione. (a) ($\Leftarrow$) L'identità di Bézout ci assicura che esistono $x, y \in \mathbb{Z}$ tali che $ax + ny = 1$. Dunque $ax \equiv 1 \pmod{n}$ e pertanto $x = a^*$. ($\Rightarrow$) Esiste $k \in \mathbb{Z}$ tale che $aa^* - 1 = kn$. Se quindi $d := \mathrm{MCD}(a, n)$, allora $d \mid (aa^* - kn)$ e dunque $d = 1$.
(b) Si ha: $a_1^* \equiv a_1^*(aa_2^*) = (a_1^*a)a_2^* \equiv a_2^* \pmod{n}$. $\square$

Osservazione 1.15. La dimostrazione della Proposizione 1.14 (a) suggerisce un metodo pratico per il calcolo di un inverso aritmetico (modulo n) di un elemento assegnato $a \in \mathbb{Z}$ con $\mathrm{MCD}(a, n) = 1$: l'algoritmo euclideo delle divisioni successive. Questo algoritmo, infatti, come è ben noto, permette di calcolare esplicitamente "i coefficienti" nell'identità di Bézout relativa ad $1 = \mathrm{MCD}(a, n)$.
Un metodo, a volte, di più facile applicazione, usando l'esponenziazione modulare, si ricaverà nel seguito, come conseguenza del "Piccolo Teorema di Fermat" (cfr. Paragrafo 3).

Osservazione 1.16. Esprimendo le congruenze modulo n tramite uguaglianze in $\mathbb{Z}/n\mathbb{Z}$ (cfr. Osservazione 1.5), è chiaro che la ricerca di un inverso aritmetico di $a \in \mathbb{Z}$ (modulo n) equivale alla ricerca dell'inverso moltiplicativo di $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$.

Nel paragrafo successivo torneremo sul problema della ricerca degli inversi aritmetici allo scopo di risolvere le congruenze lineari in una indeterminata; per il momento vogliamo applicare i risultati precedenti per "ritrovare" alcuni criteri di divisibilità elementarmente noti.

Teorema 1.17. *Sia N un intero tale che $|N|$ ammette la seguente espressione in base 10, ovvero decimale:*

$$|N| = a_m 10^m + a_{m-1}10^{m-1} + ... + a_2 10^2 + a_1 10 + a_0,$$

con $0 \leqslant a_i \leqslant 9, 0 \leqslant i \leqslant m$ e $a_m \neq 0$. Posto

$$S(N) := \sum_{i=0}^{m} a_i \quad e \quad A(N) := \sum_{i=0}^{m} (-1)^i a_i,$$

si ha:

(a) $2 \mid N \iff 2 \mid a_0$;

(b) $3 \mid N \iff 3 \mid S(N)$;

(c) $4 \mid N \iff 4 \mid a_1 10 + a_0$;

(d) $5 \mid N \iff 5 \mid a_0$;

(e) $9 \mid N \iff 9 \mid S(N)$;

(f) $11 \mid N \iff 11 \mid A(N)$;

(g) *Sia i tale che $1 \leqslant i \leqslant m$. Allora:*

$$2^i \mid N \iff 2^i \mid (a_{i-1}10^{i-1} + ... + a_1 10 + a_0)$$

Dimostrazione. (a; d) Sia $a = 2$ (oppure $a = 5$). Risulta:

$$a \mid N \iff N = \sum_{k=0}^{m} a_k 10^k \equiv 0 \pmod{a}.$$

Ma $10 \equiv 0 \pmod{a}$ e quindi:

$$a \mid N \iff a_0 \equiv 0 \pmod{a} \iff a \mid a_0.$$

(b; e) Sia $b = 3$ (oppure $b = 9$). Poichè $10 \equiv 1 \pmod{b}$, si ha:

$$b \mid N \iff \sum_{k=0}^{m} a_k \equiv 0 \pmod{b} \iff b \mid S(N).$$

(f) Poichè $10 \equiv -1 \pmod{11}$, $10^k \equiv (-1)^k \pmod{11}$ e dunque:

$$11 \mid N \iff 0 \equiv \sum_{k=0}^{m} a_k 10^k \equiv \sum_{k=0}^{m} (-1)^k a_k = A(N) \pmod{11}$$

$$\iff 11 \mid A(N).$$

(g; c) Poichè $10^j \equiv 0 \pmod{2^i}$ se $j \geqslant i$, si ha:

$$2 \mid N \quad \Longleftrightarrow \quad 0 \equiv \sum_{k=0}^{m} a_k 10^k \equiv \sum_{k=0}^{i-1} a_k 10^k \pmod{2^i}$$

$$\Longleftrightarrow \quad 2^i \mid (a_{i-1}10^{i-1} + \cdots + a_0). \qquad \square$$

I precedenti criteri di divisibilità in base 10 sono casi particolari di criteri di divisibilità che possono essere formulati in una base b qualunque.

Siano N, b due interi positivi e sia:

$$N = (a_m \dots a_1 a_0)_b := a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0$$

l'espressione esplicita di N in base b, con $0 \leqslant a_i \leqslant b-1,\ 0 \leqslant i \leqslant m$.

Proposizione 1.18. *Se d è un intero positivo tale che $d \mid b$ e se $k < m$ allora*

$$d^k \mid (a_m \dots a_1 a_0)_b \quad \Longleftrightarrow \quad d^k \mid (a_{k-1} \dots a_1 a_0)_b$$

In particolare, se $k = 1$, allora:

$$d \mid N \quad \Longleftrightarrow \quad d \mid a_0.$$

Dimostrazione. Basta osservare che:

$$d \mid b \Rightarrow d^k \mid b^k, \text{ per ogni } \quad k \geqslant 1,$$

e dunque:

$$N = a_m b^m + \cdots + a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \equiv$$

$$\equiv a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \pmod{d^k}. \qquad \square$$

Proposizione 1.19. *Se d è un intero positivo tale che $d \mid (b-1)$ allora:*

$$d \mid N \quad \Longleftrightarrow \quad d \mid \sum_{k=0}^{m} a_k.$$

Dimostrazione. Basta osservare che:

$$d \mid (b-1) \quad \Longleftrightarrow \quad b \equiv 1 \pmod{d},$$

e dunque:

$$N = a_m b^m + \cdots + a_1 b + a_0 \equiv a_m + \cdots + a_1 + a_0 \pmod{d}. \qquad \square$$

Proposizione 1.20. *Se d è un intero positivo tale che $d \mid (b+1)$ allora:*

$$d \mid N \quad \Longleftrightarrow \quad d \mid \sum_{k=0}^{m} (-1)^k a_k.$$

Dimostrazione. Basta osservare che

$$d \mid (b+1) \quad \Longleftrightarrow \quad b \equiv -1 \pmod{d},$$

e dunque:

$$N = a_m b^m + \cdots + a_1 b + a_0 \equiv (-1)^m a_m + \cdots + a_2 - a_1 + a_0 \pmod{d}. \qquad \square$$

Osservazione 1.21. Si noti che gli enunciati (a), (c), (d) e (g) del Teorema 1.17 sono casi particolari della Proposizione 1.18; gli enunciati (b) ed (e) del Teorema 1.17 sono casi particolari della Proposizione 1.19; l'enunciato (f) è un caso particolare della Proposizione 1.20

Osservazione 1.22. Particolarmente interessante è il seguente criterio di divisibilità dimostrato da B. Pascal attorno al 1654.
Conserviamo le notazioni del Teorema 1.17.
Sia a un intero non nullo e siano $r_1, r_2, \ldots$ i resti della divisione di $10, 10r_1, 10r_2, \ldots$ per a. Allora:

$$a \mid N \quad \Longleftrightarrow \quad a \mid (a_0 + a_1 r_1 + \cdots + a_m r_m).$$

Basta osservare che $10 \equiv r_1 \pmod{a}, 10^2 \equiv 10r_1 \equiv r_2 \pmod{a}$ ed, in generale, $10^k \equiv 10^{k-1} r_1 \equiv \cdots \equiv r_k \pmod{a}$ per ogni $1 \leqslant k \leqslant m$.
Ad esempio 1261 è divisibile per 13. Infatti, in questo caso $r_1 = 10$, $r_2 = 9, r_3 = 12$, dunque $1 + 6 \cdot 10 + 2 \cdot 9 + 1 \cdot 12 = 91$ e $13 \mid 91 = 13 \cdot 7$.

Vogliamo concludere il paragrafo con alcune osservazioni generali sulla teoria delle congruenze. L'importanza e l'interesse di tale teoria risiede essenzialmente nel fatto che essa gioca un ruolo fondamentale nella risoluzione delle cosidette "equazioni diofantee", cioè equazioni polinomiali a coefficienti interi di cui si ricercano le soluzioni intere.
Si consideri infatti la seguente equazione diofantea:

$$f(X_1, \ldots, X_r) = 0, \tag{1}$$

dove f è un polinomio a coefficienti interi in r indeterminate, cioè:
$f = f(X_1, \ldots, X_r) \in \mathbb{Z}[X_1, \ldots, X_r]$, con $r \geqslant 1$.
All'equazione diofantea (1) è associata una congruenza polinomiale $\pmod{n}$ per ogni n:

$$f(X_1, \ldots, X_r) \equiv 0 \pmod{n} \tag{2}$$

Definizione 1.23. Si chiama *soluzione della congruenza*:

$$f(X_1, \ldots, X_r) \equiv 0 \pmod{n}, \text{dove } f(X_1, \ldots, X_r) \in \mathbb{Z}[X_1, \ldots, X_r],$$

ogni r-upla $(a_1, \ldots, a_r)$ di interi tale che $f(a_1, \ldots, a_r) \equiv 0 \pmod{n}$.
Due soluzioni $(a_1, \ldots, a_r)$, $(b_1, \ldots, b_r)$ sono dette *distinte* o *incongruenti (modulo n)* se esiste un indice i $(1 \leqslant i \leqslant r)$ per cui risulti che $a_i \not\equiv b_i \pmod{n}$.

L'ultima parte della definizione è giustificata dal seguente risultato (semplice conseguenza delle proprietà elementari delle congruenze; cfr. Proposizione 1.3).

Proposizione 1.24. *Siano* $a_1, \ldots, a_r, b_1, \ldots, b_r$ *interi tali che si abbia:* $a_i \equiv b_i \pmod{n}$ *per ogni* i, $(1 \leqslant i \leqslant r)$. *Se* $(a_1, \ldots, a_r)$ *è soluzione della congruenza:*

$$f(X_1, \ldots, X_r) \equiv 0 \pmod{n},$$

anche $(b_1, \ldots, b_r)$ *è soluzione della stessa congruenza.* □

È ovvio che se $(b_1, \ldots, b_r) \in \mathbb{Z}^r$ è soluzione dell'equazione diofantea (1), allora $(b_1, \ldots, b_r)$ è anche soluzione della congruenza (2), per ogni $n > 0$. Pertanto, se per qualche $n > 0$, (2) non è risolubile, non sarà risolubile l'equazione diofantea (1).

Nel seguito considereremo principalmente congruenze in una sola indeterminata X.

Osservazione 1.25. (a) L'omomorfismo suriettivo canonico

$$\varphi_n : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

(con $n \geqslant 2$) di anelli si estende in modo ovvio ad un omomorfismo suriettivo tra anelli di polinomi:

$$\bar{\varphi}_n : \mathbb{Z}[X_1, \ldots, X_r] \longrightarrow (\mathbb{Z}/n\mathbb{Z})[X_1, \ldots, X_r].$$

All'equazione (1) resta quindi associata una famiglia di equazioni polinomiali:

$$\bar{f}_n(X_1, \ldots, X_r) = 0 \tag{3}$$

(con $\bar{f}_n = \bar{\varphi}_n(f) \in (\mathbb{Z}/n\mathbb{Z})[X_1, \ldots, X_r]$, $n \geqslant 2$).
È chiaro che un eventuale soluzione di (1) (cioè una r-upla di interi) determina una soluzione di ogni equazione (3) e quindi, dall'impossibilità di risolvere almeno una delle (3) segue l'irrisolubilità di (1). Più generalmente, qualunque condizione necessaria possa essere provata su almeno una delle (3) si riflette in una condizione necessaria per (1). Ad esempio il fatto che l'equazione diofantea $X^2+1-3Y^k = 0$ è irrisolubile, per ogni $k \geqslant 1$, discende dal fatto che la congruenza: $X^2 + 1 - 3Y^k \equiv 0 \pmod{3}$ non ha soluzioni.
D'altra parte, è subito visto che, se $a_1, \ldots, a_r \in \mathbb{Z}$, si ha:

$$\bar{f}_n(\bar{a}_1, \ldots, \bar{a}_r) = \bar{0} \quad \Longleftrightarrow \quad f(a_1, \ldots, a_r) \equiv 0 \pmod{n}.$$

(b) In generale, una congruenza $f(X) \equiv 0 \pmod{n}$ può ammettere soluzioni per alcuni valori di n, mentre può esserne priva per altri valori di n. Ad esempio $X^2 + 1 \equiv 0 \pmod{8}$ oppure $2X + 3 \equiv 0 \pmod{4}$, non ammettono

soluzioni, mentre $X^2 + 1 \equiv 0 \pmod 2$ e $2X + 3 \equiv 0 \pmod 5$ ammettono soluzioni (come si può verificare sperimentalmente).
(c) Semplici esempi mettono in evidenza il fatto che la risolubilità della congruenza $f(X) \equiv 0 \pmod n$, anche per infiniti valori di n, non implica la risolubilità dell'equazione diofantea $f(X) = 0$.
Ad esempio $2X + 1 = 0$ è un'equazione diofantea non risolubile, mentre $2X + 1 \equiv 0 \pmod n$ è risolubile per ogni intero n dispari, perché $n = 2k + 1$ per un qualche intero $k \geqslant 1$.
(d) Si noti che l'equazione diofantea in due indeterminate:

$$(2X - 1)(3Y - 1) = 0$$

non ha soluzioni, mentre la congruenza:

$$(2X - 1)(3Y - 1) \equiv 0 \pmod n$$

è risolubile, per ogni $n \geqslant 2$. Infatti, n si può sempre scrivere nella forma $n = 2^e(2k - 1)$ con $e \geqslant 0$ e $k \geqslant 1$.
Inoltre, $2^{2e+1} + 1 = (2 + 1)(2^{2e} - 2^{2e-1} + \cdots - 2 + 1)$ dunque $(3h - 1) = 2^{2e+1}$, con $h := (2^{2e} - 2^{2e-1} + \cdots - 2 + 1)$. Pertanto $2^{e+1}n = (2k - 1)(3h - 1)$.
Si può dimostrare, in generale, che se $a, b, c, d \in \mathbb{Z}$, se $\mathrm{MCD}(a, c) = 1$ e se $n \geqslant 2$ allora:

$$(aX + b)(cY + d) \equiv 0 \pmod n$$

è risolubile per ogni n.

1. Esercizi e Complementi

1.1. Provare che:

$$a \equiv b \pmod{n} \Rightarrow \mathrm{MCD}(a, n) = \mathrm{MCD}(b, n).$$

[Suggerimento. Basta provare che l'insieme dei divisori comuni di a ed n coincide con l'insieme dei divisori comuni di b ed n.]

1.2. Provare che:

$$a \equiv b \pmod{n},\ a \equiv b \pmod{m},\ \mathrm{MCD}(n, m) = 1 \Rightarrow a \equiv b \pmod{nm}.$$

[Suggerimento. Applicare il Lemma di Euclide, esistendo $k, h \in \mathbb{Z}$ in modo tale che $kn = a - b = hm$.]

1.3. Verificare che:
(a) il quadrato di ogni intero è congruente a 0 oppure 1 (mod 4);
(b) il quadrato di ogni intero è congruente a 0, oppure 1, oppure 4 (mod 8);
(c) nessun intero congruente a 3 (mod 4) può essere somma di due quadrati (di numeri interi);
(d) nessun intero congruente a 7 (mod 8) può essere somma di tre quadrati (di numeri interi).

1.4. Sia $S := \{r_1, \ldots, r_n\}$ un sistema completo di residui (modulo n). Provare che: scelti $a, b \in \mathbb{Z}$ con $\mathrm{MCD}(a, n) = 1$, l'insieme $S' := \{ar_1 + b, \ldots, ar_n + b\}$ è ancora un sistema completo di residui (modulo n).
[Suggerimento. Provare che: $ar_i + b \equiv ar_j + b \pmod{n} \iff i = j$.]

1.5. Siano n, m interi positivi relativamente primi.
Sia $\{x_1, \ldots, x_n\}$ (rispettivamente $\{y_1, \ldots, y_m\}$) un sistema completo di residui (modulo n) (rispettivamente (modulo m)). Provare che gli elementi $mx_i + ny_j$ (con $1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m$) descrivono un sistema completo di residui (modulo nm).
[Suggerimento. Provare che $mx_i + ny_j \equiv mx_h + ny_k \pmod{nm} \iff i = h$ e $j = k$.]

1.6. Siano $a, b, k, p \in \mathbb{Z}$ con k e p positivi e p primo. Mostrare che:
(a) $a^2 \equiv b^2 \pmod{p} \iff a \equiv b \pmod{p}$ oppure $a \equiv -b \pmod{p}$
(b) $a^k \equiv b^k \pmod{p}, a^{k+1} \equiv b^{k+1} \pmod{p}, p \nmid a \Rightarrow a \equiv b \pmod{p}$.
[Suggerimento. **(a)** $a^2 - b^2 = (a - b)(a + b)$; **(b)** se $p \nmid a$ allora $p \nmid a^k$ quindi $p \nmid b^k$, pertanto a^k e b^k possiedono un inverso aritmetico (mod p).]

1.7. Sia $n \geqslant 2$. Mostrare che:
(a) se n è dispari, allora:

$$1 + 2 + 3 + \cdots + (n - 1) \equiv 0 \pmod{n};$$

(b) per ogni n, allora:

$$1^3 + 2^3 + 3^3 + \cdots + (n - 1)^3 \equiv 0 \pmod{n};$$

(c) se $n \equiv 1, 5 \pmod{6}$, allora:

$$1^2 + 2^2 + 3^2 + \cdots + (n - 1)^2 \equiv 0 \pmod{n}.$$

Dare un controesempio esplicito per **(a)**, quando n è pari, e per **(c)**, quando $n \not\equiv 1, 5 \pmod 6$.
[Suggerimento. Per induzione su n si dimostra che:

$$1 + 2 + \cdots + (n-1) = \frac{n(n-1)}{2};$$

$$1^2 + 2^2 + \cdots + (n-1)^2 = \frac{n(n-1)(2n-1)}{6};$$

$$1^3 + 2^3 + \cdots + (n-1)^3 = \left[\frac{n(n-1)}{2}\right]^2 .]$$

2 Congruenze lineari ed equazioni diofantee lineari

Lo studio della congruenza $f(X) \equiv 0 \pmod{n}$ è particolarmente semplice nel caso in cui $f(X)$ sia un polinomio di grado 1, cioè nel caso di una *congruenza lineare*.

Definizione 2.1. Si chiama *congruenza lineare in una indeterminata X (modulo n)* una congruenza del tipo:

$$aX \equiv b \pmod{n} \tag{1}$$

con $a, b, n \in \mathbb{Z}, n > 0$.

In base alla Definizione 1.23, una soluzione di (1) è un intero $\mathring{x}$ tale che $a\mathring{x} \equiv b \pmod{n}$ e due soluzioni di (1) sono distinte se sono incongruenti modulo n. Vale il seguente fondamentale risultato:

Teorema 2.2. *Siano $a, b, n \in \mathbb{Z}, n > 0$ e sia $d := \mathrm{MCD}(a, n)$. Allora:*
(1) *la congruenza (1) è risolubile se, e soltanto se, $d \mid b$;*
(2) *se $d \mid b$, (1) ha esattamente d soluzioni distinte $\pmod{n}$, che sono date da:*

$$x_k = \alpha^* \cdot b/d + k \cdot n/d, \text{ al variare di } k \text{ con } 0 \leqslant k \leqslant d-1;$$

dove α^* è un inverso aritmetico di $a/d \pmod{n/d}$ (cfr. Proposizione 1.14(a)).

Dimostrazione. (1) Se (1) è risolubile, allora esiste $\mathring{x} \in \mathbb{Z}$ in modo tale che $n \mid (a\mathring{x} - b)$, cioè esiste $k \in \mathbb{Z}$ tale che $a\mathring{x} - b = nk$. Quindi $d \mid (a\mathring{x} - nk) = b$. Viceversa, se $b = d\,\delta$ e $d = ar + ns$ (identità di Bézout), con $\delta, r, s \in \mathbb{Z}$, allora $ar\delta + ns\delta = b$ e quindi $r\delta$ è soluzione di (1).

Alla dimostrazione di **(2)** premettiamo il seguente lemma:

Lemma 2.3. *Siano $a, b, n \in \mathbb{Z}, n > 0$. Se $\mathrm{MCD}(a, n) = 1$, la congruenza (1) ha un'unica soluzione $\mathring{x}$, e risulta:*

$$\mathring{x} \equiv a^* b \pmod{n},$$

dove a^* è un'inverso aritmetico di a (modulo n).

Dimostrazione (Lemma 2.3)**.** È immediata conseguenza della Proposizione 1.3(5), della Definizione 1.13 e della Proposizione 1.14.
Infatti, $a\mathring{x} \equiv aa^*b \equiv b \pmod{n}$. Viceversa, se x è tale che $ax \equiv b \pmod{n}$, allora moltiplicando ambo i membri della congruenza per a^*, otteniamo che $x \equiv a^*b \pmod{n}$. $\square$

Dimostrazione (Teorema 2.2 (2))**.** Poichè $d \mid b$ e $\mathrm{MCD}(a,n) = d$, esistono $\alpha, \beta, \nu \in \mathbb{Z}$ tali che $b = d\beta, a = d\alpha, n = d\nu$ e $\mathrm{MCD}(\alpha, \nu) = 1$. Per (1), esiste $x \in \mathbb{Z}$ tale che $ax \equiv b \pmod{n}$ e dunque $\alpha dx \equiv \beta d \pmod{n}$.
Dalla Proposizione 1.3(11), si ha $\alpha x \equiv \beta \pmod{\nu}$ e quindi, dal Lemma 2.3, $x \equiv \alpha^* \beta \pmod{\nu}$. Dunque, esiste $k \in \mathbb{Z}$ tale che $x = \alpha^* b/d + kn/d$. Tenendo che $d \mid a$ è facile verificare che x_k è una soluzione di (1) e per ogni $k, \quad 0 \leqslant k \leqslant d-1$.
Se h, k sono interi tali che $0 \leqslant h \leqslant d-1, \quad 0 \leqslant k \leqslant d-1$ e se

$$\alpha^* b/d + hn/d \equiv \alpha^* b/d + kn/d \pmod{n},$$

allora $hn/d \equiv kn/d \pmod{n}$. Dal momento che $\mathrm{MCD}(n, n/d) = n/d$ e $n/(n/d) = d$, cancellando (cfr. Proposizione 1.9), otteniamo $h \equiv k \pmod{d}$, cioè $h = k$, essendo $0 \leqslant h, k \leqslant d-1$. Se invece $h \equiv k \pmod{d}$, allora si ha subito $\alpha^* b/d + hn/d \equiv \alpha^* b/d + kn/d \pmod{n}$. Dunque la (2) è completamente dimostrata. $\square$

Il Teorema 2.2 riduce in pratica la ricerca delle soluzioni di (1) alla determinazione di α^*, cioè alla ricerca delle soluzioni della congruenza:

$$\alpha X \equiv 1 \pmod{\nu},$$

(con $\alpha := a/d$, $\nu := n/d$). Su questo problema ritorneremo tra breve.

Osservazione 2.4. Sfruttando meglio l'argomentazione della dimostrazione del Teorema precedente, si ottiene, più in generale, che se $\mathring{x}$ è una fissata soluzione di (1), tutte e sole le d soluzioni di (1) sono date da:

$$x_k = \mathring{x} + kn/d, \text{ al variare di } k \text{ con } 0 \leqslant k \leqslant d-1.$$

Il problema della ricerca delle soluzioni di una congruenza lineare in una indeterminata è equivalente a quello della ricerca delle soluzioni di una equazione diofantea in due indeterminate.
Infatti, $\mathring{x}$ è una soluzione di $aX \equiv b \pmod{n}$ se, e soltanto se, esiste $\mathring{y} \in \mathbb{Z}$ tale che $n\mathring{y} = a\mathring{x} - b$, ovvero se, e soltanto se, $(\mathring{x}, \mathring{y})$ è soluzione dell'equazione diofantea $aX - nY = b$.
È comunque opportuno esaminare direttamente la risoluzione di queste equazioni diofantee, in quanto ciò offrirà un diverso punto di vista per la risoluzione delle congruenze lineari.

Teorema 2.5. *L'equazione diofantea lineare:*

$$aX + cY = b \tag{2}$$

è risolubile se, e soltanto se, $d \mid b$, dove $d := \mathrm{MCD}(a,c)$. Se $(\mathring{x}, \mathring{y})$ è una particolare soluzione di (2)*, tutte e sole le soluzioni di* (2) *sono date da (x_t, y_t), con:*

$$x_t := \mathring{x} + \frac{c}{d}t, \quad y_t := \mathring{y} - \frac{a}{d}t,$$

al variare di $t \in \mathbb{Z}$.

Dimostrazione. Siano $\alpha, \gamma \in \mathbb{Z}$ tali che $d\alpha = a, d\gamma = c$ e $\mathrm{MCD}(\alpha, \gamma) = 1$. Se $(\mathring{x},\ \mathring{y})$ è soluzione di (2), si ha $b = a\mathring{x} + c\mathring{y} = d(\alpha\mathring{x} + \gamma\mathring{y})$ e dunque $d \mid b$. Viceversa, siano $\beta, r, s \in \mathbb{Z}$ tali che $b = d\beta$ e $d = ar + cs$ (identità di Bézout). Si verifica subito che $\mathring{x} := \beta r,\ \mathring{y} := \beta s$ è una soluzione di (2).
Proviamo ora la seconda parte dell'enunciato. Sia $(\mathring{x},\ \mathring{y})$ una fissata soluzione di (2). È immediato verificare che ogni coppia (x_t, y_t) (al variare di $t \in \mathbb{Z}$) è soluzione di (2).
Viceversa, sia (x', y') soluzione di (2). Si ha allora $a\mathring{x} + c\mathring{y} = b = ax' + cy'$, ovvero $a(\mathring{x} - x') = c(y' - \mathring{y})$, da cui $\alpha(x' - \mathring{x}) = \gamma(\mathring{y} - y')$. In base al Lemma di Euclide, $\gamma \mid (\mathring{x} - x')$, quindi esiste $t \in \mathbb{Z}$ tale che $x' - \mathring{x} = \gamma t$ e, dunque, $-\alpha\gamma t = \gamma(y' - \mathring{y})$. Pertanto, si ha $x' = \mathring{x} + (c/d)t$ e $y' = \mathring{y} - (a/d)t$, da cui la tesi. □

Torniamo a considerare la congruenza lineare (1):

$$aX \equiv b \pmod{n}.$$

Da quanto precede, è chiaro che il problema della ricerca di *tutte* le soluzioni di (1) si riduce alla ricerca di *una* soluzione dell'equazione diofantea nelle indeterminate X ed Y:

$$aX - nY = b,$$

oppure, come già osservato, alla ricerca di *un* inverso aritmetico di a/d (modulo n/d). Nel primo caso, *una* soluzione può essere esplicitamente trovata (come indicato nella dimostrazione del Teorema 2.5 riducendo il problema alla risoluzione dell'equazione diofantea nelle indeterminate X' ed Y':

$$aX' + nY' = d$$

(ovvero, calcolando i coefficienti della relazione di Bézout che esprime $d := \mathrm{MCD}(a, n) = \mathrm{MCD}(a, -n)$ in funzione di a e $-n$) e ció può essere fatto applicando l'algoritmo euclideo delle divisioni successive.
Nel secondo caso, ci si è ricondotti allo studio di una congruenza del tipo:

$$aX \equiv 1 \pmod{n} \quad \text{con} \quad \mathrm{MCD}(a, n) = 1,$$

la cui unica soluzione (cfr. Lemma 2.3) fornisce appunto l'inverso aritmetico a^* di $a \pmod{n}$. Perverremo ad un metodo effettivo per la determinazione esplicita di a^* nel paragrafo successivo, come conseguenza del Teorema di Euler-Fermat. Per il momento concludiamo il paragrafo con alcune definizioni e risultati utili per il seguito e, comunque, propedeutici a tale teorema.

Proposizione 2.6. *Sia n un intero $n \geqslant 2$ ed $S := \{0, 1, \ldots, n-1\}$ il sistema completo di residui (modulo n) minimo. Sia, inoltre, S^* il sottoinsieme di S così definito:*

$$S^* := \{k \in S \quad : \quad \mathrm{MCD}(k, n) = 1\}.$$

Un intero a ammette inverso aritmetico (modulo n) se, e soltanto se, esiste $k \in S^*$ in modo tale che $a \equiv k \pmod{n}$.

Dimostrazione. Tenuto conto della Proposizione 1.14(a) e dell'Esercizio 1.1 otteniamo che a ammette inverso aritmetico (modulo n) se, e soltanto se, $\mathrm{MCD}(a, n) = 1$, ovvero se, e soltanto se, esiste $k \in S$ tale che $a \equiv k \pmod{n}$ e $\mathrm{MCD}(k, n) = 1$. La conclusione è ormai evidente. □

Definizione 2.7. Si chiama *sistema ridotto di residui (modulo n)* ogni insieme $S^* := \{k_1, \ldots, k_t\}$, con $k_i \in \mathbb{Z}$ per $1 \leqslant i \leqslant t$, tale che, per ogni $a \in \mathbb{Z}$ verificante la condizione $\mathrm{MCD}(a, n) = 1$, esiste un unico $k_i \in S^*$ tale che $a \equiv k_i \pmod{n}$.

È subito visto che $\mathrm{MCD}(n, k_i) = 1$, per ogni $k_i \in S^*$.

Osservazione 2.8. Lo studio dei sistemi ridotti di residui può essere efficacemente effettuato studiando il gruppo delle unità degli anelli del tipo $\mathbb{Z}/n\mathbb{Z}$. Lasciamo al lettore il piacere di esprimere in termini gruppali la teoria che svilupperemo nel seguente scorcio di paragrafo e nel paragrafo successivo.

Definizione 2.9. Si chiama *indicatore* (o *funzione φ*) *di Eulero* l'applicazione $\varphi : \mathbb{N}^+ \to \mathbb{N}$ che associa ad ogni intero $n > 0$ il numero $\varphi(n)$ degli interi compresi tra 1 e $n - 1$ che sono relativamente primi con n.

Si verifica facilmente che ogni sistema ridotto di residui (modulo n) può essere posto in corrispondenza biunivoca con quello definito nella Proposizione 2.6, che chiameremo *sistema ridotto di residui (modulo n) minimo positivo* il quale, ovviamente, ha cardinalità $\varphi(n)$. Dunque:

Proposizione 2.10. *Ogni sistema ridotto di residui (modulo n) ha cardinalità $\varphi(n)$.* □

2. Esercizi e Complementi

2.1. Trovare tutte le eventuali soluzioni delle congruenze:

$$\begin{aligned} &(\mathbf{a}) \quad 15X \equiv 9 \pmod{25} \\ &(\mathbf{b}) \quad 17X \equiv 14 \pmod{21} \\ &(\mathbf{c}) \quad 3X \equiv 6 \pmod{9} \end{aligned}$$

[Suggerimento: **(a)** $\mathrm{MCD}(15, 25) = 5$, $5 \nmid 9$, non è risolubile.
(b) $\mathrm{MCD}(17, 21) = 1$, quindi la congruenza ha un'unica soluzione $\pmod{21}$ data da $17^* \cdot 14$ dove $17^* \equiv 5 \pmod{21}$ e quindi $5 \cdot 14 = 70 \equiv 7 \pmod{21}$.
(c) $\mathrm{MCD}(3, 9) = 3 \mid 6$, quindi la congruenza ha 3 soluzioni che sono precisamente: $x_0 = 2, \quad x_1 = 2 + 3 = 5, \quad x_2 = 2 + 2 \cdot 3 = 8 \pmod{9}$.]

2.2. Metodo ricorsivo per la risoluzione di una congruenza lineare in una indeterminata
Siano $a, b, n \in \mathbb{Z}$ con a ed n interi positivi e $\mathrm{MCD}(a, n) = 1$.
(a) Mostrare che se $x \in \mathbb{Z}$ è la soluzione della congruenza:

$$aX \equiv b \pmod{n}, \tag{$*$}$$

allora x è anche soluzione della congruenza:

$$rX \equiv -bq \pmod{n}, \tag{$*'$}$$

dove $n = a \cdot q + r$ con $q, r \in \mathbb{Z}$ ed $0 \leqslant r \leqslant a - 1$.
(b) Mostrare che, se si itera la procedura descritta in **(a)**, dopo un numero finito di passi la soluzione di $(*)$ è anche soluzione di una congruenza del tipo:

$$X \equiv c \pmod{n}, \tag{$**$}$$

per un qualche $c \in \mathbb{Z}$.
(c) Risolvere, con il metodo sopra descritto, la congruenza

$$6X \equiv 7 \pmod{23}.$$

[Suggerimento: **(a)** Si noti che se $ax \equiv b \pmod{n}$ allora:
$rx = nx - aqx \equiv -bq \pmod{n}$.
(b) È ovvia perché se $a \neq 1$ allora $0 < r < a$.
(c) Si noti che $23 = 6 \cdot 3 + 5$ e quindi:
- da $23 = 6 \cdot 3 + 5$ passiamo a $5X \equiv -7 \cdot 2 \equiv 2 \pmod{23}$;
- da $23 = 5 \cdot 4 + 3$ passiamo a $3X \equiv -2 \cdot 4 \equiv 15 \pmod{23}$;
- da $23 = 3 \cdot 7 + 2$ passiamo a $2X \equiv -15 \cdot 7 \equiv 10 \pmod{23}$;
- da $23 = 2 \cdot 11 + 1$ passiamo a $X \equiv -10 \cdot 11 \equiv 5 \pmod{23}$.]

2.3. Determinare tutte le eventuali soluzioni delle seguenti equazioni diofantee lineari in due indeterminate:
(a) $2X + 5Y = 11$;
(b) $21X - 14Y = 147$;
(c) $14X + 2Y = 9$.
[Soluzioni:**(a)** $x = 3 + 5t, y = 1 - 2t, t \in \mathbb{Z}$.
(b) $x = 7 - 14t, y = -21t, t \in \mathbb{Z}$.
(c) Non ha soluzioni.]

2.4. (Sylvester, 1884)
Siano a, b, n tre interi positivi con $\mathrm{MCD}(a, b) = 1$. Mostrare che:
(a) Per ogni $c > ab$, l'equazione

$$aX + bY = c \qquad (*_c)$$

ha soluzioni $(x, y) \in \mathbb{N}^+ \times \mathbb{N}^+$.
(b) Posto $g = g(a, b) := ab - a - b$, per ogni $c > g$, l'equazione $(*_c)$ ha soluzioni $(x, y) \in \mathbb{N} \times \mathbb{N}$. Il numero $g(a, b)$ è detto *numero di Frobenius*.
(c) Se $c = ab$, l'equazione $(*_c)$ non ha soluzioni in $\mathbb{N}^+ \times \mathbb{N}^+$.
(d) Se $c = g(a, b)$, l'equazione $(*_c)$ non ha soluzioni in $\mathbb{N} \times \mathbb{N}$.
(e) Se $c_1, c_2 \in \mathbb{N}$ e se $(*_{c_1})$ e $(*_{c_2})$ sono risolubili in $\mathbb{N}^+ \times \mathbb{N}^+$ (rispettivamente, in $\mathbb{N} \times \mathbb{N}$), allora $(*_{c_1+c_2})$ è risolubile in $\mathbb{N}^+ \times \mathbb{N}^+$ (rispettivamente, in $\mathbb{N} \times \mathbb{N}$).
(f) $g(a, b)$ è sempre dispari.
(g) Esattamente per $\dfrac{(g(a, b) + 1)}{2}$ elementi c, con $0 \leqslant c \leqslant g(a, b)$, l'equazione $(*_c)$ è risolubile in $\mathbb{N} \times \mathbb{N}$.

Data l'equazione

$$5X + 7Y = c \qquad (**)$$

(h) Determinare una soluzione in $\mathbb{N} \times \mathbb{N}$ di $(**)$, quando $c = 24$.
(i) Determinare tutti i valori di c, con $0 \leqslant c \leqslant 23$, per i quali $(**)$ è risolubile in $\mathbb{N} \times \mathbb{N}$.
[Suggerimento: Innanzitutto, utilizzando il Teorema 2.5 e scegliendo opportunamente il parametro t, è possibile trovare $u, v \in \mathbb{N}^+$ in modo tale che:

$$au - bv = 1.$$

(a) Si noti che $auc - bvc = c > ab$, dunque $\frac{uc}{b} - \frac{vc}{a} > 1$ quindi esiste $t \in \mathbb{N}$ tale che $\frac{uc}{b} > t > \frac{vc}{a}$. Si vede che $(x := uc - bt,\ y := at - vc) \in \mathbb{N} \times \mathbb{N}$ è una soluzione di $(*_c)$.
(b) Se $ab \geqslant c > ab - a - b$, allora $c' := c + a + b > ab$, quindi $(*_{c'})$ ha una soluzione $(x', y') \in \mathbb{N}^+ \times \mathbb{N}^+$. È subito visto che $(x' - 1, y' - 1) \in \mathbb{N} \times \mathbb{N}$ è una soluzione di $(*_c)$.
(c) Se $ax + by = ab$, allora si perviene facilmente ad un assurdo utilizzando il Lemma di Euclide.
(d) segue facilmente da **(c)**.
(e) È immediato che se (x_i, y_i) è soluzione di $(*_{c_i})$, allora $(x_1 + x_2, y_1 + y_2)$ è soluzione di $(*_{c_1+c_2})$.
(f) Non potendo essere a e b entrambi pari, è subito visto che, in ogni caso, $ab - a - b \equiv 1 \pmod 2$.
(g) Si noti che se c varia tra 0 e g anche $g - c$ varia tra 0 e g e quindi l'applicazione

$$\{c : 0 \leqslant c \leqslant g\} \longrightarrow \{c : 0 \leqslant c \leqslant g\} \quad c \longmapsto g - c$$

è una biiezione. Inoltre, se $(*_c)$ è risolubile in $\mathbb{N} \times \mathbb{N}$, $(*_{g-c})$ non può essere risolubile in $\mathbb{N} \times \mathbb{N}$, altrimenti $(*_{g=c+(g-c)})$ sarebbe risolubile in $\mathbb{N} \times \mathbb{N}$.
(h) In questo caso $u = 3, v = 2$, quindi $\dfrac{3 \cdot 24}{7} > 10 > \dfrac{2 \cdot 24}{5}$ dunque $(2 = 3 \cdot 24 - 7 \cdot 10, 2 = 5 \cdot 10 - 2 \cdot 24)$ è una soluzione di $(**)$ per $c = 24$.
(i) $c = 0, 5, 7, 10, 12, 14, 15, 17, 19, 20, 21, 22$.]

2.5. (a) Sia $m \geqslant 2$ e siano $a_1, \ldots, a_m$ interi non tutti nulli. Scelto $b \in \mathbb{Z}$ e posto $d := \mathrm{MCD}(a_1, \ldots, a_m)$, verificare che l'equazione diofantea:

$$a_1X_1 + a_2X_2 + \cdots + a_mX_m = b$$

è risolubile se, e soltanto se, $d \mid b$.
(b) Metodo algoritmico per la risoluzione della equazione diofantea lineare:

$$a_1X_1 + \cdots + a_mX_m = b \qquad (*)$$

dove $b, a_i \in \mathbb{Z}, a_i \neq 0$ per $1 \leqslant i \leqslant m$.

I Riduzione. Non è restrittivo limitarsi al caso in cui $a_i \in \mathbb{N}^+$ per ogni i. Infatti se $a_i < 0$, basta sostituire tali coefficienti con $-a_i$ e cambiare segno alla indeterminata X_i.

II Riduzione. Non è restrittivo supporre che $a_i \neq a_j$ se $i \neq j$. Perché se ad esempio $a_1 = a_2$, ponendo $X := X_1 + X_2$, abbiamo la seguente equazione diofantea:

$$a_1X + a_3X_3 + \cdots + a_mX_m = b. \qquad (**)$$

Una soluzione $(x_1, \cdots, x_m)$ di $(*)$ determina una soluzione di $(**)$ $(x_1 + x_2, x_3, \cdots, x_m)$. Mentre, una soluzione $(x, x_3, \cdots, x_m)$ determina infinite soluzioni di $(*)$, ottenute ponendo $x_2 := x - x_1$ e facendo variare comunque $x_1 \in \mathbb{Z}$.

Procedimento ricorsivo di risoluzione. Supponiamo che $a_i \in \mathbb{N}^+$ e che $a_i \neq a_j$, per $1 \leqslant i \neq j \leqslant m$, e supponiamo inoltre, per fissare le idee, che $a_1 = max\{a_1, \cdots, a_m\}$. Dunque, dividendo a_1 per a_2, otteniamo la seguente relazione:

$$a_1 = a_2q + r \quad \text{con} \quad 0 \leqslant r < a_2 (< a_1), \quad q \in \mathbb{Z}.$$

Poniamo

$$X_1' := qX_1 + X_2, \quad X_2' := X_1, \quad a_1' := a_2, \quad a_2' := r.$$

Dunque $(*)$ diventa:

$$a_1'X_1' + a_2'X_2' + a_3X_3 + \cdots + a_mX_m = b. \qquad (*')$$

Una soluzione $(x_1, \cdots, x_m)$ di $(*)$ determina canonicamente una soluzione di $(*')$: $(qx_1 + x_2, x_1, x_3, \cdots, x_m)$. Viceversa, la soluzione $(x_1', x_2', x_3, \cdots, x_m)$ di $(*')$ determina la soluzione $(x_2', x_1' - qx_2', x_3, \cdots, x_m)$ di $(*)$.
Pertanto, ci siamo ricondotti ad una nuova equazione diofantea lineare $(*')$ con $max\{a_1', a_2', a_3, \cdots, a_m\} < max\{a_1, a_2, a_3, \cdots, a_m\}$.

Dimostrare che questo processo conduce, dopo un numero finito di passi, ad una equazione in due indeterminate e cioè ad un caso già trattato, per il quale sappiamo descrivere tutte le soluzioni.

Osservazioni. (1) Notiamo che, se esiste un coefficiente a_i, per $2 \leqslant i \leqslant m$, tale che $a_i \mid a_1$, conviene dividere a_1 per a_i. Infatti, in tal caso, $a_1 = qa_i + r$ con $r = 0$ e, quindi, nell'equazione diofantea $(*')$, determinata in questo modo da $(*)$, appariranno giá al più $m - 1$ indeterminate.

(2) Se uno dei coefficienti a_i è uguale ad 1, allora ovviamente $(*)$ è risolubile. Tutte le soluzioni di $(*)$ si ottengono ponendo

$$x_i := b - (a_1x_1 + \cdots + a_{i-1}x_{i-1} + a_{i+1}x_{i+1} + \cdots + a_mx_m)$$

e facendo variare comunque $x_1, x_2, \cdots, x_{i-1}, x_{i+1}, \cdots, x_m \in \mathbb{Z}$.
(3) È subito visto che se $(*)$ è risolubile e se $(\mathring{x}_1, \cdots, \mathring{x}_m)$ è una soluzione di $(*)$, allora $(x_1, \cdots, x_m)$ con

$$\begin{aligned} x_i &= \mathring{x}_i + a_m t_i \qquad 1 \leqslant i \leqslant m-1 \\ x_m &= \mathring{x}_m - \sum_{i=1}^{m-1} a_i t_i \end{aligned}$$

è ancora una soluzione di $(*)$, al variare comunque di $t_1, \cdots, t_{m-1} \in \mathbb{Z}$. Non è vero, in generale, che tutte le soluzioni di $(*)$ siano del tipo sopra descritto.
Ad esempio, se consideriamo l'equazione diofantea $2X + 4Y = 6$, allora $(1, 1)$ è una soluzione. Però $(3, 0)$, che è un'altra soluzione di tale equazione, non si trova nell'insieme infinito di soluzioni $(1 + 4t, 1 - 2t)$, descritto al variare di $t \in \mathbb{Z}$.

(c) Risoluzione di un'equazione diofantea lineare in tre indeterminate
Si consideri l'equazione diofantea lineare in tre indeterminate

$$aX + bY + cZ = d \quad \text{con } \mathrm{MCD}(a, b, c) \mid d. \qquad (*)$$

Sotto tale condizione $(*)$ è risolubile. Per determinare le sue soluzioni associamo a $(*)$ due equazioni diofantee lineari ciascuna in due indeterminate:

$$aX_1 + \mathrm{MCD}(b, c)X_2 = d, \qquad (*_1)$$

$$bY_1 + cY_2 = \mathrm{MCD}(b, c) \qquad (*_2)$$

Essendo $\mathrm{MCD}(a, \mathrm{MCD}(b, c)) = \mathrm{MCD}(a, b, c)$, è evidente che $(*)$ è risolubile se e soltanto se $(*_1)$ è risolubile. Inoltre, è noto che se $(\mathring{x}_1, \mathring{x}_2)$ è una soluzione di $(*_1)$ allora tutte le soluzioni di $(*_1)$ sono descritte da:

$$\begin{aligned} x_1 &= \mathring{x}_1 + (\frac{\mathrm{MCD}(b, c)}{\mathrm{MCD}(a, b, c)})t \\ x_2 &= \mathring{x}_2 - (\frac{a}{\mathrm{MCD}(a, b, c)})t \end{aligned}$$

al variare comunque di $t \in \mathbb{Z}$.
Sappiamo che $(*_2)$ è sempre risolubile (Teorema 2.5). Sia $(\mathring{y}_1, \mathring{y}_2)$ una sua soluzione. Mostrare che tutte le soluzioni di $(*)$ sono descritte da:

$$\begin{aligned} x &= \mathring{x}_1 + (\frac{\mathrm{MCD}(b, c)}{\mathrm{MCD}(a, b, c)})t \\ y &= \mathring{y}_1\mathring{x}_2 - \mathring{y}_1\,(\frac{a}{\mathrm{MCD}(a, b, c)})t + (\frac{c}{\mathrm{MCD}(b, c)})s \\ z &= \mathring{y}_2\mathring{x}_2 - \mathring{y}_2\,(\frac{a}{\mathrm{MCD}(a, b, c)})t - (\frac{b}{\mathrm{MCD}(b, c)})s \end{aligned}$$

al variare di $t, s \in \mathbb{Z}$.
[Suggerimento: notiamo che:

$d = aX_1 + \text{MCD}(b,c)X_2 = aX_1 + (bY_1 + cY_2)X_2 = aX_1 + bY_1X_2 + cY_2X_2$, ed essendo anche $d = aX + bY + cZ$, allora, per la validità della uguaglianza formale precedente, dobbiamo avere:

$$X = X_1,\ Y = Y_1X_2,\ Z = Y_2X_2.$$

Da ciò ricaviamo che la generica soluzione (x, y, z) di $(*)$ è sempre esprimibile come $(x_1, \mathring{y}_1x_2, \mathring{y}_2x_2)$, dove (x_1, x_2) è una soluzione di $(*_1)$ ed $(\mathring{y}_1, \mathring{y}_2)$ è una qualche soluzione di $(*_2)$.
Dal momento che, quando $(\mathring{y}_1, \mathring{y}_2)$ varia tra le soluzioni $bY_1 + cY_2 = \text{MCD}(b,c)$, $(\mathring{y}_1x_2, \mathring{y}_2x_2)$ varia tra le soluzioni di

$$bY + cZ = \text{MCD}(b,c)x_2, \qquad (**_2)$$

allora l'insieme $\{(\mathring{y}_1x_2, \mathring{y}_2x_2) : (\mathring{y}_1, \mathring{y}_2) \text{ varia tra le soluzioni di } (*_2)\}$ coincide con l'insieme $\{(y,z) : (y,z) \text{ è una soluzione di } (**_2)\}$.
Poichè $(\mathring{y}_1x_2, \mathring{y}_2x_2)$ è una soluzione di $(**_2)$, allora una qualunque soluzione di $(**_2)$ è data da:

$$y = \mathring{y}_1x_2 + (\frac{c}{\text{MCD}(b,c)})s$$
$$z = \mathring{y}_2x_2 - (\frac{b}{\text{MCD}(b,c)})s$$

al variare di $s \in \mathbb{Z}$.
In conclusione, una qualunque soluzione di $(*)$ è del tipo:

$$x = x_1 = \mathring{x}_1 + \frac{\text{MCD}(b,c)}{\text{MCD}(a,b,c)})t$$
$$y = \mathring{y}_1x_2 + (\frac{c}{\text{MCD}(b,c)})s = \mathring{y}_1x_2 - \mathring{y}_1\,(\frac{a}{\text{MCD}(a,b,c)})t + (\frac{c}{\text{MCD}(b,c)})s$$
$$z = \mathring{y}_2x_2 - (\frac{b}{\text{MCD}(b,c)})s = \mathring{y}_2x_2 - \mathring{y}_2\,(\frac{a}{\text{MCD}(a,b,c)})t - (\frac{b}{\text{MCD}(b,c)})s$$

al variare di $t, s \in \mathbb{Z}$.)

(d) Determinare tutte le soluzioni dell'equazione diofantea:

$$6X - 4Y + 8Z = 12.$$

(Soluzione. Dal momento che $2 = \text{MCD}(6,-4,8) \mid 12$ e che $\text{MCD}(-4,8) = 4$, allora consideriamo le seguenti equazioni diofantee lineari in due indeterminate:

$$6X_1 + 4X_2 = 12 \quad \text{ovvero} \quad 3X_1 + 2X_2 = 6 \qquad (*_1)$$
$$-4Y_1 + 8Y_2 = 4 \quad \text{ovvero} \quad Y_1 - 2Y_2 = -1 \qquad (*_2)$$

È subito visto che $(1,1)$ è una soluzione della seconda equazione e $(2,0)$ è una soluzione della prima. Pertanto, le soluzioni dell'equazione diofantea assegnata

sono date da:

$$\begin{aligned} x &= 2 + 2t \\ y &= \left(\frac{-6}{2}\right) t + \left(\frac{8}{4}\right) s = -3t + 2s \\ z &= \left(\frac{-6}{2}\right) t + \left(\frac{4}{4}\right) s = -3t + s \end{aligned}$$

al variare comunque di $t, s \in \mathbb{Z}$.
Quindi ad esempio, per $s = t = 0$, abbiamo $(2, 0, 0)$; per $t = -1$ ed $s = 0$, abbiamo $(0, 3, 3)$; per $t = 0$ ed $s = 1$ abbiamo $(2, 2, 1)$; per $t = 1$ ed $s = 0$ abbiamo $(4, -3, -3)$; per $t = 1$ ed $s = 1$ abbiamo $(4, -1, -2)$.]

2.6. Mostrare che la congruenza $aX + bY \equiv c \pmod{n}$ è risolubile se e soltanto se $d := \mathrm{MCD}(a, b, n) \mid c$. In tal caso ha esattamente dn soluzioni incongruenti.
[Soluzione. La prima affermazione discende dal fatto che $aX + bY \equiv c \pmod{n}$ è risolubile se e soltanto se è risolubile l'equazione diofantea in tre indeterminate $aX + bY - nZ = c$.
Per quanto riguarda la seconda affermazione, notiamo che se $\widetilde{d} := \mathrm{MCD}(b, c)$, per ogni $x \pmod{n}$ che risolve la congruenza $aX \equiv c \pmod{\widetilde{d}}$ allora la congruenza $bY \equiv c - ax \pmod{n}$ è risolubile ed ha esattamente $\widetilde{d}$ soluzioni. D'altro lato, poiché $\mathrm{MCD}(a, \widetilde{d}) = \mathrm{MCD}(a, b, n) = d$, la congruenza $aX \equiv c \pmod{\widetilde{d}}$ è risolubile ed ha d soluzioni $\pmod{\widetilde{d}}$, siano esse $\{x_1, \ldots, x_d\}$.
Se k è quell'intero tale che $\widetilde{d}k = n$, allora gli elementi $\{x_i + h\widetilde{d} : 1 \leqslant i \leqslant d,\ 1 \leqslant h \leqslant k\}$ sono gli elementi non congrui $\pmod{n}$ che verificano la congruenza $aX \equiv c \pmod{\widetilde{d}}$.
Per ciascuno dei dk elementi $x \in \{x_i + h\widetilde{d} : 1 \leqslant i \leqslant d,\ 1 \leqslant h \leqslant k\}$, come abbiamo già osservato, la congruenza $bY \equiv c - ax \pmod{n}$ è risolubile ed ammette $\widetilde{d}$ soluzioni. In conclusione, la congruenza assegnata ammette $dk\widetilde{d} = dn$ soluzioni non congrue $\pmod{n}$.]

2.7. Determinare tutte le soluzioni della congruenza

$$2X + 4Y \equiv 6 \pmod{8}$$

[Soluzione. $\mathrm{MCD}(2, 4, 8) = 2 \mid 6$ quindi la congruenza è risolubile. Consideriamo la congruenza

$$2X \equiv 6 \pmod{\mathrm{MCD}(4, 8)}$$

Poiché $4 = \mathrm{MCD}(4, 8)$ e $\mathrm{MCD}(2, 4) = 2 \mid 6$, quest'ultima congruenza è risolubile ed ammette 2 soluzioni $\pmod{4}$, che sono $x_1 = 1$ ed $x_2 = 3$.
Gli elementi $x_i + 4h$, $1 \leqslant h \leqslant 2$, sono gli elementi non congrui $\pmod{8}$ che verificano la congruenza $2X \equiv 6 \pmod{4}$. Per ciascuno di tali elementi x (e cioè $x \in \{5, 1, 7, 3\}$) la congruenza $4Y \equiv 6 - 2x \pmod{8}$ è risolubile ed ammette 4 soluzioni non congrue. Precisamente:

$$\begin{aligned} x = 1 \quad &\Rightarrow \quad y = 1, 3, 5, 7 \\ x = 3 \quad &\Rightarrow \quad y = 0, 2, 4, 6 \\ x = 5 \quad &\Rightarrow \quad y = 1, 3, 5, 7 \\ x = 7 \quad &\Rightarrow \quad y = 0, 2, 4, 8.] \end{aligned}$$

2.8. Determinare le soluzioni della congruenza:

$$2X + 3Y \equiv 1 \pmod 7$$

[Soluzione. $(0,5),(1,2),(2,6),(3,3),(4,0),(5,4),(6,1) \pmod 7$.]

2.9. (a) Siano $n, c, a_1, \ldots, a_r \in \mathbb{Z}, n > 0$. Posto $d :=\text{MCD}(n, a_1, \ldots, a_r)$, dimostrare che la congruenza:

$$a_1X_1 + \cdots + a_rX_r \equiv c \pmod n$$

è risolubile se, e soltanto se, $d \mid c$.
(b) Se la congruenza considerata in (a) è risolubile, allora ammette dn^{r-1} soluzioni distinte.
[Suggerimento. Per **(a)** cfr. Esercizio 2.5(a), osservando che la congruenza data è risolubile se e soltanto se l'equazione diofantea in $(r+1)$ indeterminate:

$$a_1X_1 + \cdots + a_rX_r + nX_{r+1} = c$$

è risolubile; per **(b)** si procede per induzione su r. Se $r = 1$, il risultato è già noto (Teorema 2.2). Il caso $r = 2$ è trattato nell'Esercizio 2.6 ed indica come procedere nel passo induttivo da $r-1$ ad r indeterminate.]

2.10. Sia $S^* := \{a_1, \ldots, a_{\varphi(n)}\}$ un sistema ridotto di residui (modulo n).
(a) Verificare che se $a \in \mathbb{Z}$ e $\text{MCD}(a, n) = 1$, allora $T^* := \{aa_1, \ldots, aa_{\varphi(n)}\}$ è ancora un sistema ridotto di residui (modulo n).
(b) È vero che, scelto $b \in \mathbb{Z}, \{a_1 + b, \ldots, a_{\varphi(n)} + b\}$ è ancora un sistema ridotto di residui (modulo n)?
[Suggerimento. **(a)** Elementi distinti di S^* sono certo incongruenti $\pmod n$; inoltre risulta $\text{MCD}(aa_i, n) = 1, 1 \leqslant i \leqslant \varphi(n)$; dedurre che ogni elemento di T^* è congruente $\pmod n$ ad un elemento di S^*. **(b)** Porre $n = 4, b = 1, S^* = \{1, 3\}$.]

2.11. (a) Siano $a_1, \ldots, a_t, n \in \mathbb{Z}$ tali che $n > 0, t := \varphi(n)$, $\text{MCD}(a_i, n) = 1$ e $a_i \not\equiv a_j \pmod n$, presi comunque i, j tali che $1 \leqslant i, j \leqslant t$ e $i \neq j$. Verificare che $\{a_1, \ldots, a_r\}$ è un sistema ridotto di residui (modulo n).
(b) Provare, con opportuni esempi, che $\varphi(n)$ interi a 2 a 2 incongruenti $(\text{mod } n)$ possono non costituire un sistema ridotto di residui (modulo n).
[Suggerimento. Se $a_i = nq_i + l_i$, con $q_i, l_i \in \mathbb{Z}$ e $1 \leqslant l_i \leqslant n-1$, allora $\{l_1, \ldots, l_t\}$ è l'insieme S^* definito nella Proposizione 2.6, cioè il sistema ridotto di residui minimo positivo. Per ogni $a \in \mathbb{Z}$ tale che $\text{MCD}(a, n) = 1$, risulta $a = nq + l$ con $l, q \in \mathbb{Z}$ ed $l \in S^*$. Da ciò segue facilmente **(a)**. Per **(b)**, si prenda $n = 4$, quindi $\varphi(n) = 2$; l'insieme $\{2, 3\}$ non forma un sistema ridotto di residui $\pmod 4$, anche se $2 \not\equiv 3 \pmod 4$, perché $\text{MCD}(2, 4) \neq 1$.]

2.12. Siano n, m interi positivi relativamente primi. Sia $S^* := \{x_1, \ldots, x_{\varphi(n)}\}$ (rispettivamente, $T^* := \{y_1, \ldots, y_{\varphi(m)}\}$) un sistema ridotto di residui (modulo n) (rispettivamente, (modulo m)). Dimostrare che

$$V^* := \{mx_i + ny_i,\ 1 \leqslant i \leqslant \varphi(n),\ 1 \leqslant j \leqslant \varphi(m)\}$$

è un sistema ridotto di residui (modulo nm).
[Suggerimento. Facendo uso del Lemma di Euclide, verificare che:

se $mx_i + ny_j \equiv mx_h + ny_k \pmod{nm}$, allora $x_i \equiv x_h \pmod{n}$, $y_j \equiv y_k \pmod{m}$ e dunque $x_i = x_h$ e $y_j = y_k$. Questo assicura che gli elementi di V^* sono tutti distinti (modulo nm). Se poi $z \in \mathbb{Z}$ e $\mathrm{MCD}(z, mn) = 1$, allora necessariamente $\mathrm{MCD}(z, n) = 1$ e $\mathrm{MCD}(z, m) = 1$. Pertanto, esiste un unico i, $1 \leqslant i \leqslant \varphi(n)$, ed un unico j, $1 \leqslant j \leqslant \varphi(m)$, in modo tale che $z \equiv x_i \pmod{n}$ e $z \equiv y_j \pmod{m}$. È subito visto che $z \equiv mx_i + ny_j \pmod{nm}$.]

2.13. **(a)** Mostrare che se n ed m sono interi positivi e $\mathrm{MCD}(n, m) = 1$, allora $\varphi(nm) = \varphi(n)\varphi(m)$.
(b) Se p è primo ed $e \geqslant 1$, mostrare che:

$$\varphi(p^e) = p^e - p^{e-1} = p^e \left(1 - \frac{1}{p}\right).$$

(c) Se $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ con p_i primo, $e_i \geqslant 1, p_i \neq p_j$ se $1 \leqslant i \neq j \leqslant r$, allora

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

[Suggerimento. **(a)** È una conseguenza immediata dell'Esercizio 2.12. **(b)** Basta notare che gli interi tra 1 e p^e che sono divisibili per p sono $p, 2p, 3p, \ldots, p^2, 2p^2, \ldots, p^3, \ldots, p^{e-1}, 2p^{e-1}, \ldots, p^e$ che sono in numero di $p \cdot p \cdots p$, prodotto effettuato $(e-1)$ volte, cioè p^{e-1}. **(c)** Discende da (a) e (b).]

2.14. Siano $a, b, c, d, e, f, n \in \mathbb{Z}$ con $n \geqslant 2$. Poniamo

$$\Delta := ad - bc.$$

Consideriamo il seguente sistema di due congruenze lineari in due incognite:

$$\begin{cases} aX + bY & \equiv e \pmod{n} \\ cX + dY & \equiv f \pmod{n} \end{cases} \qquad (*)$$

Se $\mathrm{MCD}(\Delta, n) = 1$ e se Δ^* è l'inverso aritmetico di $\Delta \pmod{n}$, allora mostrare che tale sistema ha un'unica soluzione $(\mathrm{mod}\ n)$ data da:

$$x \equiv \Delta^*(de - bf) \pmod{n},$$
$$y \equiv \Delta^*(af - ce) \pmod{n}.$$

[Suggerimento. Si moltiplichi la prima congruenza del sistema per d e la seconda per b e, poi, si sottragga la seconda congruenza dalla prima congruenza. Si ottiene:

$$\Delta X \equiv (de - bf) \pmod{n}.$$

In modo analogo, moltiplicando la prima congruenza per c e la seconda per a e sottraendo la prima dalla seconda, si ottiene:

$$\Delta Y \equiv (af - ce) \pmod{n}.]$$

2.15. Trovare, al variare tra gli interi del parametro λ, le soluzioni del seguente sistema di congruenze lineari:

$$\begin{cases} 2X + 3Y & \equiv 5 \pmod{7} \\ X + \lambda Y & \equiv 6 \pmod{7} \end{cases}$$

[Soluzione. $\Delta \equiv 0 \pmod 7$ se, e soltanto se, $\lambda \equiv 5 \pmod 7$. Per $\lambda = 5$, le soluzioni del sistema sono: $(0,4),(1,1),(2,5),(3,2),(4,6),(5,3),(6,0)$. Se $\lambda \in \{0,1,2,3,4\}$, il sistema ha un'unica soluzione: $(6,0)$.]

2.16. Siano $a,b,c,d,e,f,p \in \mathbb{Z}$ con p primo. Consideriamo il seguente sistema di due congruenze lineari in due incognite:

$$\begin{cases} aX + bY & \equiv e \pmod p \\ cX + dY & \equiv f \pmod p \end{cases} \qquad (*)$$

Sia $\Delta := ad - bc, \alpha := de - bf, \beta := af - ce$. Supponiamo che $\mathrm{MCD}(a,b,p) = 1$ e $1 = \mathrm{MCD}(c,d,p)$. Mostrare che:
(a) Se $\Delta \equiv 0 \pmod p$ e se $\alpha \equiv \beta \equiv 0 \pmod p$ allora il sistema $(*)$ ha p soluzioni.
(b) Se $\Delta \equiv 0 \pmod p$ e se $\alpha \not\equiv 0 \pmod p$ oppure $\beta \not\equiv 0 \pmod p$ allora il sistema $(*)$ non è risolubile.
(c) Se $\Delta \not\equiv 0 \pmod p$, allora il sistema $(*)$ ha un'unica soluzione.
[Suggerimento. **(a)** e **(b)** Osservare che se $(*)$ è risolubile e $\Delta \equiv 0 \pmod p$ allora necessariamente $\alpha \equiv \beta \equiv 0 \pmod p$, dal momento che $\Delta X \equiv \alpha \pmod p$ e $\Delta Y \equiv \beta \pmod p$. Inoltre se $\Delta \equiv \alpha \equiv \beta \equiv 0 \pmod p$ allora si vede facilmente che $c \equiv ta \pmod p, d \equiv tb \pmod p, f \equiv te \pmod p$, per qualche $t \not\equiv 0 \pmod p$, e quindi le soluzioni di $(*)$ coincidono con le soluzioni di $aX + bY \equiv e \pmod p$, che sono in numero di p (cfr. l'Esercizio 2.6). **(c)** È un caso particolare del precedente Esercizio 2.14.]

2.17. Trovare, al variare tra gli interi del parametro λ, le soluzioni del seguente sistema di congruenze lineari:

$$\begin{cases} 4X + \lambda Y & \equiv 2 \pmod 5 \\ 2X + 3Y & \equiv 3 \pmod 5 \end{cases}$$

[Soluzione. $\Delta \equiv 0 \pmod 5$ se e soltanto se $\lambda \equiv 1 \pmod 5$.
Se $\lambda = 0$, il sistema ha un'unica soluzione: $(3,4)$.
Se $\lambda = 2$, il sistema ha un'unica soluzione: $(0,6)$.
Se $\lambda = 3$, il sistema ha un'unica soluzione: $(2,3)$.
Se $\lambda = 4$, il sistema ha un'unica soluzione: $(1,2)$.
Se $\lambda = 1$ il sistema non è risolubile.]

2.18. Trovare, al variare tra gli interi del parametro λ, le soluzioni del seguente sistema di congruenze lineari:

$$\begin{cases} 2X + Y & \equiv \lambda \pmod 3 \\ X + 2Y & \equiv 1 \pmod 3 \end{cases}$$

[Soluzione. $\Delta \equiv 0 \pmod 3, \alpha_\lambda := de - bf = 2\lambda - 1, \beta_\lambda := af - ce = 2 - \lambda$.
Se $\lambda = 2, \alpha_\lambda \equiv 0 \pmod 3, \beta_\lambda \equiv 0 \pmod 3$. In tal caso, il sistema ha come soluzioni $(1,0),(0,2),(2,1)$.
Se $\lambda = 0$ o se $\lambda = 1$, il sistema non ha soluzioni.]

2.19. Siano $A = (a_{ij}), B = (b_{ij})$ due matrici $r \times s$ ad entrate, a_{ij} e b_{ij}, intere e sia $n > 0$. Si dice che $A \equiv B \pmod n$, se $a_{ij} \equiv b_{ij} \pmod n$ presi comunque $1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant s$.

Si dice che una *matrice quadrata A, ad entrate intere è invertibile* (mod n) se esiste una matrice $\widetilde{A}$ tale che $A\widetilde{A} \equiv I \equiv \widetilde{A}A \pmod{n}$ dove I è la matrice identità.
(a) Mostrare che se C è una matrice $s \times t$ ad entrate intere e se $A \equiv B \pmod{n}$ allora $AC \equiv BC \pmod{n}$.
(b) Sia A una matrice quadrata ad entrate intere, sia A^{agg} la sua aggiunta e sia $\Delta := det(A)$. Mostrare che se $\text{MCD}(\Delta, n) = 1$, allora un'inversa della matrice A (mod n) è data da $\widetilde{A} = \Delta^* A^{agg}$, dove Δ^* è un inverso aritmetico (mod n) di Δ.
(c) Si consideri un sistema di congruenze lineari in r equazioni ed r incognite:

$$\begin{cases} \sum_{j=1}^{r} a_{ij} X_j \equiv b_i \pmod{n} \\ 1 \leqslant i \leqslant r \end{cases}$$

che scriviamo in forma compatta matriciale nella seguente maniera:

$$AX \equiv B \pmod{n}$$

dove $A = (a_{ij})$ è una matrice $r \times r$, $X = (X_j)$ e $B = (b_j)$ sono due matrici $r \times 1$. Mostrare che, se $\text{MCD}(det(A), n) = 1$, allora il sistema ammette un'unica soluzione $x = (x_j) \pmod{n}$ che può essere espressa nella maniera seguente:

$$x \equiv det(A)^* A^{agg} B \pmod{n}$$

dove $det(A)^*$ è un inverso aritmetico di $det(A) \pmod{n}$.

3 Il "piccolo" Teorema di Fermat

Pierre de Fermat, francese, giudice presso il tribunale di Tolosa, è considerato certamente uno dei padri fondatori della moderna teoria dei numeri. L'interesse per questa teoria fu suscitato in lui dalla lettura della traduzione (commentata) in latino dell'*Arithmetica* di Diofanto di Alessandria (matematico greco vissuto nel III secolo d. C.), pubblicata nel 1621 a cura di C. Bachet de Méziriac.
Una delle caratteristiche dell'attività matematica di Fermat fu quella di non scrivere esplicitamente le dimostrazioni dei suoi risultati. Egli si limitava di solito a semplici annotazioni (celebri sono quelle a margine della copia dell'*Arithmetica* di Diofanto) e le diffondeva attraverso una fitta corrispondenza che aveva stabilito con vari altri cultori della matematica suoi contemporanei (tra i quali principalmente il religioso M. Mersenne).
Nel 1640, ad esempio, Fermat comunicò a B. Frénicle de Bessy che se p è un numero primo ed a un qualunque intero non divisibile per p, allora $a^{p-1}-1$ è divisibile per p. La prima dimostrazione completa di tale risultato fu pubblicata nel 1736, quasi cento anni più tardi, da Euler.

Teorema 3.1. *(**"Piccolo" Teorema di Fermat**) Sia p un numero primo ed $a \in \mathbb{Z}$. Se $p \nmid a$, allora $a^{p-1} \equiv 1 \pmod{p}$.*

Dimostrazione (Ivory, 1806)**.** Poiché $p \nmid a$, $S = \{0, a, 2a, \ldots, (p-1)a\}$ è un sistema completo di residui (modulo p) (cfr. anche Esercizio 1.4). Quindi, dalla Proposizione 1.3(5) si ricava che:

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p},$$

ovvero

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Poiché $p \nmid (p-1)!$, necessariamente $p \mid (a^{p-1}-1)$ e da ciò segue la tesi. □

Corollario 3.2. *Sia p un numero primo. Per ogni $a \in \mathbb{Z}$ si ha:*

$$a^p \equiv a \pmod{p}. \qquad \square$$

Il "Piccolo" Teorema di Fermat non si inverte, in generale:
se un intero n ($n \geqslant 2$) è tale che $a^{n-1} \equiv 1 \pmod{n}$, per qualche $a \in \mathbb{Z}$ e $\mathrm{MCD}(a, n) = 1$, allora n *non* è necessariamente primo. Proveremo questo fatto con un controesempio, cui premettiamo il seguente lemma tecnico.

Lemma 3.3. *Siano p e q due numeri primi distinti ed $a \in \mathbb{Z}$ in modo tale che:*

$$a^q \equiv a \pmod{p} \quad e \quad a^p \equiv a \pmod{q}.$$

Allora:

$$a^{pq} \equiv a \pmod{pq}.$$

Dimostrazione. Applicando il Corollario 3.2 ad a^q, si ha che $(a^q)^p \equiv a^q \pmod{p}$ e dunque $a^{pq} \equiv a \pmod{p}$. In modo analogo si ottiene che $a^{pq} \equiv a \pmod{q}$. Essendo ovviamente $\mathrm{MCD}(p, q) = 1$, la tesi segue facilmente (cfr. Esercizio 1.2). $\square$

Veniamo al controesempio annunciato. Sia $n = 341 = 11 \cdot 31$ ed $a = 2$. Mostriamo che $2^{340} \equiv 1 \pmod{341}$ pur non essendo 341 un numero primo. È facile vedere che $2^{11} \equiv 2 \pmod{31}$ (infatti $2^{11} = 2 \cdot 2^{10} = 2 \cdot 1024 = 2(31 \cdot 33 + 1)$) e che $2^{31} \equiv 2 \pmod{11}$ (infatti $2^{31} = 2 \cdot (2^{10})^3 \equiv 2 \cdot 1^3 \pmod{11}$). Perciò, utilizzando il Lemma 3.3, $2^{341} = 2^{11 \cdot 31} \equiv 2 \pmod{341}$, da cui $2^{340} \equiv 1 \pmod{341}$, mentre 341 non è primo.

Osservazione 3.4. L'esempio precedente ci porta a considerare numeri naturali del tipo $2^n - 2$, i quali hanno un notevole interesse storico, testimoniato dal fatto che si attribuisce (anche se in maniera controversa) agli antichi matematici cinesi dell'epoca di Confucio (VI - V secolo a. C.) la seguente congettura:

$$\text{un intero } n \text{ è primo} \iff n \mid (2^n - 2).$$

Per maggiori dettagli storici su tale congettura rinviamo a [R, pag. 85]. Tale congettura è vera per $n \leqslant 340$, ma l'esempio precedente (che è dovuto a Sarrus e risale al 1819) mostra che, in generale, la congettura è falsa. Ciò ha portato alla seguente definizione:

Definizione 3.5. Si chiama *numero pseudoprimo (in base* 2) ogni intero non primo n tale che $n \mid (2^n - 2)$.

Si noti che, se n è dispari, allora:

$$n \text{ è pseudoprimo (in base 2)} \iff 2^{n-1} \equiv 1 \pmod{n}.$$

I numeri pseudoprimi $n < 10^3$ sono $341, 561 = 3 \cdot 11 \cdot 17$ e $645 = 3 \cdot 5 \cdot 43$. Il più piccolo numero pseudoprimo pari è $2 \cdot 73 \cdot 1103 = 161038$ ed è stato scoperto da Lehmer nel 1950. Nel 1938 Poulet ha determinato tutti i numeri pseudoprimi dispari $\leqslant 10^8$. Si può inoltre dimostrare che i numeri pseudoprimi sono infiniti (cfr. Esercizio 3.15) ed anzi, di più, Beeger nel 1951 ha dimostrato che i numeri pseudoprimi pari sono infiniti.

La nozione di numero pseudoprimo può essere "rafforzata" nella maniera seguente, determinando un "tipo più raro" di numeri.

Definizione 3.6. Si chiama *numero di Carmichael* ogni intero non primo n tale che, per ogni intero a, relativamente primo con n, risulti:

$$a^{n-1} \equiv 1 \pmod{n}.$$

Si può dimostrare facilmente che un intero non primo n è di Carmichael se, e soltanto se, per ogni $a \in \mathbb{Z}$ risulta che $n \mid (a^n - a)$. Dunque ogni numero di Carmichael è pseudoprimo. Il viceversa è falso, in quanto, ad esempio 341 non è un numero di Carmichael (infatti si vede che $31 \nmid (11^{341} - 11)$ e dunque $341 \nmid (11^{341} - 11)$). Si dimostra invece che 561 è un numero di Carmichael (dunque è il più piccolo numero di Carmichael. Il successivo numero di Carmichael è $1105 = 5 \cdot 13 \cdot 17$). Nel 1993 Alford, Granville e Pomerance hanno dimostrato che esistono infiniti numeri di Carmichael.

Nel 1760, 24 anni dopo la dimostrazione del "Piccolo" Teorema di Fermat, Euler dimostrò la seguente generalizzazione di tale teorema:

Teorema 3.7. *(**Teorema di Euler - Fermat**) Siano $a, n \in \mathbb{Z}, n > 0$. Se $MCD(a, n) = 1$, allora:*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dimostrazione. Sia $S^* := \{k_1, \ldots, k_{\varphi(n)}\}$ un sistema ridotto di residui (modulo n) (cfr. Definizione 2.7). Poiché $\mathrm{MCD}(a, n) = 1$, anche $T^* := \{ak_1, \ldots, ak_{\varphi(n)}\}$ è un sistema ridotto di residui (modulo n) (cfr. Esercizio 2.10 (a)) e quindi:

$$a^{\varphi(n)} \cdot k_1 \ldots k_{\varphi(n)} = ak_1 \cdots ak_{\varphi(n)} \equiv k_1 \cdots k_{\varphi(n)} \pmod{n}.$$

Poiché $\mathrm{MCD}(k_1 \cdot k_2 \cdots k_{\varphi(n)}, n) = 1$, dal Corollario 1.11 (a) segue la tesi. □

Osservazione 3.8. **(a)** Il Teorema 3.7 generalizza il Teorema 3.1, in quanto, per ogni primo p, si ha $\varphi(p) = p - 1$.
(b) Si noti che, in generale, $a^{\varphi(n)} \not\equiv 1 \pmod{n}$ (ad esempio, $n = 4, a = 2$, allora $2^2 \not\equiv 1 \pmod{4}$) e quindi anche $a^{\varphi(n)+1} \not\equiv a \pmod{n}$.

Passiamo ora a dare alcune applicazioni (conseguenze o risultati collegati) del Teorema di Euler - Fermat e della nozione di inverso aritmetico.

I APPLICAZIONE: Formula risolutiva delle congruenze lineari.
Tutte e sole le soluzioni distinte della congruenza

$$aX \equiv b \pmod{n}$$

con $n > 0$ e $MCD(a, n) =: d \mid b$, sono date da:

$$x_k := \left(\frac{a}{d}\right)^{\varphi\left(\frac{n}{d}\right)-1} \cdot \left(\frac{b}{d}\right) + k\left(\frac{n}{d}\right), \quad 0 \leqslant k \leqslant d - 1.$$

Dimostrazione. Basta applicare il Teorema 2.2 ed il Teorema 3.7. □

II APPLICAZIONE: Teorema di Wilson.
Sia p un numero primo. Allora:

$$(p-1)! \equiv -1 \pmod{p}.$$

Dimostrazione. Se $p = 2, 3$ il risultato è ovvio.
Supponiamo dunque che $p \geqslant 5$ e consideriamo il sistema ridotto di residui (modulo p) $S^* := \{1, 2, \ldots, p-1\}$. Gli elementi a di S^* coincidenti con l'inverso aritmetico (cfr. Definizione 1.13) sono esattamente 1 e $p-1$. Infatti

$$a^2 \equiv 1 \pmod{p} \iff (a-1)(a+1) \equiv 0 \pmod{p} \iff$$

$$\iff a \equiv 1 \pmod{p} \text{ oppure } a \equiv -1 \equiv p-1 \pmod{p} \iff$$

$$\iff a = 1 \text{ oppure } a = p-1.$$

I restanti elementi $2, 3, \ldots, p-2$ non coincidono con il loro inverso aritmetico in S^* e, dunque, possono essere ripartiti in paia $\{a, a'\}, a \neq a'$, tali che $aa' \equiv 1 \pmod{p}$. Si ottiene allora:

$$(p-2)! = 2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$$

e, moltiplicando ambo i membri per $p-1$:

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}. \qquad \square$$

Osservazione 3.9. (a) Il Teorema di Wilson fu enunciato nel 1770 da E. Waring sul suo *Meditationes Algebricae* e da Waring attribuito ad un suo studente, appunto J. Wilson. La prima dimostrazione completa di tale risultato viene generalmente attribuita a Lagrange nel 1771.
(b) Il Teorema di Wilson si inverte, infatti:

$$n \text{ è primo} \iff (n-1)! \equiv -1 \pmod{n}.$$

($\Leftarrow$) Se $d \mid n$ e $d \neq n$, allora $d \mid (n-1)!$. Poiché, per ipotesi, $n \mid (n-1)! + 1$, allora $d \mid (n-1)! + 1$, ma $d \mid (n-1)!$ e pertanto $d = 1$.

La problematica connessa con il teorema successivo è molto antica, infatti se ne trovano tracce in un manuale di aritmetica di Sun Tsu (matematico cinese del I secolo d.C.).

III APPLICAZIONE: Teorema Cinese dei Resti.
Siano $n_1, n_2, \ldots, n_r$ interi positivi tali che $MCD(n_i, n_j) = 1$ con $1 \leqslant i, j \leqslant r$ e $i \neq j$. Per ogni scelta di $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ il sistema di congruenze lineari:

$$\begin{cases} X \equiv a_i \pmod{n_i} \\ 1 \leqslant i \leqslant r \end{cases}$$

è risolubile ed ha un'unica soluzione modulo $n_1 \cdot n_2 \cdots n_r$.

Dimostrazione. Sia $n := n_1 \cdot n_2 \cdots n_r$ ed $N_i := \dfrac{n}{n_i}$ $(1 \leqslant i \leqslant r)$. Verifichiamo che l'intero:

$$x_0 := \sum_{i=1}^{r} a_i N_i^{\varphi(n_i)} \tag{1}$$

è soluzione del sistema assegnato. Infatti, per ogni indice $j \neq i$ risulta $N_j \equiv 0 \pmod{n_i}$ e dunque $x_0 \equiv a_i N_i^{\varphi(n_i)} \pmod{n_i}$.
Poiché $\mathrm{MCD}(N_i, n_i) = 1$, il Teorema di Euler-Fermat ci assicura che:
$N_i^{\varphi(n_i)} \equiv 1 \pmod{n_i}$; da ciò segue che x_0 è soluzione del sistema.
Se $x' \in \mathbb{Z}$ è un'altra soluzione del sistema dato, risulta $x' \equiv x_0 \pmod{n_i}$. Poiché $\mathrm{MCD}(n_i, n_j) = 1$, in base all'Esercizio 1.2 (esteso per induzione al caso di r fattori relativamente primi a coppie), si ha $x_0 \equiv x' \pmod{n}$ e, quindi, la soluzione del sistema è unica (modulo n). $\square$

Si noti che la formula (1), che determina la soluzione (modulo n) del sistema di congruenze sopra considerato, può essere sostituita dalla formula:

$$x_0' := \sum_{i=1}^{r} a_i M_i \tag{1'}$$

dove $M_i := N_i N_i^*$, con N_i^* un inverso aritmetico di $N_i \pmod{n_i}$ per ogni i, $1 \leqslant i \leqslant r$. Ciò è conveniente dal punto di vista computazionale se risulta più semplice determinare esplicitamente N_i^* (possibilmente $N_i^* < N_i^{\varphi(n_i)-1}$, senza far ricorso al Teorema di Euler-Fermat.

IV APPLICAZIONE: Risoluzione di un sistema di congruenze lineari.
Si consideri il sistema di congruenze lineari:

$$\begin{cases} a_i X \equiv b_i \pmod{m_i} \\ 1 \leqslant i \leqslant r \end{cases} \tag{2}$$

con $MCD(m_i, m_j) = 1$ *se* $i \neq j$. *Si ponga* $d_i :=MCD(a_i, m_i), a_i' := \dfrac{a_i}{d_i}$, $b_i' := \dfrac{b_i}{d_i}$ *ed* $n_i := \dfrac{m_i}{d_i}$ $(1 \leqslant i \leqslant r)$. *Se* $d_i \mid b_i$ *per ogni* i $(1 \leqslant i \leqslant r)$, *il sistema* (2) *è risolubile e l'insieme delle soluzioni (in* $\mathbb{Z}$*) coincide con l'insieme delle soluzioni (in* $\mathbb{Z}$*) del sistema:*

$$\begin{cases} X \equiv (a_i')^{\varphi(n_i)-1} b_i' \pmod{n_i} \\ 1 \leqslant i \leqslant r \end{cases} \tag{$2^{\#}$}$$

con $MCD(n_i, n_j) = 1$ *se* $i \neq j$.
Precisamente, se $m := m_1 \cdots m_r, d := d_1 \cdots d_r, n := n_1 \cdots n_r$ *e se* $\mathring{x}$ *è l'unica soluzione di* $(2^{\#})$ *(modulo* n*), allora* $\mathring{x}$ *determina* d *soluzioni di* (2)

incongruenti (modulo m) che sono tutte le soluzioni di (2)*:*

$$x_k := \mathring{x} + kn, \quad 0 \leqslant k \leqslant d-1.$$

L'insieme delle soluzioni in $\mathbb{Z}$ *di* $(2^{\#})$*, dato da* $\{\mathring{x} + tn : t \in \mathbb{Z}\}$*, coincide con l'insieme delle soluzioni in* $\mathbb{Z}$ *di* (2)*, dato da* $\{\mathring{x} + kn + sm : 0 \leqslant k \leqslant d-1,\ s \in \mathbb{Z}\}$*.*

Dimostrazione. È chiaro che $\mathrm{MCD}(n_i, n_j) = 1$ se $i \neq j$: dunque $(2^{\#})$ è risolubile. Poiché $\mathrm{MCD}(a_i', n_i) = 1$, per determinare le soluzioni del sistema $(2^{\#})$ (modulo n) basta applicare la formula risolutiva delle congruenze lineari (I Applicazione del Teorema di Euler-Fermat).
Se $\mathring{x}$ è una soluzione di $(2^{\#})$ (modulo n), allora non è difficile verificare che $\mathring{x}$ determina le seguenti d soluzioni del sistema (2), incongruenti (modulo m):

$$x_k := \mathring{x} + kn, \quad 0 \leqslant k \leqslant d-1.$$

Infatti, per ogni i, $1 \leqslant i \leqslant r$

$$a_i'(\mathring{x} + kn) \equiv b_i' \pmod{n_i}$$

e quindi, moltiplicando per d_i ambo i membri, abbiamo che:

$$a_i(\mathring{x} + kn) \equiv b_i \pmod{m_i}.$$

Il fatto che le x_k siano tutte le soluzioni incongrue (mod m) di (2) discende dal fatto che, se x è una soluzione di (2), allora x è anche una soluzione di $(2^{\#})$ e, quindi, $x \equiv \mathring{x} \pmod{n}$. □

Esempio 3.10. Si consideri il seguente sistema:

$$\begin{cases} 2X \equiv 2 \pmod 4 \\ 2X \equiv 3 \pmod 5 \\ 14X \equiv 7 \pmod{21} \end{cases} \tag{3.10.1}$$

Tenendo presente che l'inverso aritmetico di 2 (mod 5) è 3 e l'inverso aritmetico di 2 (mod 3) è 2, al sistema (3.10.1) è associato il seguente sistema:

$$\begin{cases} X \equiv 1 \pmod 2 \\ X \equiv 4 \pmod 5 \\ X \equiv 2 \pmod 3 \end{cases} \tag{3.10.2}$$

Il sistema (3.10.2) ha un'unica soluzione $\mathring{x} = 1 \cdot 15 + 4 \cdot 6^4 + 2 \cdot 10^2 \equiv -1$ (mod 30). Questa determina 14 soluzioni di (3.10.1) (modulo 420) date da:

$$x_k = -1 + k30, \quad 0 \leqslant k \leqslant 13.$$

V APPLICAZIONE: *Sia p un primo dispari. La congruenza:*

$$X^2 \equiv -1 \pmod{p}$$

è risolubile se, e soltanto se, $p \equiv 1 \pmod 4$. In tal caso $\mathring{x} := \left(\frac{(p-1)}{2}\right)!$ è una soluzione della congruenza data.

Dimostrazione. (⇒). Sia $\mathring{x} \in \mathbb{Z}$ tale che $\mathring{x}^2 \equiv -1 \pmod p$. Allora $\mathring{x}^{p-1} = (\mathring{x}^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod p$ e, in base al "Piccolo" Teorema di Fermat (Teorema 3.1), $\mathring{x}^{p-1} \equiv 1 \pmod p$, quindi $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$. Essendo $p \neq 2$, si ha che $1 = (-1)^{\frac{p-1}{2}}$ e pertanto $\frac{p-1}{2}$ è pari, cioè $p \equiv 1 \pmod 4$.
(⇐). Sia $p \equiv 1 \pmod 4$. Dopo aver osservato che:

$$\{h : \frac{p-1}{2} + 1 \leqslant h \leqslant p-1\} = \{p-k : 1 \leqslant k \leqslant \frac{p-1}{2}\},$$

si vede subito che:

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2} \cdot (p-1)(p-2) \cdot \dots \cdot \left[p - \left(\frac{p-1}{2}\right)\right] \\ &\equiv 1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2} \cdot (-1)(-2) \cdot \dots \cdot \left[-\left(\frac{p-1}{2}\right)\right] \pmod p \\ &= (-1)^{\frac{p-1}{2}} \cdot 1^2 \cdot 2^2 \cdot \dots \cdot \left(\frac{p-1}{2}\right)^2 \\ &= (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2\end{aligned}$$

Per ipotesi $\frac{p-1}{2}$ è pari e, dal Teorema di Wilson, si ricava:

$$-1 \equiv (p-1)! \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p.$$

Pertanto $\mathring{x} = (\frac{p-1}{2})!$ è soluzione della congruenza in esame. □

VI APPLICAZIONE: *Sia n un intero tale che $MCD(n, 10) = 1$. Allora n divide un intero le cui cifre sono tutte uguali ad 1.*

Dimostrazione. Dato che $\mathrm{MCD}(9, 10) = 1$, anche $\mathrm{MCD}(9n, 10) = 1$. Dal Teorema di Euler-Fermat, $10^{\varphi(9n)} \equiv 1 \pmod{9n}$, cioè esiste $k \in \mathbb{Z}$ tale che $9nk = 10^{\varphi(9n)} - 1$. Dunque $nk = (10^{\varphi(9n)} - 1)/9$ donde la conclusione. □

La dimostrazione del risultato precedente non determina un intero "minimale" con la proprietà enunciata. Infatti, se $n = 3$, allora per quanto sopra abbiamo:

$$3 \mid \left(\frac{10^{\varphi(27)} - 1}{9}\right) = \frac{10^{18} - 1}{9},$$

tuttavia è facile vedere anche che $3 \mid 111$.

VII APPLICAZIONE: *Siano* $n, a \in \mathbb{Z}$, $n > 0$ *tali che* $MCD(a, n) = MCD(a-1, n) = 1$. *Allora:*

$$1 + a + a^2 + \cdots + a^{\varphi(n)-1} \equiv 0 \pmod{n}.$$

Dimostrazione. Si noti che:

$$a^{\varphi(n)} - 1 = (a-1)(a^{\varphi(n)-1} + \cdots + a^2 + a + 1).$$

Dal Teorema di Euler-Fermat, $(a-1)(a^{\varphi(n)-1}+\cdots+a^2+a+1) \equiv 0 \pmod{n}$ e, poiché $\mathrm{MCD}(a-1, n) = 1$, è lecito "semplificare" $(a-1)$ dalla precedente congruenza: da cui la tesi. □

Si noti che, nella precedente applicazione, la condizione che $\mathrm{MCD}(a-1, n)$ sia uguale ad 1 è essenziale, perché ad esempio se $n = 4$ ed $a = 5$, allora $\varphi(n) = 2$ e $1 + 5 \not\equiv 0 \pmod{4}$.

Come mostrano le applicazioni del Teorema di Euler-Fermat e, come vedremo meglio nello sviluppo della teoria delle congruenze, sovente è necessario calcolare grandi potenze di interi modulo un intero n fissato. È pertanto opportuno disporre di una tecnica per il calcolo della esponenziazione modulare.

Ad esempio, se vogliamo trovare il più piccolo intero positivo congruo a $3^{10} \pmod{11}$, possiamo procedere nella maniera seguente.

1° Passo. Esprimere l'esponente 10 in base 2:

$$10 = (1010)_2$$

2° Passo. Utilizzando il passo precedente, scrivere 3^{10} come prodotto di potenze di 3, con esponenti potenze di 2, fino alla piú grande potenza di 2 minore di 10:

$$3^{10} = 3^{2^3+2} = 3^8 \cdot 3^2$$

3° Passo. Calcolare il più piccolo intero positivo congruo a $3^{2^k} \pmod{11}$ per $k \leqslant 3$:

$$\begin{aligned} 3 &\equiv 3 && \pmod{11} \\ 3^2 &\equiv 9 && \pmod{11} \\ 3^4 &\equiv 81 \equiv 4 && \pmod{11} \\ 3^8 &\equiv 16 \equiv 5 && \pmod{11} \end{aligned}$$

Quindi, possiamo concludere facilmente che

$$3^{10} \equiv 5 \cdot 9 \equiv 1 \pmod{11}.$$

Metodo di calcolo per l'esponenziazione modulare.
Siano dati b, N ed n interi positivi. Per calcolare il più piccolo intero positivo congruo a $b^N \pmod{n}$, si può procedere nella seguente maniera:

1° Passo. Esprimere l'esponente N in base 2:

$$N = (a_k a_{k-1} \dots a_1 a_0)_2 \text{ con } a_i \in \{0, 1\}, 0 \leqslant i \leqslant k.$$

2° Passo. Scrivere b^N come prodotto di potenze del tipo b^{2^h} per $0 \leqslant h \leqslant k$:

$$b^N = b^{a_k 2^k + a_{k-1} 2^{k-1} + \dots + a_0 2^0} = \prod_{h=0}^{k} b^{a_h 2^h} = \prod_{\substack{a_h \neq 0 \\ h=0}}^{k} b^{2^h}.$$

3° Passo. Calcolare il più piccolo intero positivo congruo a b^{2^h} (modulo n) per ogni h, $0 \leqslant h \leqslant k$:

$$b^{2^h} \equiv r_h \pmod{n}, \text{ con } 0 \leqslant r_h \leqslant n-1, \ 0 \leqslant h \leqslant k.$$

Conclusione.

$$b^N \equiv \prod_{a_h \neq 0} r_h \equiv r \pmod{n}, \text{ con } 0 \leqslant r \leqslant n-1.$$

Esempio 3.11. Per calcolare il più piccolo intero positivo congruo a $2^{138} \pmod{23}$, scriviamo:

$$138 = (10001010)_2 = 2^7 + 2^3 + 2.$$

Poiché:

$$2^2 \equiv 8 \pmod{23} \qquad 2^{2^3} = 2^8 \equiv 3 \pmod{23}$$
$$2^{2^4} \equiv 9 \pmod{23} \qquad 2^{2^5} \equiv 81 \equiv 12 \pmod{23}$$
$$2^{2^6} \equiv 144 \equiv 6 \pmod{23} \qquad 2^{2^7} \equiv 13 \pmod{23},$$

dunque:

$$2^{138} = 2^{2^7} \cdot 2^{2^3} \cdot 2^2 \equiv 13 \cdot 3 \cdot 4 \equiv 18 \pmod{23}.$$

3. Esercizi e Complementi

3.1. Siano p e q due primi distinti. Provare che, per ogni $a \in \mathbb{Z}$:

$$pq \mid (a^{pq} - a^p - a^q + a).$$

[Suggerimento: risulta $a^{pq} - a^p \equiv 0 \equiv a^q - a \pmod{q}$ e $a^{pq} - a^q \equiv 0 \equiv a^p - a \pmod{p}$, cfr. Corollario 3.2.]

3.2. (a) Siano p e q due primi distinti. Provare che:

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

(b) Siano n ed m due interi positivi distinti e relativamente primi. Provare che:

$$n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{mn}.$$

[Suggerimento: basta provare **(b)**.
Risulta $n^{\varphi(m)} - 1 \equiv 0 \pmod{m}$ e $m^{\varphi(n)} - 1 \equiv 0 \pmod{n}$ (cfr. Teorema 3.7). Moltiplicando le due congruenze tra loro, segue l'asserto.]

3.3. Sia $n \geqslant 2$. Mostrare che:
(a) $\{k \in \mathbb{Z} : \text{ MCD}(k,n) = 1,\ 1 \leqslant k \leqslant n\} = \{n - k : k \in \mathbb{Z},\ \text{MCD}(k,n) = 1,\ 1 \leqslant k \leqslant n\}$.
(b) Se $\{k_1, k_2, \ldots, k_{\varphi(n)}\}$ è il sistema ridotto di residui minimo positivo (modulo n), allora:

$$2(k_1 + k_2 + \cdots + k_{\varphi(n)}) = n\varphi(n).$$

[Suggerimento: **(b)** discende da **(a)** in quanto:

$$\sum_{i=1}^{\varphi(n)} k_i = \sum_{i=1}^{\varphi(n)} (n - k_i).]$$

3.4. Utilizzando il "Piccolo" Teorema di Fermat (cfr. Teorema 3.1 o, meglio, Corollario 3.2), mostrare che se p è primo e $a, b \in \mathbb{Z}$, allora:

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

3.5. Mostrare che le seguenti affermazioni sono equivalenti:
(i) affermazioni contenute nel "Piccolo" Teorema di Fermat e nel Teorema di Wilson;
(ii) per ogni primo p e per ogni $a \in \mathbb{Z}$, allora:

$$p \mid (a^p + (p-1)!a);$$

(iii) per ogni primo p e per ogni $a \in \mathbb{Z}$, allora:

$$p \mid ((p-1)!a^p + a).$$

[Suggerimento: **(i)** $\Rightarrow$ **(ii)** [rispettivamente **(i)** $\Rightarrow$ **(iii)**]. Si moltiplichi la congruenza $a^p \equiv a \pmod{p}$ per la congruenza $-1 \equiv (p-1)! \pmod{p}$ [rispettivamente $(p-1)! \equiv -1 \pmod{p}$]. **(ii)** [oppure **(iii)**]$\Rightarrow$ **(i)**. Posto $a = 1$, si ottiene $(p-1)! \equiv -1 \pmod{p}$. Dall'ipotesi, avendo dimostrato che $(p-1)! \equiv -1 \pmod{p}$, si ottiene allora che $a^p \equiv a \pmod{p}$.]

3.6. Siano $n_1, \ldots, n_r$ interi positivi a due a due relativamente primi. Posto $n := \prod_{i=1}^{n} n_i$, verificare che l'applicazione canonica tra anelli:

$$\varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z}),$$

definita da $\varphi(a + n\mathbb{Z}) := (a + n_1\mathbb{Z}, \ldots, a + n_r\mathbb{Z})$, è un isomorfismo di anelli.
[Suggerimento: se $a + n\mathbb{Z} \in Ker(\varphi)$, allora $a \in \cap n_i\mathbb{Z} = n\mathbb{Z}$. La suriettività di φ è un'immediata conseguenza del Teorema Cinese dei Resti.]

3.7. Dimostrare che il seguente sistema di congruenze lineari:

$$\begin{cases} X \equiv a_i \pmod{n_i} \\ 1 \leqslant i \leqslant r \end{cases}$$

con $a_i, n_i, r \in \mathbb{Z},\ r, n_i \geqslant 2$, è risolubile se, e soltanto se, $\mathrm{MCD}(n_i, n_j) \mid (a_i - a_j)$, presi comunque $i \neq j, 1 \leqslant i, j \leqslant r$. Nel caso in cui tale sistema sia risolubile, dimostrare che esso ammette un'unica soluzione (modulo $\mathrm{mcm}(n_1, n_2, \ldots, n_r)$).
[Suggerimento: si proceda per induzione su $r \geqslant 2$. Sia $r = 2$ e sia $x = a_1 + kn_1$ una soluzione della prima congruenza del sistema, per un qualche $k \in \mathbb{Z}$. Affinché x sia anche soluzione della seconda congruenza del sistema deve essere $x = a_2 + hn_2$, per un qualche $h \in \mathbb{Z}$. Dunque $a_1 - a_2 = hn_2 - kn_1$. Viceversa, se $d := \mathrm{MCD}(n_1, n_2)$, allora esistono $\alpha, \beta \in \mathbb{Z}$ in modo tale che $d = \alpha n_1 + \beta n_2$. Inoltre, per ipotesi deve esistere $t \in \mathbb{Z}$ in modo tale che $td = a_1 - a_2$, quindi $\mathring{x} := a_1 - t\alpha n_1 = a_2 + t\beta n_2$ è soluzione del sistema. Se y è un'altra soluzione del sistema e se

$$n_1' := \frac{n_1}{\mathrm{MCD}(n_1, n_2)}, \quad n_2' := \frac{n_2}{\mathrm{MCD}(n_1, n_2)},$$

allora in particolare $n_1' \mid (y - \mathring{x})$ e $n_2' \mid (y - \mathring{x})$. Essendo $\mathrm{MCD}(n_1', n_2') = 1$, allora $n_1' \cdot n_2' \mid (y - \mathring{x})$.]

3.8. Sia $p \geqslant 5$ un primo dispari, allora mostrare che:

$$2(p-3)! \equiv -1 \pmod{p}.$$

[Suggerimento: per il Teorema di Wilson:
$-1 \equiv (p-1)! = (p-3)!(p-2)(p-1) \equiv (p-3)! \cdot 2 \pmod{p}$.]

3.9. Per ogni $n \geqslant 2$ e per ogni $a \in \mathbb{Z}$ con $\mathrm{MCD}(a, n) = 1$, mostrare che:

$$a^n \equiv a^{n-\varphi(n)} \pmod{n}.$$

[Suggerimento: semplice conseguenza del Teorema di Euler-Fermat; notare che $n > \varphi(n)$ se $n \geqslant 2$ e moltiplicare ambo i membri per $a^{n-\varphi(n)}$.]

3.10. Risolvere le seguenti congruenze utilizzando il Teorema di Euler-Fermat:

(a) $7X \equiv 12 \pmod{17}$;
(b) $3X \equiv 5 \pmod{16}$.

[Soluzioni: **(a)** $x \equiv 9 \pmod{17}$; **(b)** $x \equiv 7 \pmod{16}$.]

3.11. Risolvere il seguente sistema di congruenze:

$$\begin{cases} X \equiv 2 \pmod 3 \\ X \equiv 3 \pmod 5 \\ X \equiv 2 \pmod 7 \end{cases}$$

[Suggerimento: $n = 3 \cdot 5 \cdot 7 = 105, N_1 = \dfrac{n}{n_1} = 35, N_2 = \dfrac{n}{n_2} = 21, N_3 = \dfrac{n}{n_3} = 15$. La soluzione (modulo 105) è data da: $\mathring{x} = 2 \cdot 35^2 + 3 \cdot 21^4 + 2 \cdot 15^6 \equiv 23 \pmod{105}$.]

3.12. Se $n > 2$ mostrare che:
(a) $\varphi(n)$ è pari;
(b) se $\{k_1, \ldots, k_{\varphi(n)}\}$ è un sistema ridotto di residui (modulo n), allora:

$$k_1 + \cdots + k_{\varphi(n)} \equiv 0 \pmod n.$$

[Suggerimento: **(a)** se $n = 2^k \cdot m$ con $k \geqslant 2$ e $2 \nmid m$, allora $\varphi(n) = \varphi(2^k)\varphi(m) = (2^k - 2^{k-1})\varphi(m)$. Se $n = p^k \cdot m$ con $k \geqslant 1$ e p primo dispari e $p \nmid m$, allora $\varphi(n) = \varphi(p^k)\varphi(m) = (p^k - p^{k-1})\varphi(m) = p^{k-1}(p-1)\varphi(m)$. **(b)** segue da **(a)** e dall'Esercizio 3.3(b).]

3.13. Mostrare che 63 non è primo, verificando che $2^{63} \not\equiv 2 \pmod{63}$.
[Suggerimento: $63 = 6 \cdot 10 + 3$, $2^{63} = (2^6)^{10} \cdot 2^3 = 64^{10} \cdot 2^3 \equiv 1^{10} \cdot 2^3 = 8 \pmod{63}$.]

3.14. Mostrare che $91 \mid (3^{91} - 3)$, pur essendo 91 un numero non primo.
[Suggerimento: $91 = 7 \cdot 13 = (1011011)_2 = 2^6 + 2^4 + 2^3 + 2^1 + 2^0$, $3^{91} = 3^{(2^6)} \cdot 3^{(2^4)} \cdot 3^{(2^3)} \cdot 3^2 \cdot 3$, con $3^2 \equiv 9 \pmod{91}$ $3^{(2^3)} \equiv (3^{(2^2)})^2 = 81^2 \equiv 9 \pmod{91}$, $3^{(2^4)} \equiv 81 \pmod{91}$, $3^{(2^5)} \equiv 9 \pmod{91}$, $3^{(2^6)} \equiv 81 \pmod{91}$, dunque $3^{91} \equiv 81 \cdot 81 \cdot 9 \cdot 9 \cdot 3 \equiv 9 \cdot 9 \cdot 9 \cdot 3 = 81 \cdot 27 \equiv 3 \pmod{91}$.]

3.15. Mostrare che, se n è un numero pseudoprimo (in base 2) dispari, allora anche $N := 2^n - 1$ è un numero pseudoprimo (in base 2) dispari. Dunque, esistono infiniti numeri pseudoprimi (in base 2) dispari.
[Suggerimento: Sia $n = r \cdot s$ con $2^n - 2 = kn$, con $1 < r, s < n$ e $k \geqslant 1$. L'intero N è composto, in quanto $(2^r - 1) \mid (2^n - 1) = N$; infatti $(2^n - 1) = (2^r - 1)(2^{s(r-1)} + 2^{s(r-2)} + \cdots + 2^s + 1)$. Inoltre,

$$2^{N-1} = 2^{2^n - 2} = 2^{kn}$$

Poiché $N = (2^n - 1) \mid (2^{kn} - 1)$, abbiamo che $N \mid (2^{N-1} - 1)$ cioè $2^{N-1} \equiv 1 \pmod N$.]

4 Generalità sulle congruenze polinomiali, Teorema di Lagrange e Teorema di Chevalley

Sia $f(X)$ un polinomio non nullo a coefficienti interi ed n un intero positivo. Ci occuperemo ora della ricerca delle (eventuali) soluzioni della congruenza polinomiale:

$$f(X) \equiv 0 \pmod{n}. \tag{1}$$

Vale in proposito il seguente risultato:

Teorema 4.1. *Sia $n = p_1^{e_1} \dots p_r^{e_r}$, con p_i primo, $e_i \geqslant 1$ ed $r \geqslant 1$. Le soluzioni della congruenza* (1) *coincidono con le soluzioni del sistema di congruenze:*

$$\begin{cases} f(X) \equiv 0 \pmod{p_i^{e_i}} \\ 1 \leqslant i \leqslant r \end{cases} \tag{2}$$

Dimostrazione. Se $\mathring{x}$ è una soluzione di (1), ovviamente $\mathring{x}$ è anche soluzione di ogni congruenza del sistema (2). Viceversa, se $\mathring{x}$ è soluzione di (2), allora $p_i^{e_i} \mid f(\mathring{x})$ per ogni i, e, poiché $\mathrm{MCD}(p_i^{e_i}, p_j^{e_j}) = 1$ (se $i \neq j$), possiamo concludere che $n = p_1^{e_1} \dots p_r^{e_r} \mid f(\mathring{x})$ (cfr. Esercizio 1.2). $\square$

Osservazione 4.2. Supponiamo che $f(X) \equiv 0 \pmod{p_i^{e_i}}$ ammetta s_i soluzioni distinte y_{ij_i} $(1 \leqslant j_i \leqslant s_i)$. Posto $s = \prod_{i=1}^{r} s_i$, per ogni scelta di i, $1 \leqslant i \leqslant r$, e per ogni scelta di y_{ij_i} con $1 \leqslant j_i \leqslant s_i$ si ottiene un sistema di congruenze lineari del tipo:

$$\begin{cases} X \equiv y_{ij_i} \pmod{p_i^{e_i}} \\ 1 \leqslant i \leqslant r \end{cases}$$

In base al Teorema Cinese dei Resti ed al Teorema 4.1, ciascuno di tali s sistemi fornisce una soluzione alla congruenza (1) ed è evidente che sistemi diversi forniscono soluzioni incongruenti (modulo n); dunque (2) ammette $s = \prod_{i=1}^{r} s_i$ soluzioni distinte.
Dal precedente ragionamento discende che, se denotiamo con $N(f(X), n)$ il numero delle soluzioni della congruenza (1) e se $n = hk$ con $\mathrm{MCD}(h, k) = 1$, allora:

$$N(f(X), n) = N(f(X), h)\, N(f(X), k).$$

Ad esempio le soluzioni della congruenza:

$$X^2 + 3X + 2 \equiv 0 \pmod{6}$$

sono le stesse del sistema di congruenze:

$$\begin{cases} X^2 + 3X + 2 \equiv 0 \pmod{2} \\ X^2 + 3X + 2 \equiv 0 \pmod{3} \end{cases}$$

ovvero:

$$\begin{cases} X^2 + X \equiv 0 \pmod 2 \\ X^2 + 2 \equiv 0 \pmod 3 \end{cases}$$

La prima congruenza del sistema ha soluzioni $\{y_{11} = 0, y_{12} = 1\} \pmod 2$, la seconda congruenza ha soluzioni $\{y_{21} = 1, y_{22} = 2\} \pmod 3$. Le soluzioni dei quattro sistemi seguenti, ottenuti variando $i, 1 \leqslant i \leqslant 2$ e $j, 1 \leqslant j \leqslant 2$,

$$\begin{cases} X \equiv y_{1i} \pmod 2 \\ X \equiv y_{2j} \pmod 3 \end{cases}$$

sono date da $x = 4,\ 1,\ 2,\ 5 \pmod 6$.

Dalle considerazioni precedenti discende anche che il problema della risoluzione di (2) può essere ricondotto allo studio di due problemi.

I PROBLEMA: Determinare le soluzioni di un sistema di congruenze lineari del tipo:

$$\begin{cases} X \equiv a_i \pmod{m_i} \\ 1 \leqslant i \leqslant r \end{cases}$$

con $a_i \in \mathbb{Z}$ e $\mathrm{MCD}(m_i, m_j) = 1$ se $i \neq j$.

II PROBLEMA: Determinare le soluzioni di una congruenza polinomiale del tipo:

$$f(X) \equiv 0 \pmod{p^e}$$

con $f(X) \in \mathbb{Z}[X], f(X) \neq 0$, p primo ed $e \geqslant 1$.

Al I Problema dà completa risposta il Teorema Cinese dei Resti (cfr. Paragrafo 3). Un metodo di approccio al II Problema consiste in un procedimento di tipo induttivo:

II PROBLEMA (A): Determinare le soluzioni di una congruenza polinomiale del tipo:

$$f(X) \equiv 0 \pmod p$$

con $f(X) \in \mathbb{Z}[X], f(X) \neq 0$ e p primo.

II PROBLEMA (B): Supponendo di aver determinato le soluzioni di una congruenza polinomiale del tipo:

$$f(X) \equiv 0 \pmod{p^n},$$

determinare le soluzioni della congruenza:

$$f(X) \equiv 0 \pmod{p^{n+1}},$$

con $f(X) \in \mathbb{Z}[X], f(X) \neq 0$, p primo ed $n \geqslant 1$.

In altri termini, una soluzione di $f(X) \equiv 0 \pmod{p^e}$ per $e \geqslant 2$ è determinata per successive approssimazioni (a meno di potenze di p) a partire dalle soluzioni di $f(X) \equiv 0 \pmod{p}$. L'algoritmo che descriveremo è ispirato al cosiddetto metodo di Newton utilizzato in analisi.

Affrontiamo dapprima il II Problema (B). A tale scopo richiamiamo alcune proprietà formali dei polinomi.

Definizione 4.3. Sia $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$. Si chiama *polinomio derivato di* $f(X)$ il polinomio:

$$(f(X))' := a_1 + 2a_2X + \cdots + na_nX^{n-1} = \sum_{i=1}^{n} ia_iX^{i-1}$$

Per comodità di notazione il polinomio $(f(X))'$ verrà denotato in seguito anche con $f'(X)$, o semplicemente con f', se non ci saranno pericoli di ambiguità.
In generale, si chiama *k-esimo polinomio derivato di* $f(X)$ (con $k \geqslant 1$) il polinomio $f^{(k)} = f^{(k)}(X) := (f^{(k-1)}(X))'$.
Si conviene di porre $f(X) =: f^{(0)}(X)$.

Il seguente risultato è di dimostrazione immediata:

Lemma 4.4. *Siano* $f, g \in \mathbb{Z}[X]$ *ed* $a \in \mathbb{Z}$. *Allora:*
(a) $(f+g)' = f' + g'$;
(b) $(af)' = af'$;
(c) $(fg)' = f'g + fg'$. $\square$

Vale, inoltre, il seguente risultato "formale" analogo alla formula di Taylor:

Lemma 4.5. *Sia* $f(X) = \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}[X]$. *Per ogni* $\alpha \in \mathbb{Z}$ *si ha:*

$$f(X+\alpha) = f(X) + \frac{f'(X)}{1!}\alpha + \frac{f''(X)}{2!}\alpha^2 + \cdots + \frac{f^{(m)}(X)}{m!}\alpha^m.$$

Inoltre, per ogni k *tale che* $0 \leqslant k \leqslant m$, *risulta:*

$$\frac{f^{(k)}(X)}{k!} \in \mathbb{Z}[X].$$

Dimostrazione. In base al Lemma 4.4(a), (b), è sufficiente limitarsi al caso in cui $f(X) = X^i$. Si ha allora, in base alla Definizione 4.3 ed alla nota

formula del binomio di Newton[1]:

$$(X+\alpha)^i = \sum_{k=0}^{i} \binom{i}{k} X^{i-k}\alpha^k = \\ = \sum_{k=0}^{i} \frac{i(i-1)\dots(i-k+1)}{k!} X^{i-k}\alpha^k = \\ = \sum_{k=0}^{i} f^{(k)}(X)\frac{1}{k!}\alpha^k.$$

L'ultima affermazione è ovvia, in quanto, in generale per

$$f(X) = \sum_{i=0}^{m} a_i X^i,$$

risulta:

$$\frac{f^{(k)}(X)}{k!} = \sum_{i=k}^{m} \binom{i}{k} a_i X^{i-k}$$

dove $\binom{i}{k}$, per $0 \leqslant k \leqslant i$, è un intero essendo uguale a $\frac{i!}{k!(i-k)!}$. $\square$

Al Problema II (B) fornisce una risposta completa il seguente teorema:

Teorema 4.6. *Sia $f(X) \in \mathbb{Z}[X], f(X) \neq 0$; sia p un primo ed $n \in \mathbb{Z}, n > 0$. Supponiamo che la congruenza:*

$$f(X) \equiv 0 \pmod{p^n} \qquad (*_n)$$

sia risolubile e che, di questa congruenza, siano note le soluzioni $\{y_1, \dots, y_r\}$ $\pmod{p^n}$. Consideriamo la congruenza:

$$f(X) \equiv 0 \pmod{p^{n+1}} \qquad (*_{n+1})$$

Le (eventuali) soluzioni di $(*_{n+1}) \pmod{p^{n+1}}$ sono della forma:

$$x_t := y + tp^n,$$

dove y è una soluzione di $(*_n)$ e $t \in \mathbb{Z},\ 0 \leqslant t \leqslant p-1$. Precisamente si presentano tre casi:

[1]Presi comunque $\alpha, \beta \in \mathbb{Z}[X]$ si dimostra facilmente per induzione su $r \geqslant 1$ che:

$$(\alpha+\beta)^r = \sum_{k=0}^{r} \binom{r}{k} \alpha^{r-k}\beta^k$$

I Caso. *Se* $f'(y) \not\equiv 0 \pmod{p}$, x_t *è soluzione di* $(*_{n+1})$ *se, e soltanto se, risulta:*

$$t \equiv -\frac{f(y)}{p^n}(f'(y))^{p-2} \pmod{p}.$$

II Caso. *Se* $f'(y) \equiv 0 \pmod{p}$ *e* $f(y) \equiv 0 \pmod{p^{n+1}}$, *allora* x_t *è soluzione di* $(*_{n+1})$, *per ogni* $t \in \mathbb{Z}, 0 \leqslant t \leqslant p-1$.

III Caso. *Se* $f'(y) \equiv 0 \pmod{p}$ *e* $f(y) \not\equiv 0 \pmod{p^{n+1}}$, x_t *non è soluzione di* $(*_{n+1})$, *per nessun* $t \in \mathbb{Z}$.

Conseguentemente, la soluzione y *di* $(*_n)$, $y \in \{y_1, \ldots, y_r\}$, *determina:*

- *nel I Caso, una ed una sola soluzione di* $(*_{n+1}) \pmod{p^{n+1}}$, *e cioè:*

$$x := y - f(y)(f'(y))^{p-2};$$

- *nel II Caso,* p *soluzioni distinte di* $(*_{n+1}) \pmod{p^{n+1}}$, *e cioè:*

$$x_t = y + tp^n, \quad 0 \leqslant t \leqslant p-1;$$

- *nel III Caso, nessuna soluzione di* $(*_{n+1}) \pmod{p^{n+1}}$.

Nel I Caso y è detta *soluzione non singolare* di $(*_n)$, mentre negli altri casi, y è detta *soluzione singolare* di $(*_n)$.

Dimostrazione. Le (eventuali) soluzioni x di $(*_{n+1})$ sono ovviamente soluzioni di $(*_n)$ e dunque della forma:

$$x = y + tp^n,$$

con $t \in \mathbb{Z}$ e y soluzione di $(*_n)$, cioè $y \in \{y_1, \ldots, y_r\}$. Essendo $f(y) \equiv 0 \pmod{p^n}$, allora $f(y)/p^n \in \mathbb{Z}$.
In base al Lemma 4.5, posto $m := \deg(f(X))$, si ha:

$$f(x_t) = f(y + tp^n) = f(y) + \frac{f'(y)}{1!}tp^n + \cdots + \frac{f^{(m)}(y)}{m!}(tp^n)^m.$$

Poiché $n+1 \leqslant 2n < \cdots < n \cdot m$, si ha $0 \equiv p^{2n} \equiv \cdots \equiv p^{nm} \pmod{p^{n+1}}$ e quindi, dall'uguaglianza precedente, si ottiene:

$$f(x_t) \equiv f(y) + f'(y)tp^n \pmod{p^{n+1}}.$$

Pertanto $x_t = y + tp^n$ è soluzione di $(*_n)$ se, e soltanto se, esiste $t \in \mathbb{Z}$ tale che:

$$0 \equiv f(y) + f'(y)tp^n \pmod{p^{n+1}},$$

ovvero, "cancellando" p^n (cfr. Proposizione 1.9):

$$f'(y)t \equiv -\frac{f(y)}{p^n} \pmod{p}.$$

Posto $a := f'(y), b := -\frac{f(y)}{p^n}$, ci si è ricondotti a discutere la risolubilità della congruenza lineare in una nuova indeterminata (denotata T):

$$aT \equiv b \pmod{p} \qquad (\bullet_y)$$

Distinguiamo tre casi:
I Caso. Se $a \not\equiv 0 \pmod{p}$, per ogni $y \in \{y_1, \ldots, y_r\}$, la congruenza lineare $(\bullet_y)$ ha una ed una sola soluzione $t \equiv a^* b \equiv a^{p-2} b \pmod{p}$.
In tal caso, $x_t = y + p^n t = y - p^n \frac{f(y)}{p^n} (f'(y))^{p-2} = y - f(y)(f'(y))^{p-2}$ è l'unica soluzione di $(*_{n+1}) \pmod{p^{n+1}}$ determinata dalla soluzione y di $(*_{n+1})$.
II Caso. Se $a \equiv b \equiv 0 \pmod{p}$, la congruenza $(\bullet_y)$ degenera, cioè è soddisfatta per ogni $t \in \mathbb{Z},\ 0 \leqslant t \leqslant p-1$.
In tal caso, per ogni $y \in \{y_1, \ldots, y_r\}$, le soluzioni distinte di $(*_{n+1})$ (cioè non congruenti modulo p^{n+1}) sono esattamente p, e sono date da:

$$x_t = y + tp^n, \quad 0 \leqslant t \leqslant p-1.$$

III Caso. Se $a \equiv 0 \pmod{p}$ e $b \not\equiv 0 \pmod{p}$, allora $(\bullet_y)$ non è risolubile. Quindi, $x_t = y + tp^n$ non è mai soluzione di $(*_{n+1})$, al variare comunque di $t \in \mathbb{Z}$. Cioè, in altri termini, la soluzione $y \in \{y_1, \ldots, y_r\}$ di $(*_n)$ non determina alcuna soluzione di $(*_{n+1})$. □

Vogliamo illustrare il risultato precedente con quattro esempi.

Esempio 4.7. Consideriamo la congruenza:

$$X^4 - 1 \equiv 0 \pmod{25}.$$

Notiamo, innanzitutto, che $X^4 - 1 \equiv 0 \pmod{5}$, per il "Piccolo" Teorema di Fermat, ha quattro soluzioni: $y_1 = 1, y_2 = 2, y_3 = 3, y_4 = 4$.
Se $f(X) := X^4 - 1$ allora $f'(X) = 4X^3$. Essendo $f'(y_i) \not\equiv 0 \pmod{5}$ per ogni $1 \leqslant i \leqslant 4$, allora ciascuna y_i determina un'unica soluzione di $f(X) \equiv 0 \pmod{25}$ data da:

$$x_i := y_i + \bar{t}_i \cdot 5,$$

dove $\bar{t}_i$ è l'unica soluzione $\pmod{5}$ della seguente congruenza lineare nell'indeterminata T associata ad y_i (che denotiamo semplicemente con $(\bullet_i)$ invece che con $(\bullet_{y_i})$):

$$f'(y_i)T \equiv -\frac{f(y_i)}{5} \pmod{5} \qquad (\bullet_i)$$

Per $i = 1$,

$$4T \equiv 0 \pmod{5} \qquad (\bullet_1)$$

ha come soluzione $\bar{t}_1 = 0$, dunque $x_1 = y_1 = 1 \pmod{25}$.
Per $i = 2$,

$$2T \equiv -3 \pmod{5} \qquad (\bullet_2)$$

ha come soluzione $\bar{t}_2 = 1$, dunque $x_2 = 2 + 1 \cdot 5 = 7 \pmod{25}$.
Per $i = 3$,

$$3T \equiv -1 \pmod{5} \qquad (\bullet_3)$$

ha come soluzione $\bar{t}_3 = 3$, dunque $x_3 = 3 + 3 \cdot 5 = 18 \pmod{25}$.
Per $i = 4$,

$$T \equiv -1 \pmod{5} \qquad (\bullet_4)$$

ha come soluzione $\bar{t}_4 = -1$, dunque $x_4 = 4 - 5 = -1 \equiv 24 \pmod{25}$.

Il precedente esempio può essere generalizzato nella maniera seguente:

Esempio 4.8. Sia p un primo ed e un intero $\geqslant 1$. La congruenza:

$$f(X) := X^{p-1} - 1 \equiv 0 \pmod{p^e}$$

ha esattamente $p - 1$ soluzioni distinte.
Infatti, se $e = 1$, tale risultato è un'ovvia conseguenza del "Piccolo" Teorema di Fermat. Sia $e \geqslant 2$ e sia y una soluzione di $f(X) \equiv 0 \pmod{p^{e-1}}$. È subito visto che $f'(y) = (p-1)y^{p-2} \not\equiv 0 \pmod{p}$ e, dunque, si è nel I Caso del Teorema 4.6.

Esempio 4.9. Consideriamo la congruenza:

$$X^{10} - 1 \equiv 0 \pmod{25}.$$

Notiamo innanzitutto che la congruenza

$$X^{10} - 1 \equiv 0 \pmod{5}$$

ha due soluzioni: $y_1 = 1, y_2 = 4$.
Infatti $X^{10} = (X^4)^2 X^2$, dunque $X^{10} - 1 \equiv (X^4)^2 X^2 - 1 \pmod{5}$. Dal momento che, per il "Piccolo" Teorema di Fermat, $x^4 \equiv 1 \pmod{5}$, per ogni x non congruo a $0 \pmod{5}$, allora le soluzioni di $X^{10} - 1 \equiv 0 \pmod{5}$ coincidono con le soluzioni di $X^2 - 1 \equiv 0 \pmod{5}$, che sono appunto $y_1 = 1$ ed $y_2 = 4$. Se $f(X) := X^{10} - 1$, allora $f'(X) = 10X^9$ e quindi $f'(y_i) \equiv 0 \pmod{5}$ per $i = 1, 2$. Inoltre, $f(y_i) \equiv 0 \pmod{25}$, per $i = 1, 2$ (ciò è ovvio per $y_1 = 1$, per $y_2 = 4$ è subito visto che $4^5 \equiv -1 \pmod{25}$ e dunque $4^{10} \equiv (-1)^2 = 1 \pmod{25}$). Pertanto, y_1 determina le seguenti 5 soluzioni della congruenza data:

$$x_{1,t} := 1 + t \cdot 5, \quad \text{per} \quad 0 \leqslant t \leqslant 4.$$

Analogamente, y_2 determina le seguenti 5 soluzioni della congruenza data:

$$x_{2,t} := 4 + t \cdot 5, \quad \text{per} \quad 0 \leqslant t \leqslant 4.$$

In conclusione, la congruenza assegnata ha 10 soluzioni $\pmod{25}$.

L'esempio precedente si generalizza nella forma seguente:

Esempio 4.10. Sia p un primo dispari. La congruenza:

$$f(X) = X^{p\frac{p-1}{2}} - 1 \equiv 0 \pmod{p^2} \qquad (*_2)$$

ammette $\frac{p(p-1)}{2}$ soluzioni distinte.
Si verifica preliminarmente che la congruenza $f(X) \equiv 0 \pmod{p}$ ammette esattamente $\frac{p-1}{2}$ soluzioni distinte.
Osserviamo, innanzitutto, che le soluzioni di:

$$f(X) = X^{p\frac{p-1}{2}} - 1 \equiv 0 \pmod{p} \qquad (*_1)$$

sono le stesse di quelle della congruenza:

$$g(X) = X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$$

dal momento che $X^p \equiv X \pmod{p}$ è risolubile, per ogni $x \in \mathbb{Z}$.
Mostriamo, poi, che $g(X) \equiv 0 \pmod{p}$ ha esattamente $\frac{p-1}{2}$ soluzioni $\pmod{p}$. Per questo, abbiamo bisogno del seguente

Lemma 4.11. *Sia p un primo dispari. Le due congruenze:*

$$X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p} \qquad (*)$$

$$X^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p} \qquad (**)$$

ammettono ciascuna $\frac{p-1}{2}$ soluzioni distinte (modulo p). L'unione di tali insiemi di soluzioni costituisce un sistema ridotto di residui (modulo p).

Dimostrazione. Certamente $x = 0$ non è soluzione nè di $(*)$ nè di $(**)$ e le due congruenze non possono ammettere soluzioni comuni perché $p > 2$. Considerato il sistema ridotto di residui $S^* = \{1, 2, \ldots, p-1\}$, basterà allora provare che (almeno) $\frac{p-1}{2}$ elementi di S^* verificano $(*)$ e che (almeno) altrettanti verificano $(**)$.

Osserviamo innanzitutto che gli interi $1^2, 2^2, \ldots, \left[\frac{p-1}{2}\right]^2$ sono primi con p e, a due a due incongruenti (modulo p).
Infatti se h, k sono interi tali che $1 \leqslant h, k \leqslant \frac{p-1}{2}$ e $h^2 \equiv k^2 \pmod{p}$, allora, $h^2 - k^2 = (h+k)(h-k) \equiv 0 \pmod{p}$ e quindi, $h \equiv k \pmod{p}$ (da cui $h = k$), oppure $h \equiv -k \pmod{p}$, cioè $h \equiv p - k \pmod{p}$, e perciò $h = p - k$, il che è assurdo.
Pertanto è possibile costruire un sistema ridotto di residui (modulo p), diciamo U^*, scegliendo opportunamente altri $\frac{p-1}{2}$ interi, che denotiamo con $t_1, \ldots, t_{\frac{p-1}{2}}$, nella maniera seguente:

$$U^* := \{1^2, 2^2, \ldots, \left[\frac{p-1}{2}\right]^2, t_1, \ldots, t_{\frac{p-1}{2}}\}.$$

Confrontando S^* con U^*, è chiaro che, per $\frac{p-1}{2}$ elementi $a \in S^*$, risulta $a \equiv h^2 \pmod{p}$ (con $1 \leqslant h \leqslant \frac{p-1}{2}$), mentre per altri $\frac{p-1}{2}$ elementi $a \in S^*$ risulta $a \equiv t_i \pmod{p}$ (con $1 \leqslant i \leqslant \frac{p-1}{2}$).
Se $a \equiv h^2 \pmod{p}$, allora $a^{\frac{p-1}{2}} \equiv h^{p-1} \equiv 1 \pmod{p}$ (infatti $p \nmid h$ e, dunque, è applicabile il Teorema 3.1): pertanto a è soluzione di $(*)$.
Sia $a \in S^*$ tale che $a \equiv t_i \pmod{p}$. Per ogni $k \in S^*$, (in particolare per $1 \leqslant k \leqslant \frac{p-1}{2}$) l'insieme $T^* := \{k, 2k, \ldots, (p-1)k\}$ è ancora un sistema ridotto di residui (modulo p) (cfr. Esercizio 2.10) e, dunque, esiste un unico elemento $k' \in S^*$ tale che $kk' \equiv a \pmod{p}$. L'elemento k' è detto *associato di k relativamente ad a* $\pmod{p}$ e, per ipotesi, è distinto da k. Infatti, è ovvio che $k^2 \equiv (p-k)^2 \pmod{p}$; se fosse $k = k'$, allora $a \equiv k^2 \equiv (p-k)^2$ e uno dei due interi $k, p-k$ dovrebbe essere minore o uguale a $\frac{p-1}{2}$. Ciò è escluso quando $1 \leqslant k \leqslant \frac{p-1}{2}$.
Allora, fissato $a \in S^*$ con $a \equiv t_i \pmod{p}$, gli elementi di S^* si ripartiscono in due sottoinsiemi (disgiunti) di elementi non associati, cioè:

$$S^* : \{h_1, \ldots, h_{\frac{p-1}{2}}\} \sqcup \{h'_1, \ldots, h'_{\frac{p-1}{2}}\}$$

in modo che:

$$h_i h'_i \equiv a \pmod{p},\ 1 \leqslant i \leqslant \frac{p-1}{2}.$$

Ne segue che:

$$(p-1)! = h_1 h'_1 \ldots h_{\frac{p-1}{2}} h'_{\frac{p-1}{2}} \equiv a \ldots a = a^{\frac{p-1}{2}} \pmod{p}$$

e dunque, in base al Teorema di Wilson:

$$(p-1)! \equiv -1 \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

In tal caso, a è soluzione di $(**)$ e la tesi è così dimostrata. $\square$

Abbiamo visto sopra che le soluzioni di $(*_1)$ coincidono con quelle di $(*)$. Sia y una delle $\frac{p-1}{2}$ soluzioni distinte di

$$X^{p\left(\frac{p-1}{2}\right)} - 1 \equiv 0 \pmod{p}.$$

allora: $f'(y) = p\left(\frac{p-1}{2}\right) \cdot y^{p\left(\frac{p-1}{2}\right)-1} \equiv 0 \pmod{p}$. Inoltre, si vede facilmente che $f(y) \equiv 0 \pmod{p^2}$. Infatti $y^{p\left(\frac{p-1}{2}\right)} - 1 = kp$ per qualche k, elevando al quadrato abbiamo che

$$k^2 p^2 = (y^{p\left(\frac{p-1}{2}\right)} - 1)^2 = y^{p(p-1)} + 1 - 2y^{p\left(\frac{p-1}{2}\right)} \qquad (\diamondsuit)$$

Inoltre, $\varphi(p^2) = p(p-1)$ e quindi per il Teorema di Euler:

$$z^{p(p-1)} \equiv 1 \pmod{p^2}$$

per ogni z relativamente primo con p^2. Dunque, per $z = y$, da $(\diamondsuit)$ abbiamo che:

$$0 \equiv 2 - 2y^{p\left(\frac{p-1}{2}\right)} \pmod{p^2}$$

e dunque che

$$y^{p\left(\frac{p-1}{2}\right)} - 1 \equiv 0 \pmod{p^2}.$$

Dunque si è nella condizione del II Caso del Teorema 4.6 e ciò permette di concludere quanto enunciato nell'Esempio 4.10.

Veniamo ora al Problema II (A). Non esiste un procedimento teorico generale per determinare se una congruenza del tipo:

$$f(X) \equiv 0 \pmod{p},$$

con p primo e $f(X) \in \mathbb{Z}[X]$, ammetta soluzioni e, nel caso affermativo, per calcolarle esplicitamente. Ci limiteremo qui a svolgere semplici considerazioni generali tendenti a semplificare il problema e che, comunque, saranno utili nel seguito per la risoluzione delle congruenze quadratiche (modulo p), cioè congruenze tali che $\deg(f) = 2$.

Cominciamo con la seguente definizione:

Definizione 4.12. Sia $n \in \mathbb{Z}, n > 0$ e siano

$$f = \sum_{i=0}^{r} a_i X^i, \quad g = \sum_{j=0}^{s} b_j X^j \in \mathbb{Z}[X].$$

(a) Si dice che il polinomio f è *identicamente congruo a zero modulo* n (in simboli, $f(X) \equiv_X 0 \pmod{n}$) se $a_i \equiv 0 \pmod{n}$ preso comunque $1 \leqslant i \leqslant r$.

(b) Si dice che f è *identicamente congruente a* g *modulo* n (e si scrive $f \equiv_X g \pmod{n}$) se $f - g$ è identicamente congruo a zero modulo n (cioè se risulta $a_i \equiv b_i \pmod{n}$, per ogni i tale che $0 \leqslant i \leqslant \max(r, s)$).

(c) Si chiama *grado di* f *modulo* n (e si scrive $\deg_n(f)$) il massimo intero m tale che $a_m \not\equiv 0 \pmod{n}$.

(d) Si dice che f *divide* g *modulo* n (e si scrive $f \mid g \pmod{n}$) se esiste $l \in \mathbb{Z}[X]$ tale che $fl \equiv_X g \pmod{n}$.

(e) Si dice inoltre che $f(X)$ è *equivalente a* $g(X)$ *modulo* n, (in simboli $f(X) \sim g(X) \pmod{n}$) se, per ogni $a \in \mathbb{Z}$, $f(a) \equiv g(a) \pmod{n}$.

Se $f(X) \sim g(X) \pmod{n}$ allora le congruenze

$$f(X) \equiv 0 \pmod{n} \quad \text{e} \quad g(X) \equiv 0 \pmod{n}$$

hanno le stesse soluzioni (modulo n).

Osservazione 4.13. Si consideri l'omomorfismo suriettivo tra anelli di polinomi:

$$\bar{\varphi}_n : \mathbb{Z}[X] \longrightarrow (\mathbb{Z}/n\mathbb{Z})[X],\ f \mapsto \bar{f},$$

che estende in modo naturale l'omomorfismo canonico suriettivo

$$\varphi_n : \mathbb{Z} \longrightarrow (\mathbb{Z}/n\mathbb{Z}),$$

(cioè $\bar{\varphi}_n$ è così definito:
per ogni $f := \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}[X]$, $\bar{\varphi}_n(f) = \bar{f} := \sum_{i=0}^{m} \bar{a}_i X^i$, con $\bar{a}_i := a_i + n\mathbb{Z}$).
È del tutto evidente che:
(a′) $f \equiv_X 0 \pmod{n} \iff \bar{f} = 0$;
(b′) $f \equiv_X g \pmod{n} \iff \bar{f} = \bar{g}$;
(c′) $\deg_n(f) = \deg(\bar{f})$;
(d′) $f \mid g \pmod{n} \iff \bar{f} \mid \bar{g}$.

Proposizione 4.14. *Siano $a, n \in \mathbb{Z}$, $n > 0$ ed $f, g \in \mathbb{Z}[X]$. Risulta:*
(a) $(X - a) \mid f \pmod{n}$ *se, e soltanto se,* $f(a) \equiv 0 \pmod{n}$.
(b) *Se $f \equiv_X g \pmod{n}$, allora $f \sim g \pmod{n}$. In particolare, quindi, le congruenze:*

$$f(X) \equiv 0 \pmod{n} \quad e \quad g(X) \equiv 0 \pmod{n}$$

hanno le stesse soluzioni.

Dimostrazione. Semplice esercizio. □

Osservazione 4.15. Le affermazioni della Proposizione 4.14(b) non si invertono, in generale. Ad esempio posto $f(X) = X, g(X) = X^p$ con p primo, si ha che $f \not\equiv_X g \pmod{p}$ (cfr. Definizione 4.12(b)), mentre $f(a) \equiv g(a) \pmod{p}$, per ogni $a \in \mathbb{Z}$, cioè $f \sim g \pmod{p}$ (cfr. Corollario 3.2).

Corollario 4.16. *Sia $n \in \mathbb{Z}, n > 0$, e sia $f := \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}[X]$. Posto $\hat{f}(X) := \sum_{i=0}^{m} \hat{a}_i X^i$ con $a_i \equiv \hat{a}_i \pmod{n}, 0 \leqslant \hat{a}_i \leqslant n - 1$ e $0 \leqslant i \leqslant m$, allora:*

$$f(X) \equiv_X \hat{f}(X) \pmod{n}. \qquad \square$$

Corollario 4.17. *Sia p primo ed $f(X) \in \mathbb{Z}[X]$. Esiste un polinomio $\widetilde{f}(X) \in \mathbb{Z}[X]$ di grado $\leqslant p - 1$, eventualmente uguale al polinomio nullo, tale che:*

$$f(X) \sim \widetilde{f}(X) \pmod{p}.$$

Dimostrazione. Sia $f(X) := \sum_{i=0}^{m} a_i X^i$ con $m = \deg_p(f(X))$.
Se $m \leqslant p - 1$, si pone $\widetilde{f} := f$.
Se invece $m \geqslant p$, si pone:

$$\widetilde{f} := \sum_{i=0}^{p-1} a_i X^i + \sum_{j=p}^{m} a_j X^{r_j},$$

dove r_j, con $1 \leqslant r_j \leqslant p-1$, è il "resto" della seguente divisione di j per $p-1$:

$$j = q_j(p-1) + r_j, \text{ (con } p \leqslant j \leqslant m).$$

Utilizzando il "Piccolo" Teorema di Fermat, si verifica subito che:
$f(a) - \widetilde{f}(a) \equiv 0 \pmod{p}$ per ogni $a \in \mathbb{Z}$ e da ciò segue la tesi. $\square$

Per illustrare il Corollario 4.17, si noti che se p è un primo dispari e $f(X) := X^{p\left(\frac{p-1}{2}\right)} - 1$ allora $\widetilde{f}(X) = X^{\frac{p-1}{2}} - 1$. Abbiamo già notato sopra (Esempio 4.10) che:

$$f(X) \sim \widetilde{f}(X) \pmod{p}.$$

Teorema 4.18. (**Teorema di Lagrange**)
Sia p un primo ed $f \in \mathbb{Z}[X]$ tale che $deg_p(f) = m$. La congruenza:

$$f(X) \equiv 0 \pmod{p}$$

ammette al più m soluzioni distinte (cioè incongruenti modulo p).

Dimostrazione. Si procede per induzione su m.
Se $m = 1$, allora $f(X) \equiv a_0 + a_1X \equiv 0 \pmod{p}$, con $\text{MCD}(a_1, p) = 1$. In tal caso è ben noto (cfr. Lemma 2.3) che la congruenza ammette un'unica soluzione (modulo p).
Sia $m \geqslant 2$ ed assumiamo che il teorema sia vero per un polinomio di grado $\leqslant m-1$ (modulo p). Se la congruenza in esame non ha soluzioni, la tesi è ovvia; se viceversa $a \in \mathbb{Z}$ ne è una soluzione, si divide $f(X)$ per $X - a$ ottenendo un polinomio $q(X) \in \mathbb{Z}[X]$ tale che:

$$f(X) = (X-a)q(X) + f(a).$$

Da ciò segue che $f(X) \equiv_X (X-a)q(X) \pmod{p}$ e pertanto le congruenze:

$$f(X) \equiv 0 \pmod{p} \quad \text{e} \quad (X-a)q(X) \equiv 0 \pmod{p}$$

hanno lo stesso insieme di soluzioni (mod p). Se ora $b \in \mathbb{Z}$ è un'altra soluzione della prima congruenza e se $b \not\equiv a \pmod{p}$, allora $(b-a)q(b) \equiv 0 \pmod{p}$ e quindi, essendo p primo, $q(b) \equiv 0 \pmod{p}$.
Tenendo presente che $\deg_p(q) \leqslant m-1$, la tesi discende immediatamente dalla ipotesi induttiva. $\square$

Corollario 4.19. *Siano f, g ed m come nel Teorema 4.18 e sia $\widetilde{f}$ in $\mathbb{Z}[X]$ come nel Corollario 4.17 (cioè $f \sim \widetilde{f} \pmod{p}$ e $deg_p(\widetilde{f}) \leqslant p-1$) allora la congruenza $f(X) \equiv 0 \pmod{p}$ ha al più $\widetilde{m}$ soluzioni distinte (mod p), dove $\widetilde{m} := deg_p(\widetilde{f}) \leqslant deg_p(f)$.*

Dimostrazione. Semplice conseguenza del Teorema 4.18, applicato ad $\widetilde{f}$, dal momento che le congruenze

$$f(X) \equiv 0 \pmod{p} \quad \text{e} \quad \widetilde{f}(X) \equiv 0 \pmod{p}$$

hanno le stesse soluzioni (modulo p). $\square$

Esempio 4.20. Sia $p = 3$, $f(X) = X^5 + X + 1$. Allora $\deg_3(f) = 5$, $X^5 \sim X^3 \sim X \pmod 3$, quindi $\widetilde{f} := X+X+1 = 2X+1$. Pertanto le soluzioni della congruenza $X^5 + X + 1 \equiv 0 \pmod 3$ sono al più tante quante le soluzioni di $2X + 1 \equiv 0 \pmod 3$, cioè una. Precisamente, $\widetilde{f}(X) \equiv 0 \pmod 3$ (e $f(X) \equiv 0 \pmod 3$) hanno un'unica soluzione, che è data da $x \equiv 1 \pmod 3$.

Osservazione 4.21. Il Teorema di Lagrange non vale, in generale, per congruenze modulo un intero non primo. Ad esempio, la congruenza:

$$X^2 - 1 \equiv 0 \pmod 8$$

ammette quattro soluzioni distinte (e cioè $1, 3, 5, 7$), pur essendo $\deg_8(X^2 - 1) = 2$. Per un'estensione di questo esempio rinviamo al successivo Esercizio 4.4.

Corollario 4.22. *Conservando le notazioni del Teorema 4.18 e denotando con $a_1, \ldots, a_t$ $(0 \leqslant t \leqslant m)$ le soluzioni distinte di $f(X) \equiv 0 \pmod p$, si ha:*

$$f(X) \equiv_X g(X)(X - a_1)^{e_1} \cdots (X - a_t)^{e_t} \pmod p$$

dove $e_1, \ldots, e_t$ sono interi positivi tali che $\sum_{i=1}^{t} e_i \leqslant m$ e dove $g(X)$ in $\mathbb{Z}[X]$, $deg_p(g) \geqslant 0$ e la congruenza $g(X) \equiv 0 \pmod p$ non è risolubile.

Dimostrazione. Basta iterare l'argomentazione usata nella dimostrazione del Teorema 4.18. □

Proposizione 4.23. *Sia p primo, $f \in \mathbb{Z}[X]$ e t il numero delle soluzioni distinte della congruenza:*

$$f(X) \equiv 0 \pmod p.$$

Risulta:

$$t = deg_p(f) \iff f \mid (X^p - X) \pmod p.$$

Dimostrazione. Notiamo innanzitutto che, per il Corollario 4.22,

$$X^p - X \equiv_X X(X - 1)(X - 2)\ldots(X - (p - 1)) \pmod p$$

(⇒) Se $t = \deg_p(f)$, allora per il Corollario 4.22

$$f(X) \equiv_X (X - a_1)(X - a_2)\ldots(X - a_t) \pmod p$$

con $\{a_1, \ldots, a_t\} \subseteq \{0, 1, \ldots, p - 1\}$.
Dunque è ovvio che $f(X) \mid (X^p - X) \pmod p$.
(⇐) Se $f(X)g(X) \equiv_X X^p - X \pmod p$ per un qualche $g(X) \in \mathbb{Z}[X]$, allora $\deg_p(f(X)g(X)) = \deg_p(f(X))+\deg_p(g(X)) = \deg_p(X^p - X) = p$ ed inoltre le seguenti congruenze:

$$\begin{aligned} X^p - X &\equiv 0 \pmod p \\ f(X)g(X) &\equiv 0 \pmod p \end{aligned} \qquad (*_{fg})$$

hanno le stesse soluzioni. Poiché la prima congruenza ha p soluzioni, anche la seconda congruenza deve avere p soluzioni.
Osserviamo che le soluzioni della congruenza $(*_{fg})$ sono le soluzioni di almeno una delle seguenti due congruenze:

$$f(X) \equiv 0 \pmod{p} \qquad (*_f)$$
$$g(X) \equiv 0 \pmod{p}. \qquad (*_g)$$

Per il Teorema di Lagrange $(*_f)$ ha al più $\deg_p(f)$ soluzioni e $(*_g)$ ha al più $\deg_p(g)$ soluzioni, quindi $(*_{fg})$ ha al più $\deg_p(f(X))+ \deg_p(g(X))$ soluzioni. Pertanto, affinché accada che $(*_{fg})$ abbia esattamente p soluzioni distinte, deve accadere che tanto $(*_f)$ quanto $(*_g)$ abbiano ciascuna il massimo di soluzioni distinte possibili e cioè, rispettivamente, $\deg_p(f)$ e $\deg_p(g)$. □

Osservazione 4.24. La proposizione precedente è un semplice corollario del seguente risultato più generale:

Siano $p, f(X)$ e t come nella Proposizione 4.23. Sia $\bar{F} \in (\mathbb{Z}/p\mathbb{Z})[X]$ il massimo comun divisore dei polinomi $\bar{f}$ e $X^p - X \in (\mathbb{Z}/p\mathbb{Z})[X]$ (cfr. Osservazione 4.13). Risulta allora:

$$t = deg(\bar{F}).$$

Dimostrazione. Si noti che $(\mathbb{Z}/p\mathbb{Z})$ è un campo e quindi in $(\mathbb{Z}/p\mathbb{Z})[X]$ esiste il massimo comun divisore di due polinomi non nulli. In $(\mathbb{Z}/p\mathbb{Z})[X]$ si ha: $X^p - X = X(X - \bar{1}) \dots (X - \overline{p-1})$ (cfr. Corollario 3.2) e quindi:
$\bar{f} = \bar{g} \cdot (X - \bar{a}_1)^{e_1} \dots (X - \bar{a}_t)^{e_t}$ (cfr. Corollario 4.22).
Ne segue che $\bar{F} = (X - \bar{a}_1) \dots (X - \bar{a}_t)$ e dunque che $\deg(\bar{F}) = t$. □

Terminiamo questo paragrafo con un teorema dimostrato da C. Chevalley e che riguarda polinomi in più indeterminate.

Sia $f \in \mathbb{Z}[X_1, \dots, X_r]$, dunque possiamo rappresentare f nella maniera seguente:

$$f = \sum_{0 \leqslant i_1, \dots, i_r \leqslant t} a_{i_1,\dots,i_r} X_1^{i_1} X_2^{i_2} \dots X_r^{i_r},$$

con $a_{i_1,\dots,i_r} \in \mathbb{Z}$ e $i_1, \dots, i_r \geqslant 0$.
Poniamo, per semplicità di notazione, $f = \sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$, dove $\mathbf{i} := (i_1, \dots, i_r)$ e $\mathbf{X}^{\mathbf{i}} := X_1^{i_1} X_2^{i_2} \dots X_r^{i_r}$. L'intero $i_1 + \dots + i_r$ si chiama *grado (complessivo)* del monomio $a_{i_1,\dots,i_r} X_1^{i_1} X_2^{i_2} \dots X_r^{i_r}$. Il massimo dei gradi dei monomi del polinomio f si dice *grado (complessivo)* di f e viene denotato con $\deg(f)$.

Definizione 4.25. Sia $f := \sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}} \in \mathbb{Z}[X_1, X_2, \dots, X_r]$ e sia $n \geqslant 0$. Diremo che il polinomio f è *identicamente congruo a zero (modulo n)*, in simboli $f \equiv_{\mathbf{X}} 0 \pmod{n}$, se $a_{\mathbf{i}} \equiv 0 \pmod{n}$ per ciascun multi-indice $\mathbf{i}$.
Se $f, g \in \mathbb{Z}[X_1, X_2, \dots, X_r]$, diremo che f è *congruo identicamente a g (modulo n)*, in simboli $f \equiv_{\mathbf{X}} g \pmod{n}$, se $f - g \equiv_{\mathbf{X}} 0 \pmod{n}$.

Diremo che f è *equivalente a g (modulo n)*, in simboli $f \sim g \pmod n$, se preso comunque $(a_1, \ldots, a_r) \in \mathbb{Z}^r$,

$$f(a_1, \ldots, a_r) \equiv g(a_1, \ldots, a_r) \pmod n$$

È ovvio che:

$$f \equiv_{\mathbf{X}} g \pmod n \Rightarrow f \sim g \pmod n.$$

Abbiamo già osservato che per polinomi in una indeterminata non è vero il viceversa.

Proposizione 4.26. *Sia $f \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$, sia m il grado complessivo di f e sia p un numero primo.*
Esiste un polinomio $\widetilde{f} \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$, eventualmente nullo, con il grado di $\widetilde{f}$ in ciascuna indeterminata $\leqslant p-1$, tale che

$$f \sim \widetilde{f} \pmod p.$$

Dimostrazione. Per ogni $k \geqslant p-1$, si consideri una divisione con il "resto" di k rispetto a $(p-1)$, del tipo:

$$k = q \cdot (p-1) + r \quad \text{con } 1 \leqslant r \leqslant p-1.$$

È ovvio che, per ogni $1 \leqslant i \leqslant r$, se $k = q \cdot (p-1) + r$ allora:

$$X_i^k \sim X_i^r \pmod p.$$

Applicando questa "trasformazione" ad ogni indeterminata X_i ed ad ogni esponente $\geqslant p-1$, si ottiene un polinomio $\widetilde{f}$ che soddisfa alla proprietà enunciata.□

Proposizione 4.27. *Siano $f, g \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$ sia p un primo fissato e siano $\widetilde{f}, \widetilde{g} \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$ come nella Proposizione 4.26.*

$$\widetilde{f} \sim \widetilde{g} \pmod p \iff \widetilde{f} \equiv_{\mathbf{X}} \widetilde{g} \pmod p$$

Dimostrazione. **(⇒)** Passando al polinomio $f-g$, basta dimostrare che se $h \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$, con grado di $h \leqslant p-1$ in ogni indeterminata, allora:

$$h \sim 0 \pmod p \Rightarrow h \equiv_{\mathbf{X}} 0 \pmod p.$$

Si proceda per induzione sul numero delle indeterminate r.
Se $r = 1$, un polinomio di grado $\leqslant p-1$ con p radici distinte deve essere identicamente congruo a zero (modulo p) per il Teorema di Lagrange.
Sia $(x_2, \ldots, x_r) \in \mathbb{Z}^{r-1}$, poniamo

$$w(X_1) := h(X_1, x_2, \ldots, x_r) = \sum_{j=0}^{p-1} h_j(x_2, \ldots, x_r) X_1^j \in \mathbb{Z}[X_1]$$

Riapplicando il Teorema di Lagrange a $w(X_1)$ abbiamo che:

$$w \equiv_{X_1} 0 \pmod{p}, \text{ cioè } h_j \sim 0 \pmod{p} \text{ per ogni } j.$$

Dunque, per ipotesi induttiva, h_j è identicamente congruo a 0 (modulo p) per ogni j, e quindi $h \equiv_{\mathbf{X}} 0 \pmod{p}$.
($\Leftarrow$) È banale. $\square$

Nel 1935 E. Artin congetturò che una congruenza polinomiale priva di termine noto (modulo p), con p primo, ha sempre una soluzione non banale se il numero delle indeterminate del polinomio è maggiore del grado (complessivo) del polinomio. Ad esempio, se $a, b, c \in \mathbb{Z}$, con $abc \not\equiv 0 \pmod{p}$,

$$aX^2 + bY^2 + cZ^2 \equiv 0 \pmod{p}$$

ha sempre almeno una soluzione non banale. Tale congettura fu dimostrata nel 1936 da C. Chevalley.

Teorema 4.28. (C. Chevalley)
Sia p un primo e siano $f, g \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$ due polinomi ciascuno con grado (complessivo) $\leqslant r - 1$.
(a) *Se la congruenza*

$$f(X_1, X_2, \ldots, X_r) \equiv 0 \pmod{p} \tag{3}$$

è risolubile, allora ha almeno due soluzioni.
(b) *Se g è un polinomio privo di termine noto (ad esempio un polinomio omogeneo non costante), allora la congruenza*

$$g(X_1, X_2, \ldots, X_r) \equiv 0 \pmod{p} \tag{4}$$

ha sempre una soluzione non banale.

Dimostrazione. (b) segue immediatamente da (a), in quanto la congruenza (4) possiede sempre la soluzione banale $(0, 0, \ldots, 0)$.
(a) Supponiamo che (3) possieda un'unica soluzione:

$$(a_1, \ldots, a_r) \pmod{p}.$$

Consideriamo il polinomio

$$h(X_1, \ldots, X_r) := 1 - f(X_1, \ldots, X_r)^{p-1}$$

È ovvio che:

$$h(x_1, \ldots, x_r) = \begin{cases} 1, & \text{se } x_i \equiv a_i \pmod{p}, \text{ per ogni } i \\ 0, & \text{altrimenti} \end{cases}$$

Sia $\widetilde{h}$ un polinomio di grado $\leqslant p-1$ in ciascuna indeterminata tale che $h \sim \widetilde{h}$ (mod p) (cfr. Proposizione 4.26).
Si consideri, poi, il seguente polinomio:

$$h^*(X_1, \ldots, X_r) := \prod_{i=1}^{r} \left(1 - (X_i - a_i)^{p-1}\right)$$

È subito visto che $h^* \sim h \pmod{p}$ e dunque $h^* \sim \widetilde{h} \pmod{p}$. Quindi, per la Proposizione 4.27, $h^* \equiv_{\mathbf{X}} \widetilde{h} \pmod{p}$. Questo è impossibile perchè $\deg(h^*) = (p-1) \cdot r$, mentre $\deg(\widetilde{h}) \leqslant \deg(h) = (p-1)\deg(f) < (p-1) \cdot r$. Pertanto la congruenza (3) non può possedere un'unica soluzione. $\square$

4. Esercizi e Complementi

4.1. Siano p un primo ed e, d due interi positivi. Mostrare che:
(a) Se la congruenza $f(X) \equiv 0 \pmod{p}$ ammette s soluzioni distinte e tutte non singolari, lo stesso è vero per la congruenza $f(X) \equiv 0 \pmod{p^e}$, per ogni $e \geqslant 1$.
(b) Se $d \mid (p-1)$, la congruenza $X^d - 1 \equiv 0 \pmod{p^e}$ ha esattamente d soluzioni per ogni $e \geqslant 1$.
[Suggerimento. **(a)**. Sia y una soluzione non singolare della congruenza

$$f(X) \equiv 0 \pmod{p^n} \qquad (*_n)$$

e sia $x = y + \bar{t}p^n$ l'unica soluzione della congruenza

$$f(X) \equiv 0 \pmod{p^{n+1}} \qquad (*_{n+1})$$

con $1 \leqslant n \leqslant e-1$. Utilizzando il Lemma 4.5 per il polinomio $f'(X)$ calcolato in x, abbiamo che

$$f'(x) = f'(y) + \bar{t}\, p^n\, f''(y) + \cdots \equiv f'(y) \pmod{p}$$

(b). Se $y^d \equiv 1 \pmod{p}$, allora $dy^{d-1} \not\equiv 0 \pmod{p}$. L'asserto discende da (a) e dalla Proposizione 4.23 (cfr. anche il successivo Lemma 5.11).]

4.2. **(a)** Verificare le seguenti congruenze polinomiali modulo un primo p:
(1) $X^{p-1} - 1 \equiv_X (X-1)(X-2)\dots[X-(p-1)] \pmod{p}$;
(2) $X^{p-2} + X^{p-3} + \cdots + X + 1 \equiv_X (X-2)\dots[X-(p-1)] \pmod{p}$.
(b) Utilizzando la (1) di (a), ridimostrare il Teorema di Wilson.
[Suggerimento. **(a)**(1) Si osservi che $(X-k) \mid (X^{p-1}-1) \pmod{p}$, per ogni $k:\ 1 \leqslant k \leqslant p-1$.
(2) segue da (1) e dal fatto che $X^{p-1} - 1 = (X-1)(X^{p-2} + X^{p-3} + \cdots + X + 1)$.
(b) Basta porre $X = p$ in (1).]

4.3. Sia $f(X) \in \mathbb{Z}[X]$ con $\deg(f) \geqslant 1$. Dimostrare che esistono infiniti primi p tali che la congruenza $f(X) \equiv 0 \pmod{p}$ è risolubile.
[Suggerimento. Se $f(X) = a_0 + a_1X + \cdots + a_nX^n$, allora $f(a_0X) = a_0(1 + Xg(X))$, con $g(X) \in \mathbb{Z}[X]$.
Questa osservazione permette di limitarci al caso in cui $a_0 = 1$ ovvero $f(X) = 1 + Xg(x)$. Se, per assurdo $f(X) \equiv 0$, fosse risolubile soltanto $\pmod{p_i}$ per $i = 1, 2, \dots, t$, allora poniamo $N := p_1p_2\cdots p_t$. Sia $h >> 0$ in modo tale che, per $M := N^h$, $|f(M)| \neq 1$.
Essendo $f(M) = 1 + Mg(M)$ deve essere $\mathrm{MCD}(f(M), M) = 1$. Pertanto se $p \mid M$ allora $p \nmid f(M)$ e quindi perveniamo ad un assurdo.]

4.4. Mostrare che, per ogni $s > 0$, esiste un intero $N > 0$ tale che la congruenza $X^2 \equiv 1 \pmod{N}$ ha più di s soluzioni.
[Suggerimento. Se p è un primo dispari, $X^2 \equiv 1 \pmod{p}$ ha le due soluzioni $1, p-1$. Quindi, se $p_1, \dots, p_r$ sono primi distinti, $X^2 \equiv 1 \pmod{p_1 \cdots p_r}$ ha esattamente 2^r soluzioni distinte. Basta trovare r tale che $2^r > s$ e porre $N = p_1 \cdots p_r$.]

4.5. Verificare che il Corollario 4.17 non è più valido se si sostituiscono p e $p-1$ rispettivamente con n e $\varphi(n)$ (con $n \in \mathbb{Z}, n \geqslant 2$).
[Suggerimento. Si scelga, ad esempio, $n = 4$ e $f(X) = X^3 - X$.]

4.6. Siano $p, f(X)$ e t definiti come nella Proposizione 4.23.
Posto $F = \mathrm{MCD}(f, X^p - X)$, è vero che $t = \deg_p(F)$?
[Suggerimento. La risposta è negativa: si ponga $p = 5$ ed $f(X) = (X+2)(X+1)^2$ da cui $t = 2$ e $F(X) = X + 1$, perché

$$\begin{aligned} X^5 - X = X(X^4 - 1) = \\ = X(X^2 - 1)(X^2 + 1) = \\ = X(X + 1)(X - 1)(X^2 + 1).] \end{aligned}$$

4.7. (Teorema di Warning) Sia $f \in \mathbb{Z}[X_1, \ldots, X_r]$, con $\deg(f) < r$, e sia p un numero primo. La congruenza $f \equiv 0 \pmod{p}$ ha un numero di soluzioni (in $\mathbb{Z}^r$) divisibile per p.
[Suggerimento. Seguire un'argomentazione simile a quella utilizzata per dimostrare il Teorema di Chevalley. Precisamente se $\underline{a}_i = (a_{i1}, \ldots, a_{ir})$, per $i = 1, \ldots, s$, sono le soluzioni della congruenza data, considerare il polinomio:

$$h^*(X_1, \ldots, X_r) := \sum_{i=1}^{s} \prod_{j=1}^{r} \left(1 - (X_j - a_{ij})^{p-1}\right) .]$$

4.8. Determinare le soluzioni della congruenza:

$$f(X) := X^2 + X + 7 \equiv 0 \pmod{27}.$$

[Soluzione. La congruenza:

$$X^2 + X + 7 \equiv 0 \pmod{3} \tag{$*_1$}$$

ha un'unica soluzione $y \equiv 1 \pmod{3}$.
Consideriamo la congruenza:

$$X^2 + X + 7 \equiv 0 \pmod{3^2}. \tag{$*_2$}$$

Osserviamo che $f'(X) = 2X + 1$, quindi $f'(y) \equiv 0 \pmod{3}$. Inoltre, $f(1) \equiv 0 \pmod{9}$, dunque gli elementi $y_1 = 1,\ y_2 = 1 + 3 = 4,\ y_3 = 1 + 2 \cdot 3 = 7$ sono soluzioni di $(*_2)$.
Per calcolare le soluzioni della congruenza data:

$$X^2 + X + 7 \equiv 0 \pmod{3^3} \tag{$*_3$}$$

osserviamo che:

$$\begin{aligned} f'(y_1) = 3 \equiv 0 \pmod{3} \qquad & f(y_1) \equiv 9 \pmod{27} \\ f'(y_2) = 9 \equiv 0 \pmod{3} \qquad & f(y_2) = 27 \equiv 0 \pmod{27} \\ f'(y_3) = 15 \equiv 0 \pmod{3} \qquad & f(y_3) = 63 \equiv 9 \pmod{27}. \end{aligned}$$

Quindi, y_1 non determina soluzioni di $(*_3)$ (cioè non esiste nessuna soluzione t della congruenza

$$3T \equiv -\frac{9}{9} = -1 \pmod{3} \tag{$\bullet_1$}$$

e quindi nessun intero $x = y_1 + t \cdot 3^2$ è tale che $f(x) \equiv 0 \pmod{27}$). Mentre, y_2 determina tre soluzioni di $(*_3)$ date da:

$$x_{2,1} = y_2 + 0 \cdot 3^2 = 4,\ x_{2,2} = y_2 + 1 \cdot 3^2 = 13,\ x_{2,3} = y_2 + 2 \cdot 3^2 = 22 \pmod{27}$$

(dal momento che la congruenza

$$9T \equiv -\frac{27}{9} = -3 \pmod{3} \qquad (\bullet_2)$$

è risolubile per $t = 0, 1, 2 \pmod 3$).
Infine, y_3 non determina soluzioni di $(*_3)$ (in quanto la congruenza

$$15T \equiv -\frac{63}{9} \equiv -1 \pmod{3} \qquad (\bullet_3)$$

non è risolubile).
In definitiva, le soluzioni della congruenza assegnata sono: $x = 4, 13, 22 \pmod{27}$.]

5 Radici primitive dell'unità e congruenze del tipo $\mathbf{X^m \equiv a} \pmod{n}$

Oggetto di questo paragrafo è lo studio della risolubilità di congruenze del tipo:

$$X^m \equiv a \pmod{n}$$

con $m, n, a \in \mathbb{Z}$ ed $m, n > 0$. Per l'effettiva ricerca delle soluzioni di tali congruenze svilupperemo, in modo essenziale, la teoria delle radici primitive dell'unità e la teoria degli indici.

I risultati qui esposti sono stati in gran parte ottenuti da Gauss, che li ha trattati (più o meno nella forma in cui essi sono stati qui presentati) nel suo celebre *Disquisitiones Arithmeticae* (cfr. [G]). Tuttavia, alcuni teoremi furono congetturati e in parte dimostrati precedentemente: ad esempio il Teorema dell'esistenza di radici primitive modulo un primo fu congetturato da Lambert nel 1769 e dimostrato da Legendre nel 1785. Il termine *radice primitiva* fu introdotto da Euler nel 1773.

Definizione 5.1. Siano $a, n \in \mathbb{Z}$ tali che $n > 0$ e $\mathrm{MCD}(a, n) = 1$. Si chiama *ordine di* $a \pmod{n}$ (e si scrive $\mathrm{ord}_n(a)$) il minimo intero positivo k per cui risulti

$$a^k \equiv 1 \pmod{n}.$$

Osservazione 5.2. È bene sottolineare che la *definizione precedente ha senso se, e soltanto se,* $\mathrm{MCD}(a, n) = 1$.
Infatti, se $\mathrm{MCD}(a, n) \neq 1$ la congruenza $aX \equiv 1 \pmod{n}$ non è risolubile (cfr. Teorema 2.2) e quindi $a^k \not\equiv 1 \pmod{n}$ per ogni $k \geqslant 1$; viceversa, se $\mathrm{MCD}(a, n) = 1$ l'asserto è immediata conseguenza del Teorema di Euler-Fermat (cfr. Teorema 3.7).

D'ora in poi, quindi, nel considerare l'ordine (mod n) di un elemento a, $\mathrm{ord}_n(a)$, *supporremo sempre tacitamente che* $\mathrm{MCD}(a, n) = 1$.
Vale, innanzi tutto, il seguente risultato (di immediata verifica):

Proposizione 5.3. *Siano* $a, b, n \in \mathbb{Z}, n > 0$. *Se* $a \equiv b \pmod{n}$, *allora* $\mathrm{ord}_n(a) = \mathrm{ord}_n(b)$. □

Si noti che il viceversa dell'enunciato precedente è falso: ad esempio $\mathrm{ord}_5(2) = 4 = \mathrm{ord}_5(3)$ e $2 \not\equiv 3 \pmod{5}$.

Proposizione 5.4. *Siano* $a, b, n, m \in \mathbb{Z}, n > 0$ *e* $m > 0$. *Risulta:*

(1) $a^m \equiv 1 \pmod{n} \iff \mathrm{ord}_n(a) \mid m$;

(2) $\mathrm{ord}_n(a) \mid \varphi(n)$ *(cfr. Definizione 2.9);*

(3) $\mathrm{ord}_n(a^m) = \mathrm{ord}_n(a)/\mathrm{MCD}(m, \mathrm{ord}_n(a))$. *Ne segue che:*
$\mathrm{ord}_n(a^m) = \mathrm{ord}_n(a) \iff \mathrm{MCD}(m, \mathrm{ord}_n(a)) = 1$;

(4) $\mathrm{ord}_n(a) = \mathrm{ord}_n(a^*)$, *dove* a^* *è un inverso aritmetico di* $a \pmod n$*;*

(5) $\mathrm{MCD}(\mathrm{ord}_n(a), \mathrm{ord}_n(b)) = 1 \Rightarrow \mathrm{ord}_n(ab) = \mathrm{ord}_n(a) \cdot \mathrm{ord}_n(b)$.

Dimostrazione. (1) ($\Leftarrow$). È ovvio.
($\Rightarrow$). Si ponga $h := \mathrm{ord}_n(a)$ e si operi la divisione euclidea:

$$m = qh + r, \quad 0 \leqslant r < h.$$

Allora, $1 \equiv a^m = (a^h)^q \cdot a^r \equiv a^r \pmod n$ (in quanto $a^h \equiv 1 \pmod n$); per la minimalità dell'ordine, deve risultare $r = 0$ e dunque $h \mid m$.
(2) È un'immediata conseguenza di (1) e del Teorema 3.7.
(3) Si ponga $h := \mathrm{ord}_n(a)$ e $d := \mathrm{MCD}(m, h)$. Se k è un intero positivo, da (1) si ha:

$$(a^m)^k = a^{mk} \equiv 1 \pmod n \iff h \mid mk \iff \frac{h}{d} \mid \frac{m}{d} \cdot k.$$

Poiché $\mathrm{MCD}(h/d, m/d) = 1$, allora $(h/d) \mid k$; quindi h/d è il minimo intero positivo k per cui $(a^m)^k \equiv 1 \pmod n$, cioè $\mathrm{ord}_n(a^m) = h/d$.
(4) Si ponga $h := \mathrm{ord}_n(a)$ e $h^* := \mathrm{ord}_n(a^*)$. Si ha:

$$(a^*)^h = 1 \cdot (a^*)^h \equiv a^h \cdot (a^*)^h = (aa^*)^h \equiv 1 \pmod n$$

e dunque, in base a (1), $h^* \mid h$. Procedendo in modo analogo, si prova che $h \mid h^*$ e dunque: $h = h^*$.
(5) Si ponga $h_1 := \mathrm{ord}_n(a)$ e $h_2 := \mathrm{ord}_n(b)$ e $h := \mathrm{ord}_n(ab)$. Poiché $(ab)^{h_1 h_2} \equiv 1 \pmod n$, in base al punto (1), si ha che $h \mid h_1 h_2$. D'altra parte:

$$a^h b^h = (ab)^h \equiv 1 \pmod n \text{ e quindi } a^h \equiv (b^h)^* \pmod n.$$

Da (4) segue che $\mathrm{ord}_n(a^h) = \mathrm{ord}_n(b^h)$ e quindi da (3):

$$\frac{h_1}{\mathrm{MCD}(h_1, h)} = \frac{h_2}{\mathrm{MCD}(h_2, h)}.$$

Poiché, per ipotesi, $\mathrm{MCD}(h_1, h_2) = 1$, si ha che:

$$h_1 \mid \mathrm{MCD}(h_1, h) \text{ e } h_2 \mid \mathrm{MCD}(h_2, h).$$

Pertanto $h_1 \mid h$ e $h_2 \mid h$ e, quindi, $h_1 h_2 \mid h$. □

È immediato verificare che l'enunciato **(5)** della proposizione precedente vale, più in generale, per $r \geqslant 2$ interi i cui ordini siano a due a due relativamente primi.

Corollario 5.5. *Siano* $a, n \in \mathbb{Z}$ *con* $n > 0$ *e* $MCD(a, n) = 1$*. Allora:*

$$a^i \equiv a^j \pmod n \iff i \equiv j \pmod{\mathrm{ord}_n(a)}.$$

Dimostrazione. Sia $h := \mathrm{ord}_n(a)$.
($\Leftarrow$)**.** Se $i - j = th$ per qualche $t \in \mathbb{Z}$, poiché $a^h \equiv 1 \pmod{n}$, allora:

$$a^i = a^{j+th} = a^j(a^h)^t \equiv a^j \pmod{n}.$$

($\Rightarrow$)**.** Supponiamo per fissare le idee che $j \geqslant i$, con $a^i \equiv a^j \pmod{n}$. Dal momento che $\mathrm{MCD}(a, n) = 1$ allora anche $\mathrm{MCD}(a^i, n) = 1$. Inoltre:

$$a^j = a^i a^{j-i} \equiv a^i \pmod{n}.$$

Moltiplicando ambo i membri della congruenza per l'inverso aritmetico di $a^i \pmod{n}$, otteniamo che

$$a^{j-i} \equiv 1 \pmod{n},$$

quindi $h \mid (j - i)$, cioè $i \equiv j \pmod{h}$. □

Ad esempio $3^6 \equiv 3^{14} \pmod{5}$, perché $\mathrm{ord}_5(3) = 4$.

Il seguente risultato approfondisce i legami tra l'ordine e la funzione φ di Euler (cfr. Proposizione 5.4(2)) ed introduce la successiva definizione di radice primitiva dell'unità.

Lemma 5.6. *Siano $a, n \in \mathbb{Z}, n > 0$. Le seguenti affermazioni sono equivalenti:*

(i) $\mathrm{ord}_n(a) = \varphi(n)$*;*

(ii) $\{1, a, a^2, \ldots, a^{\varphi(n)-1}\}$ *è un sistema ridotto di residui (modulo n).*

Dimostrazione. (i) $\Rightarrow$ (ii). Certamente $\mathrm{MCD}(a^k, n) = 1$, per ogni k tale che $0 \leqslant k \leqslant \varphi(n) - 1$.
Inoltre, se $a^h \equiv a^k \pmod{n}$ con $0 \leqslant h < k \leqslant \varphi(n) - 1$, si avrebbe $a^{k-h} \equiv 1 \pmod{n}$ con $1 \leqslant k - h \leqslant \varphi(n) - 1$ e ciò è assurdo. La tesi è dunque ovvia (cfr. anche l'Esercizio 2.11(a)).
(ii) $\Rightarrow$ (i). Ovviamente $a^{\varphi(n)} \equiv 1 \pmod{n}$ (cfr. Teorema 3.7); inoltre, per ipotesi, $a^k \not\equiv 1 \pmod{n}$ per ogni k tale che $1 \leqslant k \leqslant \varphi(n) - 1$. Dunque $\mathrm{ord}_n(a) = \varphi(n)$ □

Definizione 5.7. Sia $n \in \mathbb{Z}, n > 0$. Si chiama *radice primitiva dell'unità (modulo n)* un intero a verificante una delle due condizioni (equivalenti) del Lemma 5.6.

Ad esempio, per $n = 5$, allora 2 è una radice primitiva (modulo 5), in quanto $\{2, 2^2, 2^3, 2^4\}$ è un sistema ridotto di residui (modulo 5), ovvero $\mathrm{ord}_5(2) = 4 = \varphi(5)$.
Se $n = 8$, si può verificare direttamente che non esistono radici primitive (modulo 8).

Proposizione 5.8. *Sia n un intero positivo tale che esiste (almeno) una radice primitiva (modulo n). Allora, esistono esattamente $\varphi(\varphi(n))$ radici primitive distinte (modulo n) (cioè, non congruenti (modulo n)).*

Dimostrazione. Sia a una radice primitiva (mod n).
Poiché $S^* := \{a, a^2, \ldots, a^{\varphi(n)}\}$ è un sistema ridotto di residui (mod n), ogni radice primitiva (mod n) è congrua ad un (ed un solo) elemento di S^* e, inoltre, $a^k \in S^*$ è una radice primitiva (mod n) se e soltanto se si ha che $\mathrm{ord}_n(a^k) = \varphi(n) = \mathrm{ord}_n(a)$. In base alla Proposizione 5.4(3), le radici primitive (mod n) sono in corrispondenza biunivoca con gli interi k tali che $1 \leqslant k \leqslant \varphi(n)$ e $\mathrm{MCD}(k, \varphi(n)) = 1$, cioè sono in numero di $\varphi(\varphi(n))$. □

Osservazione 5.9. Sia $n \in \mathbb{Z}, n > 0$ ed U_n il gruppo (moltiplicativo) delle unità dell'anello $\mathbb{Z}/n\mathbb{Z}$ (cfr. anche Osservazione 2.8). È chiaro che:

$$U_n = \{\bar{k} = k + n\mathbb{Z} \mid k \in \mathbb{Z} \text{ e } \mathrm{MCD}(k, n) = 1\},$$

e dunque $\#(U_n) = \varphi(n)$. Invitiamo il lettore a tradurre le nozioni introdotte in questo paragrafo nel linguaggio gruppale, con riferimento al gruppo moltiplicativo U_n.

Ci occuperemo ora del problema dell'esistenza di radici primitive (modulo n), esaminando dapprima il caso in cui $n = p$ sia un numero primo. Vale in proposito il seguente risultato:

Teorema 5.10. *Se p è un numero primo, esiste sempre una radice primitiva (modulo p). Più precisamente, esistono esattamente $\varphi(p-1)$ radici primitive (modulo p), non congruenti (modulo p).*

Del Teorema 5.10 daremo due differenti dimostrazioni. Ad esse premettiamo alcuni risultati utili per il seguito.

Lemma 5.11. *Sia p un primo e d un intero positivo tale che $d \mid (p-1)$. La congruenza:*

$$X^d \equiv 1 \pmod{p}$$

ha esattamente d soluzioni non congruenti (modulo p).

Dimostrazione. Verifichiamo, innanzitutto, che $(X^d - 1) \mid (X^p - X)$.
Per ipotesi esiste $k \in \mathbb{Z}, k > 0$ tale che $dk = p - 1$. Dunque, è subito visto che:

$$X^p - X = X(X^{dk} - 1) = X(X^d - 1)(X^{d(k-1)} + X^{d(k-2)} + \cdots + X^d + 1). \square$$

La conclusione discende dalla Proposizione 4.23.
Alla conclusione si può pervenire anche utilizzando il Teorema di Lagrange. Infatti, le congruenze (mod p), associate a ciascuno dei polinomi a secondo membro della precedente decomposizione di $X^p - X$, hanno ciascuna un numero di soluzioni minore od uguale del grado del polinomio. Poiché $X^p - X \equiv 0 \pmod{p}$ ha esattamente p soluzioni allora, in particolare, $X^d - 1 \equiv 0 \pmod{p}$ non può avere meno di d soluzioni (mod p).

Osservazione 5.12. (a). Se $d \nmid (p-1)$, la congruenza $X^d \equiv 1 \pmod{p}$ (che è sempre banalmente risolubile) ammette un numero di soluzioni distinte inferiori a d.
Ad esempio, posto $d = 4$ e $p = 7$, si verifica subito che $X^4 \equiv 1 \pmod{7}$ ha soltanto due soluzioni (cioè 1 e 6) (mod 7).
Più precisamente, se $t := \mathrm{MCD}(d, p-1)$ le soluzioni distinte della congruenza in questione sono esattamente t; tale fatto può essere provato utilizzando la Proposizione 4.23 oppure come semplice conseguenza di un successivo teorema (cfr. Teorema 5.18).
(b) Se $d \nmid (p-1)$, nessun intero ha ordine d (modulo p); infatti $\mathrm{ord}_p(a) \mid \varphi(p) = p-1$ (cfr. Proposizione 5.4(2)).

Teorema 5.13. *Sia p un primo e d un intero positivo tale che si abbia: $d \mid (p-1)$. Allora, esistono esattamente $\varphi(d)$ interi non congruenti* (mod p) *ed aventi ordine d* (mod p).

Dimostrazione. Sia $S^* = \{1, 2, \ldots, p-1\}$ il sistema ridotto di residui minimo positivo (mod p) e, per ogni intero positivo d tale che $d \mid (p-1)$, si ponga:

$$\psi(d) := \#\{k \in S^* \mid \mathrm{ord}_p(k) = d\}.$$

Vogliamo dimostrare che $\varphi(d) = \psi(d)$.
Poiché l'ordine di ogni elemento di S^* è un divisore di $\varphi(p) = p-1$, è chiaro che:

$$p - 1 = \sum_{d \mid (p-1)} \psi(d). \tag{1}$$

Consideriamo ora, per ogni intero positivo d tale che $d \mid (p-1)$, i seguenti insiemi:

$$S_d^* := \{k \in S^* : \mathrm{MCD}(k, p-1) = d\}$$
$$\tilde{S}_d := \{k' \in \mathbb{Z} : 1 \leqslant k' \leqslant \frac{p-1}{d} \text{ e } \mathrm{MCD}(k', \frac{p-1}{d}) = 1\}.$$

È chiaro che la famiglia $\{S_d^* : d \mid (p-1)\}$ costituisce una partizione di S^* ed è altresì chiaro che S_d^* e $\tilde{S}_d$ sono equipotenti (l'applicazione $f : S_d^* \longrightarrow \tilde{S}_d$ tale che $f(k) = k/d$ è certamente biiettiva).
Ne segue che:

$$\#(S_d^*) = \#(\tilde{S}_d) = \varphi\left(\frac{p-1}{d}\right)$$

e, dunque, che

$$p - 1 = \sum_{d \mid (p-1)} \varphi\left(\frac{p-1}{d}\right) = \sum_{d \mid (p-1)} \varphi(d) \tag{2}$$

(L'ultima uguaglianza sussiste perché $(p-1)/d$ descrive, al variare di d, l'insieme di tutti i divisori di $p-1$, cioè:

$$\{d : d \mid (p-1), 1 \leqslant d \leqslant p-1\} = \{(p-1)/d : d \mid (p-1), 1 \leqslant d \leqslant p-1\}.)$$

Confrontando (2) con (1) si ha:

$$\sum_{d|(p-1)} \psi(d) = \sum_{d|(p-1)} \varphi(d)$$

e, quindi, per dimostrare che $\psi(d) = \varphi(d)$, basta verificare che, per ogni divisore d di $p-1$, si abbia $\psi(d) \leqslant \varphi(d)$.
Supponiamo che $\psi(d) > 0$, per ogni d tale che $d \mid (p-1)$, (altrimenti la diseguaglianza è ovvia) e dunque sia $a \in S^*$ tale che $\mathrm{ord}_p(a) = d$. L'insieme $T := \{a, a^2, \ldots, a^d\}$ è costituito da d interi non congrui $\pmod p$ che sono soluzioni della congruenza:

$$X^d \equiv 1 \pmod p$$

(infatti, $(a^h)^d = (a^d)^h \equiv 1 \pmod p$, per ogni h tale che $1 \leqslant h \leqslant d$).
Il Lemma 5.11 ci assicura che la congruenza in questione ha esattamente d soluzioni non congruenti $(\mathrm{mod}\ p)$: quindi ogni intero di S^* di ordine d $(\mathrm{mod}\ p)$ è necessariamente congruente $\pmod p$ ad un elemento di T. Dunque (cfr. Proposizione 5.4(3)):

$$\begin{aligned}\psi(d) &\leqslant \#\{a^k \in T \ :\ \mathrm{ord}(a^k) = d\} = \#\{a^k \in T \ :\ \mathrm{MCD}(k,d) = 1\} = \\ &= \#\{k \in \mathbb{Z} \ :\ 1 \leqslant k \leqslant d \text{ e } \mathrm{MCD}(k,d) = 1\} = \varphi(d) \quad \square\end{aligned}$$

I Dimostrazione del Teorema 5.10. È una conseguenza immediata del Teorema 5.13. $\square$

II Dimostrazione del Teorema 5.10 (senza far uso del Teorema 5.13)**.** In base alla Proposizione 5.8, basta dimostrare che esiste una radice primitiva $(\mathrm{mod}\ p)$.
Se $p = 2$, ogni intero dispari è una radice primitiva (mod 2).
Sia quindi p dispari e supponiamo che $p-1$ ammetta la seguente fattorizzazione in numeri primi:

$$p - 1 = q_1^{e_1} \cdots q_r^{e_r} \quad (\text{con } e_i \geqslant 1,\ 1 \leqslant i \leqslant r).$$

In base alla Proposizione 5.4(5), basta verificare che per ogni i, con $1 \leqslant i \leqslant r$, esiste un intero a_i, tale che $\mathrm{ord}_p(a_i) = q_i^{e_i}$; in tal caso, infatti, l'intero $\prod_{i=1}^r a_i$ ha ordine $p-1$ ed è quindi una radice primitiva $(\mathrm{mod}\ p)$.

Per semplicità di notazione, fissato comunque $i, 1 \leqslant i \leqslant r$, poniamo $q_i = q, e_i = e$. Poiché $q^e \mid (p-1)$ e quindi anche $q^{e-1} \mid (p-1)$, le congruenze:

$$X^{q^e} \equiv 1 \pmod p \quad \text{e} \quad X^{q^{e-1}} \equiv 1 \pmod p$$

ammettono rispettivamente q^e e q^{e-1} soluzioni distinte (cfr. Lemma 5.11). Dunque, essendo $q^{e-1} < q^e$, è possibile determinare $a \in \mathbb{Z}$ che sia soluzione della prima congruenza ma non della seconda, cioè:

$$a^{q^e} \equiv 1 \pmod{p} \quad \text{e} \quad a^{q^{e-1}} \not\equiv 1 \pmod{p}.$$

Si tratta ora di verificare che $\mathrm{ord}_p(a) = q^e$ e cioè che $a^k \not\equiv 1 \pmod{p}$ per ogni k tale che $1 \leqslant k \lneqq q^e$. Per assurdo, sia $h := \mathrm{ord}_p(a),\ h < q^e$. Allora $h \mid q^e$ e quindi $h = q^f$, con $0 \leqslant f < e$; pertanto $q^{e-1} = q^{e-1-f}h$ e quindi

$$a^{q^{e-1}} = (a^h)^{q^{e-1-f}} \equiv 1 \pmod{p}$$

il che è assurdo. □

Osservazione 5.14. La seconda dimostrazione del Teorema 5.10 ha il vantaggio, rispetto alla prima, di suggerire un metodo operativo per la ricerca delle radici primitive. Tale metodo tuttavia non è in generale di un effettivo aiuto pratico: infatti, se p è grande, non ci sono metodi pratici per determinare la decomposizione in fattori primi di $p-1$, e poi per risolvere una congruenza del tipo $X^{q^e} \equiv 1 \pmod{p}$. Tuttavia, le idee sopra esposte permettono spesso di semplificare i termini del problema, come è suggerito dal seguente esempio.

Esempio 5.15. Sia $p = 23$. Ci proponiamo di calcolare le radici primitive (mod 23), che, in base al Teorema 5.10, sono in numero di $\varphi(22) = 10$.
Per ogni intero a tale che $23 \nmid a$, $\mathrm{ord}_{23}(a) \mid 22$ e dunque ord_a può assumere uno dei seguenti valori: $1, 2, 11, 22$.
Verifichiamo che 21 è una radice primitiva (mod 23). Infatti, si ha:

$$2^1 \not\equiv 1 \pmod{23},\ 2^2 \not\equiv 1 \pmod{23},\ 2^{2^2} \equiv 16 \not\equiv 1 \pmod{23},$$

$$2^{2^3} \equiv 3 \not\equiv 1 \pmod{23},\ 2^{11} = 2^{2^3} \cdot 2^2 \cdot 2 \equiv 3 \cdot 4 \cdot 2 \equiv 1 \pmod{23}$$

e $(-1)^1 \not\equiv 1 \pmod{23},\ (-1)^2 \equiv 1 \pmod{23}$.
Ne segue che $\mathrm{ord}_{23}(2) = 11$ e $\mathrm{ord}_{23}(-1) = \mathrm{ord}_{23}(22) = 2$ e quindi, essendo $\mathrm{MCD}(11, 2) = 1$, allora (cfr. Proposizione 5.4(5)) si ha:

$$\mathrm{ord}_{23}(21) = \mathrm{ord}_{23}(-2) = \mathrm{ord}_{23}(-1) \cdot \mathrm{ord}_{23}(2) = 2 \cdot 11 = 22.$$

Le radici primitive (mod 23) sono quindi date (a meno della congruenza (mod 23)) dall'insieme:

$$\{(-2)^k | 1 \leqslant k \leqslant 22,\ \mathrm{MCD}(k, 22) = 1\} =$$

$$= \{(-2)^k | k = 1, 3, 5, 7, 9, 13, 15, 17, 19, 21\},$$

e cioè (come si verifica con semplici calcoli):

$$\{21, 15, 14, 10, 17, 19, 7, 5, 20, 11\}.$$

Il metodo precedente per determinare una radice primitiva (modulo 23) è suggerito dalla II dimostrazione del Teorema 5.10. Poiché $22 = 2 \cdot 11$, basta determinare una soluzione di $X^2 \equiv 1 \pmod{23}$ che *non* sia soluzione di $X \equiv 1 \pmod{23}$ (ad esempio, -1) ed una soluzione di $X^{11} \equiv 1 \pmod{23}$ che *non* sia soluzione di $X^k \equiv 1 \pmod{23}$, con $1 \leqslant k \leqslant 10$, (ad esempio, 2). Dunque $a = (-1) \cdot 2 = -2 \equiv 21 \pmod{23}$ è una radice primitiva $\pmod{23}$.

Il calcolo di una radice primitiva $\pmod{p}$, con p primo, può essere effettuato anche con un metodo algoritmico semplice indicato da Gauss [G, Art. 73 e 74].

Algoritmo di Gauss per il calcolo di una radice primitiva modulo un intero primo p

Passo 1. Scegliere un intero a, $2 \leqslant a \leqslant p-1$, e calcolare $\mathrm{ord}_p(a)$. Se $\mathrm{ord}_p(a) = p-1$, allora a è una radice primitiva $\pmod{p}$.

Passo 2. Se $d := \mathrm{ord}_p(a) \neq p-1$, allora scegliere un intero b, con $2 \leqslant b \leqslant p-1, b \not\equiv a^i$ per ogni $i, 1 \leqslant i \leqslant d$. Calcolare $t := \mathrm{ord}_p(b)$ e mostrare che $t \nmid d$. Se $t = p-1$, allora b è una radice primitiva $\pmod{p}$.

Passo 3. Se $t \neq p-1$, sia $d_1 := \mathrm{mcm}(d,t)$. Allora $d_1 = d't'$ con $d' \mid d, t' \mid t$ e $\mathrm{MCD}(d', t') = 1$.
Se $\alpha \equiv a^{\frac{d}{d'}} \pmod{p}$ e $\beta \equiv b^{\frac{t}{t'}} \pmod{p}$ allora $a_1 := \alpha\beta$ è tale che $\mathrm{ord}_p(a_1) = d_1$ (perché $\mathrm{ord}_p(\alpha) = d'$ e $\mathrm{ord}_p(\beta) = t'$). Mostrare che $d_1 > d$. Se $d_1 = p-1$, allora a_1 è una radice primitiva. Se $d_1 \neq p-1$, allora si ritorna al Passo 2. Il procedimento termina dopo un numero finito di passi e permette di trovare una radice primitiva $\pmod{p}$ che non è necessariamente la più piccola radice primitiva positiva.

Esempio 5.16. Si prenda $p = 41, a = 10, b = 9$. È subito visto che $\mathrm{ord}_{41}(a) = 5$. Sia $b = 9$ con $b \not\equiv 10^i$ per ogni $1 \leqslant i \leqslant 5$. Si vede che $\mathrm{ord}_{41}(9) = 4$. Dunque $d = 5$, $t = 4$ e quindi $d_1 = \mathrm{mcm}(5,4) = 20$. Pertanto $20 = 5 \cdot 4$ con $\mathrm{MCD}(5,4) = 1$, quindi $d' = d = 5$, $t' = t = 4$. Da ciò segue che $\alpha = a = 10$, $\beta = b = 9$ e dunque $a_1 = 10 \cdot 9 \equiv 8 \pmod{41}$, con $\mathrm{ord}_{41}(8) = 5 \cdot 4 = 20$. Ripetiamo il Passo 2. Sia $b_1 = 3$ con $3 \not\equiv 8^i$, per ogni $1 \leqslant i \leqslant 20$. Si vede facilmente che $\mathrm{ord}_{41}(3) = 8$. Essendo $\mathrm{mcm}(20,8) = 40 = 5 \cdot 8$ con $\mathrm{MCD}(5,8) = 1$, allora i nuovi α e β sono dati da $8^{\frac{20}{5}}$ e $3^{\frac{8}{8}}$. Quindi $8^4 \cdot 3 \equiv 29 \pmod{41}$ con $\mathrm{ord}_{41}(29) = \mathrm{ord}_{41}(8^4) \cdot \mathrm{ord}_{41}(3) = 5 \cdot 8 = 40$, cioè 29 è una radice primitiva (mod 41). Si noti che 29 non è la più piccola radice primitiva $\pmod{41}$, infatti si verifica facilmente che 6 è la più piccola radice primitiva positiva (mod 41).

Come vedremo tra breve, l'esistenza di una radice primitiva (modulo n)

permette di risolvere facilmente congruenze del tipo:

$$X^m \equiv a \pmod{n}, \text{ con } \mathrm{MCD}(a,n) = 1 \qquad (\bullet)$$

D'altra parte, in virtù di quanto esposto nel Paragrafo 4, lo studio di congruenze di tipo $(\bullet)$ può essere ricondotto a quello di congruenze del tipo:

$$X^m \equiv a \pmod{p} \qquad (\star)$$

con p primo e $p \mid n$. Dunque, tramite tale riduzione, l'esistenza di radici primitive modulo un primo sarà sufficiente per la soluzione di congruenze del tipo $(\bullet)$, in quanto daremo un metodo effettivo di risoluzione di ogni congruenza del tipo $(\star)$, facendo uso di una radice primitiva $\pmod{p}$.
Per completezza, tuttavia, desideriamo anche accennare al problema dell'esistenza di radici primitive modulo un intero positivo arbitrario. Vale in proposito il seguente risultato:

Teorema 5.17. (Gauss, 1801). *Sia n un intero positivo. Esiste una radice primitiva $\pmod{n}$ se, e soltanto se, n è uno dei seguenti interi:*

$$2, 4, p^k, 2p^k$$

con $k \geqslant 1$ e p primo dispari.

Dimostrazione. Cfr. Esercizio 5.15 e seguenti $\square$

Pertanto, dal teorema precedente discende che $8, 12, 15$ e 16 sono i soli interi $n < 20$ che non possiedono radici primitive.

Veniamo ora al risultato centrale di questo paragrafo.

Teorema 5.18. *Sia p un numero primo, m un intero positivo ed a un intero tale che $p \nmid a$; sia inoltre r una radice primitiva (mod p) ed h l'intero tale che:*

$$r^h \equiv a \pmod{p}, \quad 1 \leqslant h \leqslant p-1$$

(h è univocamente determinato da a ed r ed è detto indice di a rispetto ad r*; in simboli* $\mathrm{ind}_r(a) := h$*). Posto $d := \mathrm{MCD}(m, p-1)$, allora la congruenza*

$$X^m \equiv a \pmod{p} \qquad (\star)$$

è risolubile se, e soltanto se, $d \mid h$.
In questo caso, la congruenza $(\star)$ ha esattamente d soluzioni distinte.

Dimostrazione. Poichè $p \nmid a$, ogni (eventuale) soluzione di $(\star)$ non può essere divisibile per p e, dunque, è congruente (mod p) a:

$$r^y, \text{ con } y \in \mathbb{Z},\ 1 \leqslant y \leqslant p-1.$$

Dunque $(\star)$ è risolubile se, e soltanto se, esiste un intero y $(1 \leqslant y \leqslant p-1)$ che risolve la congruenza:

$$r^{my} \equiv r^h \pmod{p},$$

Pertanto, per il Corollario 5.5, $(\star)$ è risolubile se, e soltanto se, $my \equiv h \pmod{\mathrm{ord}_p(r)}$, cioè se, e soltanto se, la congruenza lineare

$$mY \equiv h \pmod{p-1}$$

è risolubile.
La conclusione discende immediatamente dal Teorema 2.2. □

Il seguente criterio può essere attribuito ad Euler anche se la dimostrazione originaria riguardava il caso $m = 2$, (cfr. la successiva Proposizione 6.5).

Corollario 5.19. (Criterio di Euler). *Con le notazioni ed ipotesi del Teorema 5.18, la congruenza $(\star)$ è risolubile se, e soltanto se, risulta:*

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}.$$

Dimostrazione. Siano r, h come nell'enunciato del Teorema 5.18. Risulta:

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p} \iff r^{\frac{h(p-1)}{d}} \equiv 1 \pmod{p} \iff$$
$$\iff \frac{h(p-1)}{d} \equiv 0 \pmod{p-1}.$$

L'ultima condizione è ovviamente equivalente al fatto che $d \mid h$ e dunque la tesi discende immediatamente dal Teorema 5.18. □

Corollario 5.20. *Sia p un primo ed m un intero positivo. La congruenza:*

$$X^m \equiv a \pmod{p} \qquad (\star)$$

è risolubile esattamente per $1 + \left[\frac{(p-1)}{\mathrm{MCD}(m,\, p-1)}\right]$ valori distinti (mod p) di a. In particolare, $(\star)$ è risolubile per p valori distinti di $a \pmod{p}$ se, e soltanto se, $\mathrm{MCD}(m, p-1) = 1$.

Dimostrazione. Sia $a \not\equiv 0 \pmod{p}$ ed r una radice primitiva (modulo p). Tenuto conto del Teorema 5.18, gli interi a distinti (mod p) per i quali $(\star)$ è risolubile corrispondono agli esponenti h tali che $d := \mathrm{MCD}(m, p-1) \mid h$ e $1 \leqslant h \leqslant p-1$. Tali interi sono esattamente

$$d, 2d, \ldots, sd \quad \text{con } sd = p-1$$

e pertanto sono in numero di $\frac{p-1}{d}$.
Se $a \equiv 0 \pmod{p}$ allora la congruenza $(\star)$ è risolubile (avendo come soluzione la soluzione banale $x = 0$): dunque complessivamente $(\star)$ è risolubile per $1 + \left[\frac{(p-1)}{d}\right]$ valori distinti (mod p) di a.
L'ultima asserzione è, ormai, del tutto ovvia. □

La tecnica dimostrativa del Teorema 5.18 può essere applicata anche e direttamente per la soluzione di congruenze del tipo:

$$X^m \equiv a \pmod{n}, \text{ con } \mathrm{MCD}(a,n) = 1 \qquad (\bullet)$$

dove n è un intero positivo per il quale esista una radice primitiva $\pmod{n}$. A tale scopo è opportuno premettere la definizione ed alcune proprietà elementari degli "indici".

Definizione 5.21. Sia n un intero positivo tale che esista una radice primitiva $r \pmod{n}$ (cfr. Teorema 5.17). Si verifica immediatamente che l'insieme $S^* := \{r, r^2, \ldots, r^{\varphi(n)}\}$ è un sistema ridotto di residui $\pmod{n}$ e, dunque, per ogni $a \in \mathbb{Z}$ tale che $\mathrm{MCD}(a,n) = 1$ esiste un unico $r^h \in S^*$ $(1 \leqslant h \leqslant \varphi(n))$ tale che $r^h \equiv a \pmod{n}$. L'intero h (univocamente determinato $\pmod{\varphi(n)}$ da a, fissato r) è detto *indice di a relativamente ad r* (in simboli, $\mathrm{ind}_r(a) := h$).

Proposizione 5.22. *Sia n un intero positivo tale che esista una radice primitiva $r \pmod{n}$. Presi comunque $a, b \in \mathbb{Z}$ tali che $\mathrm{MCD}(a,n) = 1 = \mathrm{MCD}(b,n)$ e preso comunque $k > 0$, si ha:*

(a) $a \equiv b \pmod{n} \iff \mathrm{ind}_r(a) = \mathrm{ind}_r(b)$;

(b) $\mathrm{ind}_r(ab) \equiv \mathrm{ind}_r(a) + \mathrm{ind}_r(a) \pmod{\varphi(n)}$;

(c) $\mathrm{ind}_r(a^k) \equiv k \cdot \mathrm{ind}_r(a) \pmod{\varphi(n)}$;

(d) $\mathrm{ind}_r(r) = 1$;

(e) $\mathrm{ind}_r(1) = \varphi(n) \equiv 0 \pmod{\varphi(n)}$;

(f) *se a^* è un inverso aritmetivo di $a \pmod{n}$, risulta:* $\mathrm{ind}_r(a^*) \equiv -\mathrm{ind}_r(a) \pmod{\varphi(n)}$;

(g) *se $\bar{r}$ è un'altra radice primitiva $\pmod{n}$, risulta:* $\mathrm{ind}_{\bar{r}}(a) \equiv \mathrm{ind}_{\bar{r}}(r) \cdot \mathrm{ind}_r(a) \pmod{\varphi(n)}$.

Dimostrazione. Le semplici verifiche sono lasciate al lettore.
Ad esempio, per **(b)** basta osservare che:

$$r^{\mathrm{ind}_r(ab)} \equiv r^{\mathrm{ind}_r(a)+\mathrm{ind}_r(b)} \pmod{n}$$

ed applicare il Corollario 5.5.
Analogamente per **(g)** basta osservare che:

$$\bar{r}^{\mathrm{ind}_{\bar{r}}(a)} \equiv r^{\mathrm{ind}_{\bar{r}}(r)\cdot\mathrm{ind}_r(a)} \equiv \left(\bar{r}^{\mathrm{ind}_{\bar{r}}(r)}\right)^{\mathrm{ind}_r(a)} \pmod{n}. \ \square$$

Veniamo ora alla risoluzione di congruenze del tipo $(\bullet)$.

Teorema 5.23. *Sia n un intero positivo tale che esista una radice primitiva $r \pmod n$. Siano a, m interi tali che $m > 0$ e $\mathrm{MCD}(a, n) = 1$.*
Posto $d := \mathrm{MCD}(\varphi(n), m)$, la congruenza:

$$X^m \equiv a \pmod n \qquad (\bullet)$$

è risolubile se, e soltanto se, $d \mid \mathrm{ind}_r(a)$.
In tal caso la congruenza $(\bullet)$ ha esattamente d soluzioni distinte.

Dimostrazione. Procedendo come nella dimostrazione del Teorema 5.18, si verifica che risolvere $(\bullet)$ equivale a risolvere la congruenza lineare:

$$mY \equiv \mathrm{ind}_r(a) \pmod{\varphi(n)}$$

dove $Y = \mathrm{ind}_r(X)$.
La conclusione segue subito dal Teorema 2.2. $\square$

Corollario 5.24. (Criterio di Gauss). *Con le notazioni ed ipotesi del Teorema 5.23, la congruenza $(\bullet)$ è risolubile se, e soltanto se, risulta:*

$$a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod n.$$

Dimostrazione. Applicando le proprietà dell'indice, si ha:

$$\begin{aligned} a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod n &\iff \mathrm{ind}_r(a^{\frac{\varphi(n)}{d}}) = \mathrm{ind}_r(1) \\ &\iff \left(\frac{\varphi(n)}{d}\right) \cdot \mathrm{ind}_r(a) \equiv 0 \pmod{\varphi(n)} \\ &\iff d \mid \mathrm{ind}_r(a). \quad \square \end{aligned}$$

Osservazione 5.25. (1) È chiaro che il Teorema 5.18 e il Criterio di Euler (Corollario 5.19) sono casi particolari rispettivamente del Teorema 5.23 e del criterio di Gauss (Corollario 5.24).
(2) Particolarmente importante è il caso di congruenze del tipo $(\bullet)$ tali che $m = 2$ e $n = p$ è primo dispari. In tal caso risulta $\mathrm{MCD}(2, p-1) = 2$ e dunque la congruenza

$$X^2 \equiv a \pmod p$$

è risolubile se, e soltanto se, $\mathrm{ind}_r(a)$ è pari. Sulla risoluzione di tali congruenze (quadratiche) torneremo ampiamente nel paragrafo successivo.
(3) Il Corollario 5.24 vale, assumendo come si è fatto che n possieda una radice primitiva. Se tale ipotesi non è soddisfatta si possono dare controesempi (cfr. il punto successivo e l'Osservazione 6.11).
(4) Si noti che una congruenza del tipo $X^m \equiv a \pmod n$ può essere risolubile anche nel caso in cui n non possieda una radice primitiva, ovvero nel caso in cui n possieda una radice primitiva, ma si verifichi che $\mathrm{MCD}(a, n) \neq 1$.
Ad esempio se $n = 8$, la congruenza $X^2 \equiv 1 \pmod 8$ è risolubile; se $n = 6$, la congruenza $X^2 \equiv 4 \pmod 6$ è risolubile; se $n = 12$, la congruenza $X^3 \equiv 8 \pmod{12}$ è risolubile.

I risultati precedenti, relativi alla risoluzione di congruenze del tipo (•), hanno il difetto di rinviare a priori al calcolo di una radice primitiva e, come già osservato (cfr. Osservazione 5.14), non esistono metodi pratici generali per il calcolo di radici primitive. Sono però disponibili delle tavole, calcolate sperimentalmente, che forniscono esplicitamente le radici primitive (mod n) per valori anche molto grandi di n. Ci limitiamo qui a presentare la seguente tavola in cui g_p denota la minima radice primitiva (mod p), per ogni primo $p < 100$.

p	2	3	5	7	11	13	17	19	23	29	31	37	41
g_p	1	2	2	3	2	2	3	2	5	2	3	2	6
p	43	47	53	53	61	67	71	73	79	83	89	97	
g_p	3	5	2	2	2	2	7	5	3	2	3	5	

Osservazione 5.26. (a) Una tra le prime raccolte di tavole è contenuta nel famoso *Canon Arithmeticus* di C. Jacobi del 1839 (ristampa del 1956). Jacobi è riuscito ad elencare tutte le soluzioni (a, b) della congruenza

$$g_p^a \equiv b \pmod{p}$$

dove $1 \leqslant a, b \leqslant p-1$ e g_p è la radice primitiva minima (mod p) e con $p < 1000$. Naturalmente oggi esistono delle tavole molto più esaurienti che possono essere ulteriormente estese progressivamente con il miglioramento delle prestazioni dei mezzi di calcolo (cfr. ad esempio A. E. Western - J. C. Miller, Tables of indices and primitive roots, Royal Society Math. Tables, Cambridge University Press, 1968).
(b) Nel 1944 S. Pillai ha dimostrato che

$$\limsup_{p \longrightarrow +\infty} g_p = +\infty$$

più precisamente, per infiniti primi p, risulta

$$g_p > c \cdot \log(\log(p)),$$

dove c è una costante positiva.

Il risultato precedente è stato migliorato da Friedlander nel 1949 che ha dimostrato che, per un'infinità di primi p,

$$g_p > C \cdot \log p$$

(dove C è una costante positiva opportuna).

D'altra parte è stato dimostrato da Burgers nel 1962 che g_p non cresce "troppo in fretta", poiché

$$g_p \leqslant C \cdot p^{\frac{1}{4}+\varepsilon},$$

dove C è una costante positiva ed $\varepsilon > 0$, per p sufficientemente grande.

Ricordiamo inoltre che Kearnes nel 1984 ha dimostrato il seguente risultato congetturato da Powell nel 1983: preso comunque un intero N esistono infiniti primi p tali che

$$N < g_p < p - N.$$

Segnaliamo infine due classiche congetture non ancora risolte:

(1) Esistono infiniti primi p tali che $g_p = 2$?

(2) (Gauss). Esistono infiniti primi p tali che ammettano 10 come radice primitiva?

Queste congetture sono state riformulate nel 1927 da E. Artin nella seguente forma più generale:

(3) Sia a un intero non nullo, non quadrato perfetto e distinto da 1 e -1. È vero che a è una radice primitiva per infiniti primi?

Più precisamente, la congettura di Artin è la seguente.

(3′) Se $N_a(x) := \#\{p : p \text{ primo} \leqslant x \text{ tale che } a \text{ è una radice primitiva } (\text{mod } p)\}$ allora:

$$N_a(x) \sim A\frac{x}{\log x}$$

dove A dipende soltanto da a?

Le restrizioni su a nella congettura di Artin si giustificano in questo modo. Se $a = \pm 1$, allora $a^2 = 1$ e quindi $a = \pm 1$ non è radice primitiva (mod p) per $p - 1 > 2$. Se $a = x^2$ e se p è primo dispari tale che $p \nmid x$, applicando il "Piccolo" Teorema di Fermat (cfr. Teorema 3.1) si ha:

$$a^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \pmod{p}$$

e, dunque, a non è radice primitiva (mod p). Ne segue che, in tal caso, i primi che ammettono a come radice primitiva sono al più in numero finito.

Vogliamo concludere il paragrafo con alcuni esempi di risoluzioni di congruenze di tipo $(\star)$.

Esempio 5.27. Vogliamo studiare le congruenze:

$$X^5 \equiv a \pmod{7}, \quad \text{con } 1 \leqslant a \leqslant 6. \tag{$*$}$$

Si noti che $m = 5, p = 7$ e quindi $\text{MCD}(m, p-1) = 1$. È facile verificare che esistono $\varphi(\varphi(7)) = \varphi(6) = 2$ radici primitive distinte (mod 7) che sono, a calcoli fatti, $r = 3$ ed $s = 5$. Calcoliamo l'indice di ogni intero a $(1 \leqslant a \leqslant 6)$ relativamente ad r ed s. Si ha:

a	1	2	3	4	5	6
$\mathrm{ind}_r(a)$	6	2	1	4	5	3

a	1	2	3	4	5	6
$\mathrm{ind}_s(a)$	6	4	5	2	1	3

Ogni congruenza $(*)$ si trasforma in:

$$5 \cdot \mathrm{ind}_r(X) \equiv \mathrm{ind}_r(a) \pmod 6 \quad \text{oppure} \quad 5 \cdot \mathrm{ind}_s(X) \equiv \mathrm{ind}_s(a) \pmod 6,$$

e poiché $\mathrm{MCD}(5,6) = 1$, entrambe le congruenze sono risolubili per ogni valore di a. A tale conclusione si poteva arrivare anche utilizzando il Criterio di risolubilità di Euler. Infatti $p = 7, m = 5, d = \mathrm{MCD}(5,6) = 1$ e quindi $a^6 \equiv 1 \pmod 7$ per ogni a, tale che $p \nmid a$.
Le congruenze (mod 6) sopra considerate ammettono, fissato a, un'unica soluzione (la quale determina un'unica soluzione x per la congruenza $(*)$). Precisamente si ha:

a	1	2	3	4	5	6	(mod 7)
$\mathrm{ind}_r(a)$	0	4	5	2	1	3	(mod 6)
x	1	4	5	2	3	6	(mod 7)

a	1	2	3	4	5	6	(mod 7)
$\mathrm{ind}_s(a)$	0	2	1	4	5	3	(mod 6)
x	1	4	5	2	3	6	(mod 7)

Esempio 5.28. Vogliamo studiare le congruenze:

$$X^3 \equiv a \pmod{13}, \quad \text{con } 1 \leqslant a \leqslant 12. \qquad (**)$$

In base al Criterio di Euler (cfr. Corollario 5.19), le congruenze $(**)$ sono risolubili se, e soltanto se, $a^{\frac{12}{d}} \equiv 1 \pmod{13}$ e cioè (essendo $d = 3$) se, e soltanto se, $a^4 \equiv 1 \pmod{13}$. Poiché risulta:

(mod 13) a	1	2	3	4	5	6	7	8	9	10	11	12
(mod 13) a^4	1	3	3	9	1	9	9	1	9	3	3	1

le $(**)$ sono risolubili per $a = 1, 5, 8, 12$.
Si verifica subito che $r = 2$ è una radice primitiva (mod 13) e gli indici relativamente ad $r = 2$ sono i seguenti:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_2(a)$	12	1	4	2	9	5	11	3	8	10	7	6

Pertanto, le soluzioni delle quattro congruenze $(**)$ risolubili sono ottenute risolvendo le quattro congruenze lineari:

$$3Y \equiv \mathrm{ind}_2(a) \pmod{12},$$

con $a = 1, 5, 8, 12$ e con $Y = \mathrm{ind}_2(X)$. Ciascuna di esse ammette tre soluzioni (mod 12), che si ottengono dall'unica soluzione della congruenza

$$Y \equiv \frac{\mathrm{ind}_2(a)}{3} \pmod 4.$$

Pertanto, le soluzioni sono:

$$y \equiv \frac{\mathrm{ind}_2(a)}{3} + 4k \pmod{12},\ k = 0, 1, 2.$$

Precisamente, si ha:

(mod 13) a	(mod 12) $\mathrm{ind}_2(a)$	(mod 12) $y = \mathrm{ind}_2(x)$	(mod 13) x
1	12	4	3
		8	9
		12	1
5	9	3	8
		7	11
		11	7
8	3	1	2
		5	6
		9	5
12	6	2	4
		6	12
		10	10

5. Esercizi e Complementi

5.1. Siano $a, n \in \mathbb{Z}, n \geqslant 2$. Mostrare che:
(a) se $h, k \in \mathbb{Z}, k, h > 0$ e $\mathrm{ord}_n(a) = hk$, allora $\mathrm{ord}_n(a^h) = k$;
(b) se p è un primo dispari, $k \in \mathbb{Z}, k > 0$ e $\mathrm{ord}_p(a) = 2k$, allora $a^k \equiv -1 \pmod{p}$;
(c) se $\mathrm{ord}_n(a) = n-1$, allora n è primo (e quindi a è una radice primitiva $\pmod{n}$);
(d) se p è primo e $\mathrm{ord}_p(a) = 3$, allora $\mathrm{ord}_p(a+1) = 6$.
[Suggerimento: **(a)** è evidente. Per **(b)** si osservi che se $a^k \equiv b \not\equiv 1 \pmod{p}$ allora da $b^2 \equiv 1 \pmod{p}$ e $b \not\equiv 1 \pmod{p}$ si ricava che $b \equiv -1 \pmod{p}$. Per **(c)** basta ricordare che $\mathrm{ord}_n(a) \mid \varphi(n)$ e $\varphi(n) \leqslant n-1$. Per **(d)** si osservi che $a^2 + a + 1 \equiv 0 \pmod{p}$ e dunque $(a+1)^2 \equiv a \pmod{p}, (a+1)^3 \equiv -1 \pmod{p}$.]

5.2. Sia p un primo dispari ed r una radice primitiva (mod p). Mostrare che:
(a) $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$;
(b) se r' è un'altra radice primitiva (mod p) (cioè $r' \not\equiv r \pmod{p}$), allora rr' non è mai una radice primitiva (mod p);
(c) se $a \in \mathbb{Z}$ è tale che $ar \equiv 1 \pmod{p}$, allora a è una radice primitiva (mod p);
(d) se $p \geqslant 5$, l'insieme delle radici primitive (mod p) può essere ripartito in paia di elementi distinti di tipo $\{r, r'\}$ con $rr' \equiv 1 \pmod{p}$;
(e) se $p \equiv 1 \pmod{4}$, $-r$ è una radice primitiva (mod p);
(f) se $p \equiv 3 \pmod{4}$, $\mathrm{ord}_p(-r) = \frac{p-1}{2}$.
[Suggerimento: **(a)** $r^{\frac{p-1}{2}}$ è soluzione di $X^2 \equiv 1 \pmod{p}$ (Si tenga presente anche l'Esercizio 5.1(b)). **(b)** segue immediatamente da **(a)**. **(c)** è una conseguenza della Proposizione 5.4(4). **(d)** basta porre $r' = r^{p-2}$. **(e)**, **(f)** si calcoli $(-r)^{\frac{p-1}{2}}$.]

5.3. Se p è un primo dispari ed n un intero positivo, allora:

$$1^n + 2^n + \cdots + (p-1)^n \equiv \begin{cases} 0 \pmod{p} & \text{se } (p-1) \nmid n, \\ -1 \pmod{p} & \text{se } (p-1) \mid n. \end{cases}$$

[Suggerimento: se r è una radice primitiva (mod p), la somma in questione è congruente (mod p) a $1 + r^n + r^{2n} + \cdots + r^{(p-2)n}$. Se $(p-1) \mid n$, l'asserto è evidente dal momento che l'espressione precedente è congrua a $p-1 \pmod{p}$; se $(p-1) \nmid n$, poiché $(r^{(p-2)n} + \cdots + r^n + 1) \cdot (r^n - 1) = (r^{(p-1)n} - 1) \equiv 0 \pmod{p}$ e $r^n - 1 \not\equiv 0 \pmod{p}$, si ricava che $1 + r^n + r^{2n} + \cdots + r^{(p-2)n} \equiv 0 \pmod{p}$.]

5.4. Se p è un primo dispari ed r è una radice primitiva (mod p^n) con $n \geqslant 2$, allora r è una radice primitiva (mod p).
[Suggerimento: se $h := \mathrm{ord}_p(r)$, risulta $r^{hp} \equiv 1 \pmod{p^2}$. Infatti $p \mid (r^h - 1)$ e $p \mid (r^{p(h-1)} + r^{p(h-2)} + \cdots + r + 1)$ (poiché $p \mid (r^{(h-1)} + r^{(h-2)} + \cdots + r + 1)$ e $p \nmid (r-1)$). Quindi, per induzione su n, si dimostra che $r^{hp^{n-1}} \equiv 1 \pmod{p^n}$. Ne segue che $\varphi(p^n) \mid p^{n-1}h$, da cui discende l'asserto.]

5.5. Sia p un primo dispari ed r una radice primitiva (mod p). Mostrare che $\mathrm{ind}_r(-1) = \mathrm{ind}_r(p-1) = \frac{p-1}{2}$.
[Suggerimento: $0 \equiv (r^{p-1} - 1) = (r^{\frac{p-1}{2}} - 1) \cdot (r^{\frac{p-1}{2}} + 1) \pmod{p}$, da cui si ricava che $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ e quindi che $\mathrm{ind}_r(-1) = \frac{p-1}{2}$.]

5.6. (a) Un metodo algoritmico per il calcolo delle potenze di un intero a (mod n).

Calcolare dapprima tutti i prodotti $a, 2a, \ldots, (n-1)a \pmod n$. Procedere poi induttivamente: se $h \geqslant 1$ e se $a^h \equiv j \pmod n$, allora $a^{h+1} \equiv ja \pmod n$.
(b) Calcolare la potenza dodicesima di 3 (mod 21).

5.7. Stabilire se la congruenza $X^4 \equiv 4 \pmod{17}$ è risolubile. In caso affermativo determinare le soluzioni.
[Suggerimento: $r = 3$, $\mathrm{ind}_3(4) = 12$. La congruenza $4 \cdot \mathrm{ind}_3(X) \equiv 12 \pmod{16}$ ha quattro soluzioni $(3, 7, 11, 15) \pmod{16}$, da cui segue che le soluzioni cercate sono, rispettivamente, $x = 10, 11, 7, 6 \pmod{17}$.]

5.8. Mostrare che se r è una radice primitiva (mod n), allora:

$$1 + r + r^2 + \cdots + r^{\varphi(n)-1} \equiv 0 \pmod n.$$

[Suggerimento: si usi l'Esercizio 3.12(b).]

5.9. Determinare per quali valori di a la congruenza nell'indeterminata X

$$7^X \equiv a \pmod{17}$$

è risolubile. Per ogni valore di a, per il quale la congruenza è risolubile, determinare le soluzioni (mod 16).
[Suggerimento: la radice primitiva minima positiva (mod 17) è $r = 3$. La tabella degli indici è la seguente:

(mod 17)	a	1	2	3	4	5	6	7	8
(mod 16)	$\mathrm{ind}_3(a)$	16	14	1	12	5	15	11	10
(mod 17)	a	9	10	11	12	13	14	15	16
(mod 16)	$\mathrm{ind}_3(a)$	2	3	7	13	4	9	6	8

Quindi la congruenza precedente diviene:

$$X \,\mathrm{ind}_3(7) \equiv \mathrm{ind}_3(a) \pmod{16}$$

cioè

$$11X \equiv \mathrm{ind}_3(a) \pmod{16}.$$

Poiché $\mathrm{MCD}(11, 16) = 1$. Tale congruenza è risolubile per ogni a ed ha un'unica soluzione data da $x \equiv 3 \cdot \mathrm{ind}_3(a) \pmod{16}$.]

5.10. Determinare per quali valori di a la congruenza

$$8X^5 \equiv a \pmod{17}$$

è risolubile. Per ogni valore di a per il quale la congruenza è risolubile determinare le soluzioni (mod 17).
[Suggerimento: se r è una radice primitiva (mod 17) la congruenza data si riconduce alla congruenza

$$5Y \equiv \mathrm{ind}_r(a) - \mathrm{ind}_r(8) \pmod{16}, \text{ con } Y := \mathrm{ind}_r(X).$$

Dal momento che $\mathrm{MCD}(5, 16) = 1$. La congruenza data è risolubile per ogni valore di a ed ammette per ogni a un'unica soluzione.
Per $r = 3$ abbiamo, pertanto, la seguente tabella:

(mod 17)	a	1	2	3	4	5	6	7	8
(mod 16)	$\text{ind}_3(a)$	16	14	1	12	5	15	11	10
(mod 16)	$\text{ind}_3(a)$ - $\text{ind}_3(8)$	6	4	7	2	11	5	1	16
(mod 16)	y	14	4	11	10	15	1	13	16
(mod 17)	x	2	13	7	8	6	3	12	11
(mod 17)	a	9	10	11	12	13	14	15	16
(mod 16)	$\text{ind}_3(a)$	2	3	7	13	4	9	6	8
(mod 16)	$\text{ind}_3(a)$ - $\text{ind}_3(8)$	8	9	13	3	10	15	12	14
(mod 16)	y	8	5	9	7	2	3	12	6
(mod 17)	x	16	5	14	11	9	10	4	15

.]

5.11. Determinare per quali valori di a la congruenza

$$X^6 \equiv a \pmod{23}$$

è risolubile e determinare, per ciascun valore di a per il quale è risolubile, le soluzioni (mod 23).
[Suggerimento: la radice primitiva minima positiva (mod 23) è $r = 2$. Essendo $\text{MCD}(6, 22) = 2$, la congruenza è risolubile se e soltanto se, $\text{ind}_2(a)$ è pari ed in tal caso ha due soluzioni:

(mod 23)	a	1	2	3	4	5	6	7	8
(mod 22)	$\text{ind}_2(a)$	22	12	8	2	17	20	15	14
(mod 22)	$\text{ind}_2(x)$	11, 22	2, 13	5, 16	4, 15	-	7, 18	-	6, 17
(mod 23)	x	22, 1	4, 19	14, 9	16, 7	-	10, 13	-	18, 5

(mod 23)	a	9	10	11	12	13	14	15	16
(mod 22)	$\text{ind}_2(a)$	16	7	21	10	18	5	3	4
(mod 22)	$\text{ind}_2(x)$	10, 21	-	-	9, 20	3, 14	-	-	8, 19
(mod 23)	x	12, 11	-	-	17, 6	15, 8	-	-	3, 20

(mod 23)	a	17	18	19	20	21	22
(mod 22)	$\text{ind}_2(a)$	9	6	13	19	1	11
(mod 22)	$\text{ind}_2(x)$	-	1, 12	-	-	-	-
(mod 23)	x	-	21, 2	-	-	-	-

.]

5.12. Sia p un primo e $a \in \mathbb{Z}$ con $p \nmid a$. Mostrare che se $\text{ord}_p(a) = n \cdot m$ con $\text{MCD}(n, m) = 1$, allora esistono $b, c \in \mathbb{Z}$ con $\text{ord}_p(b) = n$, $\text{ord}_p(c) = m$ e $b \cdot c \equiv a \pmod{p}$.
[Suggerimento: innanzitutto (Teorema 2.5) è possibile trovare due interi $u, v > 0$ tali che $nu - mv = 1$. Si ponga $c := a^{nu}, b := (a^*)^{mv}$ dove a^* è inverso aritmetico di $a \pmod{p}$.]

5.13. Determinare le eventuali soluzioni della congruenza:

$$2^X \equiv X \pmod{13}.$$

[Suggerimento: si vede facilmente che $r = 2$ è una radice primitiva (mod 13). Il problema della risoluzione della congruenza data si trasforma nel problema della risoluzione della congruenza:

$$X \text{ind}_2(2) \equiv \text{ind}_2(X) \pmod{12}$$

ovvero $X - \text{ind}_2(X) \equiv 0 \pmod{12}$.
Essendo:

(mod 13)	a	1	2	3	4	5	6	7	8	9	10	11	12
(mod 12)	$\text{ind}_2(a)$	12	1	4	2	9	5	11	3	8	10	7	6

le soluzioni sono $x = 10, 16, 57, 90, 99, 115, 131, 134, 145, 149, 152 \pmod{12 \cdot 13}$.]

5.14. Determinare per quali valori di a la congruenza:

$$9X^8 \equiv a \pmod{14}$$

è risolubile. Per ciascuno dei valori di a per il quale la congruenza è risolubile, determinare le soluzioni della congruenza.
[Suggerimento: $n = 14, \varphi(n) = 6$. Si vede che $r = 3$ è una radice primitiva (mod 14).
Le soluzioni per gli interi a tali che $\text{MCD}(a, 14) = 1$ si ottengono facilmente nella seguente maniera:

(mod 14)	a, con $\text{MCD}(a, 14) = 1$	1	3	5	9	11	13
(mod 6)	$\text{ind}_3(a)$	0	1	5	2	4	3
(mod 6)	$\text{ind}_3(a) - 2$	4	5	3	0	2	1

per tali valori di a, la congruenza:

$$8\text{ind}_3(X) \equiv \text{ind}_3(a) - 2 \pmod{6}$$

è risolubile se e soltanto se $2 \mid (\text{ind}_3(a) - 2)$, quindi se e soltanto se $a \equiv 1, 9, 11 \pmod{14}$.
Le soluzioni sono: per $a \equiv 1$, $x \equiv 5, 9 \pmod{14}$; per $a \equiv 9$, $x \equiv 1, 13 \pmod{14}$; per $a \equiv 11$, $x \equiv 3, 11 \pmod{14}$.
Tuttavia, la congruenza potrebbe essere risolubile anche per valori di a non necessariamente primi con 14.
Per determinare quindi *tutte* le soluzioni, posto $f(X) := 9X^8 - a$, si debbono determinare le soluzioni del sistema di congruenze:

$$\begin{cases} f(X) \equiv 0 \pmod{2} \\ f(X) \equiv 0 \pmod{7} \end{cases} \quad \text{ovvero} \quad \begin{cases} X - a \equiv 0 \pmod{2} \\ 2X^2 - a \equiv 0 \pmod{7} \end{cases} \qquad (\diamond)$$

La seconda congruenza del sistema è risolubile se e soltanto se $(4a)^3 \equiv 1 \pmod{7}$ cioè per $a \equiv 1, 2, 4 \pmod{7}$, mentre la prima congruenza è risolubile per qualsiasi valore di $a \pmod{2}$.
In definitiva, le soluzioni della congruenza data si ottengono per a che soddisfa uno qualunque dei seguenti sistemi (mod 14):

$$\begin{cases} a \equiv 0 \pmod{2} \\ a \equiv 1 \pmod{7} \end{cases} \quad \begin{cases} a \equiv 0 \pmod{2} \\ a \equiv 2 \pmod{7} \end{cases} \quad \begin{cases} a \equiv 0 \pmod{2} \\ a \equiv 4 \pmod{7} \end{cases}$$

$$\begin{cases} a \equiv 1 \pmod{2} \\ a \equiv 1 \pmod{7} \end{cases} \quad \begin{cases} a \equiv 1 \pmod{2} \\ a \equiv 2 \pmod{7} \end{cases} \quad \begin{cases} a \equiv 1 \pmod{2} \\ a \equiv 4 \pmod{7} \end{cases}$$

e cioè $a \equiv 8, 2, 4, 1, 9, 11 \pmod{14}$. In corrispondenza di ciascuno di tali valori di a, si deve risolvere il sistema $(\diamond)$, il quale

per $a \equiv 8$ ha come soluzioni $x \equiv 2, 12 \pmod{14}$;
per $a \equiv 2$ ha come soluzioni $x \equiv 6, 8 \pmod{14}$;
per $a \equiv 4$ ha come soluzioni $x \equiv 4, 10 \pmod{14}$;
per $a \equiv 1$ ha come soluzioni $x \equiv 5, 9 \pmod{14}$;
per $a \equiv 9$ ha come soluzioni $x \equiv 1, 13 \pmod{14}$;
per $a \equiv 11$ ha come soluzioni $x \equiv 3, 11 \pmod{14}$.]

5.15. Mostrare che, se $n = 2^k$, con $k \geqslant 3$, non esiste una radice primitiva (mod n).

5.16. Se $r, s \geqslant 3$ e se $\mathrm{MCD}(r, s) = 1$, allora mostrare che:
(a) non esiste una radice primitiva (mod $r \cdot s$);
(b) se $n = p \cdot q$ ed p e q sono primi dispari, allora non esiste una radice primitiva (mod n);
(c) se $n = 2^e p^k$ con $e \geqslant 2, k \geqslant 1$, p primo dispari, allora non esiste una radice primitiva (mod n).

5.17. Se p è un primo dispari, mostrare che:
(a) esiste sempre una radice primitiva $r \pmod{p}$ tale che:

$$r^{p-1} \not\equiv 1 \pmod{p^2};$$

(b) se r è una radice primitiva (mod p), allora $r + p$ oppure $r - p$ è una radice primitiva (mod p^2);
(c) se r è una radice primitiva (mod p) e se

$$r^{p-1} \not\equiv 1 \pmod{p^2}$$

allora:

$$r^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}$$

per ogni $k \geqslant 2$;
(d) se r è una radice primitiva (mod p) e se

$$r^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}$$

allora r è una radice primitiva $\pmod{p^k}$.

5.18. Sia p un primo dispari e $k \geqslant 1$. Mostrare che:
(a) esiste sempre una radice primitiva $r \pmod{p^k}$ con $r \equiv 1 \pmod{2}$;
(b) se r è una radice primitiva (mod p^k), e se $r \equiv 1 \pmod{2}$ allora r è anche una radice primitiva $\pmod{2 \cdot p^k}$.

6 Congruenze quadratiche e legge di reciprocità

Il punto centrale di questo paragrafo è la dimostrazione della Legge di Reciprocità Quadratica (abbreviata LRQ). La prima dimostrazione completa di tale legge risale a Gauss, che la terminò nell'aprile del 1796 (e successivamente lo stesso Gauss ne ha dato almeno altre otto dimostrazioni differenti). Il primo a congetturare la validità della LQR era stato comunque Euler (nel 1745), che ne aveva poi dato anche una dimostrazione (sbagliata) nel 1783, nel suo *Opuscula Analytica*. Infine, A.M. Legendre nel suo lavoro *Recherches d'Analyse Indeterminée* (1785) dapprima, e poi nel volume *Essai sur la Théorie des Nombres* (1798), aveva ridimostrato la LRQ (in forma però incompleta), introducendo una nuova notazione (cioè, il *simbolo di Legendre*), che ne permetteva una formulazione più elegante.

Questa pluralità di contributi doveva quindi scatenare un'accesa disputa tra Euler, Legendre e Gauss, per l'attribuzione di priorità e meriti nella dimostrazione della LRQ. Informazioni più precise al riguardo si trovano in un libro di Bachmann [B], che si è ispirato ad un famoso articolo di Kronecker [K] del 1875.

La teoria delle congruenze quadratiche, cioè delle congruenze del tipo:

$$aX^2 + bX + c \equiv 0 \pmod{p} \tag{1}$$

con $a, b, c \in \mathbb{Z}$ e p primo, è certamente più complessa della teoria delle congruenze lineari, sviluppata nel Paragrafo 2 (ricordiamo che l'ipotesi che p sia primo non è restrittiva, perché possiamo sempre ricondurci a tale caso in base a quanto esposto nel Paragrafo 4). In effetti, la congruenza (1) può non essere risolubile e, se è risolubile, può non essere facile calcolarne le soluzioni. In questo paragrafo illustreremo un procedimento che permetterà di stabilire se (1) è o non è risolubile, ma non forniremo alcun metodo specifico pratico, veramente efficace, per il calcolo delle soluzioni, rinviando per questo alle tecniche generali del paragrafo precedente.

Nel considerare (1) possiamo senz'altro supporre che $p \nmid a$ (in caso contrario, (1) è una congruenza lineare) e che $p \neq 2$ (se $p = 2$, la ricerca delle soluzioni di (1) si riduce ad una banale verifica, cfr. anche il successivo Esercizio 6.1). In tali ipotesi $p \nmid 4a$ e, dunque, (1) è equivalente alla congruenza:

$$4a(aX^2 + bX + c) = (2aX + b)^2 - (b^2 - 4ac) \equiv 0 \pmod{p}.$$

Ponendo $Y := 2aX + b$ e $d := b^2 - 4ac$, (1) è equivalente a

$$Y^2 \equiv d \pmod{p}. \tag{2}$$

La risoluzione di (1) si riduce alla risoluzione di (2) e successivamente, nel caso in cui y_0 sia soluzione di (2), alla risoluzione della congruenza lineare:

$$2aX + b \equiv y_0 \pmod{p}.$$

Si noti che tale congruenza, fissato y_0 ha un'unica soluzione (mod p) data da:

$$x := \frac{p+1}{2}\, a^*(y_0 - b),$$

essendo a^* un inverso aritmetico di $a \pmod p$ e $\frac{p+1}{2}$ un inverso aritmentico di $2 \pmod p$.

Nella prima parte di questo paragrafo ci occuperemo di congruenze quadratiche della forma:

$$X^2 \equiv a \pmod p \tag{3}$$

con p primo dispari ed a intero tale che $\mathrm{MCD}(a, p) = 1$.

Proposizione 6.1. *Se la congruenza* (3) *è risolubile, allora essa ha due soluzioni distinte (cioè incongruenti* (mod p)*).*

Dimostrazione. Il Teorema di Lagrange (cfr. Teorema 4.18) assicura che (3) ha al più due soluzioni. Se x_0 è una soluzione di (3), anche $p - x_0 =: x_1$ è soluzione di (3) (infatti $(p - x_0)^2 \equiv x_0^2 \equiv a \pmod p$).
Inoltre $x_0 \not\equiv x_1 \pmod p$ (altrimenti risulterebbe $p - x_0 \equiv x_0 \pmod p$, da cui $2x_0 \equiv 0 \pmod p$, mentre $p \nmid 2$ e $p \nmid x_0$). □

Definizione 6.2. Sia p un primo dispari ed a un intero tale che si abbia $\mathrm{MCD}(a, p) = 1$. Se la congruenza (3) è risolubile, si dirà che a è un *residuo quadratico* di p; in caso contrario, si dirà che a è un *non residuo quadratico* di p.

Proposizione 6.3. *Sia p un primo dispari ed a un intero tale che si abbia $MCD(a, p) = 1$. Allora a è un residuo quadratico di p se, e soltanto se, a è congruente (mod p) ad uno dei seguenti interi:*

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Quindi, tra gli interi $1, 2, \ldots, p-1$, esattamente $\frac{p-1}{2}$ sono residui quadratici di p, mentre gli altri $\frac{p-1}{2}$ non lo sono.

Dimostrazione. È sufficiente osservare che, se a è un residuo quadratico di p, una delle due soluzioni della congruenza (3) è congruente ad uno degli interi $1, 2, \ldots, \frac{p-1}{2}$ (ciò segue immediatamente dalla dimostrazione della Proposizione 6.1). L'implicazione inversa è ovvia.

Per quanto concerne l'ultima affermazione, basta verificare che gli interi $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ sono a due a due incongruenti (mod p) (cfr. anche la dimostrazione del Lemma 4.11). □

Per caratterizzare quando un intero a è un residuo quadratico di p è conveniente introdurre la seguente notazione, dovuta a Legendre:

Definizione 6.4. Sia p un primo dispari ed a un intero tale che si abbia $\text{MCD}(a,p)=1$. Si chiama *simbolo di Legendre* il simbolo così definito:

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{se } a \text{ è un residuo quadratico di } p \\ -1, & \text{se } a \text{ non è un residuo quadratico di } p \end{cases}$$

A volte, per avere una definizione valida per ogni intero a, si pone $(\frac{a}{p}) := 0$ se $p \mid a$.

Un primo importante risultato, che otteniamo riformulando il Corollario 5.19, per $m=2$, è il seguente:

Proposizione 6.5. (Criterio di Euler). *Sia p un primo dispari ed a un intero tale che MCD$(a,p)=1$. Risulta:*

$$\left(\frac{a}{p}\right) = 1 \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \square$$

Proposizione 6.6. *Sia p un primo dispari ed siano $a, b \in \mathbb{Z}$ tali che si abbia MCD$(a,p)=1=$MCD(b,p). Allora:*

(a) $a \equiv b \pmod{p} \Rightarrow (\frac{a}{p}) = (\frac{b}{p})$*;*

(b) $(\frac{a^2}{p}) = 1$*;*

(c) $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$*;*

(d) $(\frac{a}{p}) = (-1)^{ind_r(a)}$*, dove r è una radice primitiva* $\pmod{p}$*;*

(e) $(\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p})$*;*

(f) $(\frac{1}{p}) = 1$*;*

(g) $(\frac{a}{p}) = (\frac{a^*}{p})$*, dove a^* è un inverso aritmetico di a* $\pmod{p}$*;*

(h) $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{se } p \equiv 1 \pmod{4}, \\ -1 & \text{se } p \equiv 3 \pmod{4}; \end{cases}$

(i) $(\frac{ab^2}{p}) = (\frac{a}{p})$.

Dimostrazione. (a): è del tutto ovvio. **(b)**: basta osservare che a è soluzione della congruenza $X^2 \equiv a^2 \pmod{p}$. **(c)**: dal "Piccolo" Teorema di Fermat segue che $(a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$ e dunque $a^{\frac{p-1}{2}} \equiv \pm 1$

(mod p). Per concludere basta utilizzare il Criterio di Euler (cfr. Proposizione 6.5). **(d)**: è un'immediata conseguenza del Teorema 5.23 ovvero dell'Osservazione 5.25(2). Infatti, $X^2 \equiv a \pmod{p}$ è risolubile se e soltanto se $2 = \mathrm{MCD}(2, p-1) \mid \mathrm{ind}_r(a)$. **(e)**: risulta $(\frac{ab}{p}) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \cdot (\frac{b}{p}) \pmod{p}$. Poiché il simbolo di Legendre assume soltanto valori ± 1 e $p \geqslant 2$, la congruenza $(\frac{ab}{p}) \equiv (\frac{a}{p}) \cdot (\frac{b}{p}) \pmod{p}$ è un'uguaglianza. **(f)**: è immediata . **(g)**: risulta: $(\frac{a}{p}) \cdot (\frac{a^*}{p}) = (\frac{aa^*}{p}) = (\frac{1}{p}) = 1$. Da ciò segue l'asserto. **(h)**: da (c) segue che $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Ragionando come in (e), essendo $p \geqslant 2$, si ha l'uguaglianza. Infine, si osservi che $\frac{p-1}{2}$ è pari (rispettivamente dispari) se, e soltanto se, $p \equiv 1 \pmod{4}$ (rispettivamente, $p \equiv 3 \pmod{4}$). **(i)**: risulta $(\frac{ab^2}{p}) = (\frac{a}{p}) \cdot (\frac{b^2}{p}) = (\frac{a}{p})$. □

Si noti che l'affermazione **(a)** della proposizione precedente non si inverte. Infatti $2 \not\equiv 3 \pmod{5}$, mentre $X^2 \equiv 2 \pmod{5}$ e $X^2 \equiv 3 \pmod{5}$ non sono risolubili, quindi:

$$\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Oppure, $1 \not\equiv 4 \pmod{5}$, però come è subito visto:

$$\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

Corollario 6.7. *Nella situazione della Proposizione 6.6, si ha:*

$$\left(\frac{-a^2}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$$

In altre parole la congruenza $X^2 + a^2 \equiv 0 \pmod{p}$ è risolubile se, e soltanto se, $p \equiv 1 \pmod{4}$. □

Corollario 6.8. *Sia p un primo dispari ed a un intero tale che $\mathrm{MCD}(a, p) = 1$. La congruenza:*

$$aX^2 + bX + c \equiv 0 \pmod{p} \tag{1}$$

è risolubile se, e soltanto se, l'intero $b^2 - 4ac$ è un residuo quadratico di p oppure è congruente a zero $\pmod{p}$. □

Dimostrazione. L'enunciato segue dalla "riduzione" discussa all'inizio del paragrafo. □

Corollario 6.9. *Sia p un primo dispari ed $a = \pm p_1^{e_1} \cdots p_r^{e_r}$ un intero tale che $\mathrm{MCD}(a, p) = 1$. Allora:*

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \cdot \left(\frac{p_1}{p}\right)^{e_1} \cdots \left(\frac{p_r}{p}\right)^{e_r}. \quad \square$$

Dal precedente corollario discende che per calcolare $(\frac{a}{p})$ è sufficiente saper calcolare i simboli di Legendre del tipo $(\frac{\pm 1}{p})$ e $(\frac{q}{p})$, con p, q primi distinti. La Legge di Reciprocità Quadratica, come vedremo, riguarderà il calcolo del simbolo $(\frac{q}{p})$, nel caso in cui p, q siano primi distinti *dispari*.

Corollario 6.10. *Sia p un primo dispari ed r una radice primitiva (modulo p). I residui quadratici di p sono congruenti alle potenze pari di r. Quindi:*

$$\sum_{a=1}^{p-1} (\frac{a}{p}) = 0.$$

Dimostrazione. La prima affermazione è una conseguenza immediata della Proposizione 6.6(d) e la seconda della Proposizione 6.3. □

Osservazione 6.11. Siano a, n interi tali che $n > 2$ e $\mathrm{MCD}(a, n) = 1$. In analogia con quanto esposto sopra, diremo che a è un *residuo quadratico* di n se la congruenza $X^2 \equiv a \pmod{n}$ è risolubile. Si verifica facilmente (utilizzando il Teorema di Euler - Fermat) che se a è un residuo quadratico di n, allora $a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{n}$. L'affermazione reciproca è però falsa, in generale. Infatti, se $n = 8$ e $a = 3$, si ha $\varphi(8) = 4$ e $3^2 \equiv 1 \pmod{8}$ mentre la congruenza $X^2 \equiv 3 \pmod{8}$ non è risolubile. (Questo fatto non è in disaccordo con il Corollario 5.24: infatti $n = 8$ è un intero che non ammette radici primitive!)

La maggior parte delle numerose differenti dimostrazioni della LRQ utilizza il seguente risultato, noto come "Lemma di Gauss".

Teorema 6.12. (Lemma di Gauss). *Sia p un primo dispari ed a un intero tale che* $\mathrm{MCD}(a, p) = 1$. *Consideriamo il sistema completo di residui minimo in valore assoluto (modulo p):*

$$\Sigma := \{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$$

e l'insieme

$$S(a) := \{a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a\}.$$

Indicato con $\nu = \nu(a)$ il numero degli elementi di $S(a)$ congruenti (modulo p) agli interi negativi di Σ, si ha:

$$\left(\frac{a}{p}\right) = (-1)^{\nu(a)}.$$

Dimostrazione. Osserviamo dapprima che, se h e k sono interi tali che $1 \leqslant h < k \leqslant \frac{p-1}{2}$, allora $ha \not\equiv \pm ka \pmod{p}$. Infatti, se fosse $ha \equiv \pm ka \pmod{p}$, allora $h \equiv \pm k \pmod{p}$ e ciò è assurdo in base alle ipotesi fatte su

h e k. Per ogni k tale che $1 \leqslant k \leqslant \frac{p-1}{2}$, esiste un unico $r_k \in \Sigma$ tale che $r_k \equiv ka \pmod p$ e, per quanto osservato sopra, l'insieme $\{r_1, \ldots, r_{\frac{p-1}{2}}\}$ è costituito da interi a due a due differenti in valore assoluto (cioè $|r_h| \neq |r_k|$ se $h \neq k$). Ne segue che gli insiemi $\{1, 2, \ldots, \frac{p-1}{2}\}$ e $\{|r_1|, \ldots, |r_{\frac{p-1}{2}}|\}$ coincidono e quindi, in base alla definizione di ν, si ha:

$$\prod_{i=1}^{\frac{p-1}{2}} r_i = (-1)^\nu \prod_{i=1}^{\frac{p-1}{2}} |r_i| = (-1)^\nu \left(\frac{p-1}{2}\right)!.$$

D'altra parte, essendo $r_k \equiv ka \pmod p$ $(1 \leqslant k \leqslant \frac{p-1}{2})$, si ha:

$$\left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \equiv \prod_{i=1}^{\frac{p-1}{2}} r_i = (-1)^\nu \left(\frac{p-1}{2}\right)! \pmod p$$

e pertanto, poichè $p \nmid \left(\frac{p-1}{2}\right)!$, applicando la Proposizione 6.6(c), si ha:

$$(-1)^\nu \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p,$$

da cui (essendo $p > 2$) segue la tesi. □

Osservazione 6.13. Confrontando la Proposizione 6.6(d) con il Teorema 6.12, si ha $(-1)^{\nu(a)} = (-1)^{\mathrm{ind}_r(a)}$ e dunque $\nu(a) \equiv \mathrm{ind}_r(a) \pmod 2$. Non è detto però che $\nu(a) = \mathrm{ind}_r(a)$: ad esempio, ponendo $p = 7, r = 5$ e $a = 2$ si verifica che $\nu(2) = 2$ e $\mathrm{ind}_5(2) = 4$. (Infatti, in tal caso: $\Sigma = \{-3, -2, -1, 0, 1, 2, 3\}$, $S(2) = \{2, 4, 6\}$, $\nu(2) = 2$; $5, 5^2 \equiv 4 \pmod 7, 5^3 \equiv 6 \pmod 7, 5^4 \equiv 2 \pmod 7$ dunque $\mathrm{ind}_5(2) = 4$.)

Ci proponiamo, ora, di applicare il Lemma di Gauss per calcolare $(\frac{2}{p})$ e $(\frac{3}{p})$.

Corollario 6.14. *Sia p un primo dispari. Allora:*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se, e soltanto se, } p \equiv 1 \text{ oppure } p \equiv 7 \pmod 8, \\ -1 & \text{se, e soltanto se, } p \equiv 3 \text{ oppure } p \equiv 5 \pmod 8. \end{cases}$$

Ne segue che:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Dimostrazione. Per calcolare $\nu(2)$ basta osservare che gli elementi del tipo $2k \in S(2)$ congruenti (modulo p) agli interi negativi di Σ verificano la diseguaglianza

$$\frac{p+1}{2} \leqslant 2k \leqslant p-1 \quad \text{e cioè} \quad \frac{p+1}{4} \leqslant k \leqslant \frac{p-1}{2}.$$

Dividendo p per 8, restano individuati $m, r \in \mathbb{N}$ tali che:

$$p = m8 + r, \quad \text{con } 0 \leqslant r \leqslant 7$$

e dunque, si ha:

$$2m + \frac{r+1}{4} \leqslant k \leqslant 4m + \frac{r-1}{2}.$$

Poichè p è dispari, r assume i valori $1, 3, 5, 7$.
Se quindi $r = 1$, risulta $\frac{2m+1}{2} \leqslant k \leqslant 4m$ e, dunque, $2m + 1 \leqslant k \leqslant 4m$. Ne segue che $\nu = 4m - (2m + 1) + 1 = 2m$.
Procedendo in modo analogo, si ha:
se $r = 3$, $2m + 1 \leqslant k \leqslant 4m + 1$ e quindi $\nu = 2m + 1$,
se $r = 5$, $2m + 2 \leqslant k \leqslant 4m + 2$ e quindi $\nu = 2m + 1$,
se $r = 7$, $2m + 2 \leqslant k \leqslant 4m + 3$ e quindi $\nu = 2m + 2$.
Pertanto ν è pari se, e soltanto se, $r = 1, 7$ cioè $p \equiv 1, 7 \pmod 8$.

Relativamente all'ultima parte dell'enunciato, basta verificare che:
se $p \equiv 1, 7 \pmod 8$, allora $\frac{p^2-1}{8}$ è pari, mentre se $p \equiv 3, 5 \pmod 8$, allora $\frac{p^2-1}{8}$ è dispari. □

Corollario 6.15. *Sia p un primo, $p \geqslant 5$. Allora:*

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \textit{se, e soltanto se, } p \equiv 1, 11 \pmod{12}, \\ -1 & \textit{se, e soltanto se, } p \equiv 5, 7 \pmod{12}. \end{cases}$$

Dimostrazione. Procedendo in modo analogo alla dimostrazione precedente, si vede che $\nu = \nu(3)$ coincide con il numero degli interi k tali che

$$\frac{p+1}{2} \leqslant 3k \leqslant p \quad \text{e cioè} \quad \frac{p+1}{6} \leqslant k \leqslant \frac{p}{3}.$$

Dividendo p per 12, per le restrizioni poste su p si ha che:

$$p = 12m + r \quad \text{con } r = 1, 5, 7, 11,$$

($r \neq 3, 9$ perché altrimenti p sarebbe divisibile per 3).
Pertanto, si ha:
se $r = 1$, $2m + 1 \leqslant k \leqslant 4m$ e, quindi, $\nu = 2m$,
se $r = 5$, $2m + 1 \leqslant k \leqslant 4m + 1$ e, quindi, $\nu = 2m + 1$,
se $r = 7$, $2m + 2 \leqslant k \leqslant 4m + 2$ e, quindi, $\nu = 2m + 1$,
se $r = 11$, $2m + 2 \leqslant k \leqslant 4m + 3$ e, quindi, $\nu = 2m + 2$.
Da ciò discende la tesi. □

Osservazione 6.16. Riotterremo il risultato precedente come semplice applicazione della LRQ (cfr. il successivo Esempio 6.24). Questa dimostrazione risulterà quindi superflua, ma ci sembra, comunque, particolarmente istruttiva in vista della dimostrazione della LRQ.

Richiamiamo, ora, alcuni concetti e proprietà che saranno utili per dimostrare la LRQ.

Definizione 6.17. Sia α un numero reale. Si chiama *parte intera di* α (e si denota $[\alpha]$) il più grande intero $\leqslant \alpha$. Si chiama *parte residuale di* α il numero reale $\alpha_1 := \alpha - [\alpha]$ (ovviamente $0 \leqslant \alpha_1 < 1$ e $\alpha = [\alpha] + \alpha_1$).

Proposizione 6.18. *Siano α, β numeri reali tali che $\alpha \leqslant \beta$. Allora:*
(a) *il numero degli interi k tali che $\alpha \leqslant k \leqslant \beta$ è uguale a $[\beta]-[\alpha]$, se $\alpha \notin \mathbb{Z}$, oppure a $[\beta] - [\alpha] + 1$ se $\alpha \in \mathbb{Z}$;*
(b) *per ogni intero n, $[n + \beta] = n + [\beta]$;*
(c) *siano n_1, n_2 interi tali che $n_1 \leqslant n_2$. Si ponga:*

$$\nu := \#\{k \in \mathbb{Z}; 2n_1 + \alpha \leqslant k \leqslant 2n_2 + \beta\} \quad e$$

$$\mu := \#\{h \in \mathbb{Z} : \alpha \leqslant h \leqslant \beta\}.$$

Allora:

$$\mu \equiv \nu \pmod 2.$$

Dimostrazione. **(a)**: gli interi cercati sono $[\alpha]+1, [\alpha]+2, \ldots, [\beta]$ e dunque sono esattamente $[\beta]-[\alpha]$ se $\alpha \notin \mathbb{Z}$; se $\alpha \in \mathbb{Z}$, agli interi sopra elencati si deve aggiungere $[\alpha] = \alpha \in \mathbb{Z}$. **(b)**: sia $\beta_1 := \beta - [\beta]$. Allora $n + \beta = (n + [\beta]) + \beta_1$ ed $n + [\beta]$ è un intero. Da ciò segue la tesi. **(c)**: da (a) e (b) segue che $\nu = [2n_2 + \beta] - [2n_1 + \alpha] = 2n_2 + [\beta] - 2n_1 - [\alpha] = 2(n_2 - n_1) + \mu$ se $\alpha \notin \mathbb{Z}$. Ad analoga conclusione si perviene se $\alpha \in \mathbb{Z}$. □

Proposizione 6.19. *Siano p un primo dispari ed a un intero anch'esso dispari tale che* $\mathrm{MCD}(a, p) = 1$. *Allora*

$$\left(\frac{a}{p}\right) = (-1)^{\sigma_a} \quad con\ \sigma_a := \prod_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]$$

Dimostrazione. Come nel Teorema 6.12, sia $S(a) := \{ka : 1 \leqslant k \leqslant \frac{p-1}{2}\}$. Dividendo gli elementi di $S(a)$ per p, si ottiene:

$$ka = q_k p + t_k \text{ con } q_k, t_k \in \mathbb{N} \text{ e } 1 \leqslant t_k \leqslant p - 1.$$

Ne segue che $\frac{ka}{p} = q_k + \frac{t_k}{p}$ e quindi $\left[\frac{ka}{p}\right] = q_k$; pertanto si ha:

$$ka = \left[\frac{ka}{p}\right] \cdot p + t_k, \quad 1 \leqslant k \leqslant \frac{p-1}{2}.$$

Si denoti con $\{s_1, \ldots, s_\mu\}$ l'insieme $\{t_k : \text{con } 1 \leqslant t_k \leqslant \frac{p-1}{2}$, al variare di k e con $1 \leqslant k \leqslant \frac{p-1}{2}\}$ e con $\{r_1, \ldots, r_\nu\}$ l'insieme $\{t_k : \text{e con } \frac{p+1}{2} \leqslant t_k \leqslant p - 1$, al variare di k e con $1 \leqslant k \leqslant \frac{p-1}{2}\}$. Si noti che ν è lo stesso intero, $\nu(a)$,

considerato nel Lemma di Gauss (cfr. Teorema 6.12).
Vogliamo verificare che l'insieme $\{s_1, \ldots, s_\mu, p - r_1, \ldots, p - r_\nu\}$ coincide con l'insieme $\{1, 2, \ldots, \frac{p-1}{2}\}$. A tale scopo basta provare che $s_{i'} \not\equiv p - r_{j'} \pmod{p}$ (con $1 \leqslant i' \leqslant \mu$ e $1 \leqslant j' \leqslant \nu$). Se infatti $s_{i'} \equiv ia \pmod{p}$ e $r_{j'} \equiv ja \pmod{p}$; dove $1 \leqslant i \neq j \leqslant \frac{p-1}{2}$), allora $(i+j)a \equiv s_{i'} + r_{j'} \pmod{p}$; se, per assurdo, fosse $s_{i'} \equiv p - r_{j'} \pmod{p}$, allora $(i+j)a \equiv 0 \pmod{p}$ e dunque $i + j \equiv 0 \pmod{p}$, il che è ovviamente assurdo.
Si ha allora:

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^{\mu} s_i + \sum_{j=1}^{\nu} (p - r_j) = p\nu + \sum_{i=1}^{\mu} s_i + \sum_{j=1}^{\nu} r_j$$

ed anche:

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] \cdot p + \sum_{i=1}^{\mu} s_i + \sum_{j=1}^{\nu} r_j$$

da cui, sottraendo la prima uguaglianza dalla seconda, si ottiene:

$$(a-1) \sum_{k=1}^{\frac{p-1}{2}} k = p(\sigma_a - \nu) + 2 \sum_{j=1}^{\nu} r_j.$$

Tenendo presente che $p \equiv a \equiv 1 \pmod{2}$, si ha $0 \equiv \sigma_a - \nu \pmod{2}$ e dunque, applicando il Teorema 6.12, si ha la tesi. □

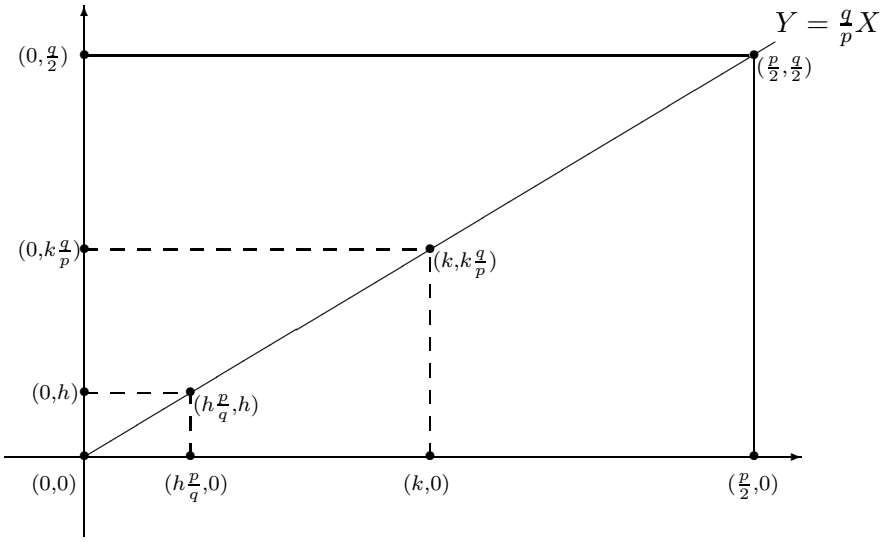
Veniamo finalmente alla LRQ. La dimostrazione che ne daremo è dovuta a F. G. Eisenstein (allievo di Gauss) ed è, in pratica, una semplificazione di una delle varie dimostrazioni che Gauss dette di tale legge.

Osservazione 6.20. Si noti che ormai la prima dimostrazione di Gauss, scritta "in a very repulsive form", come scrisse H. J. Smith, è stata rivisitata e riscritta in maniera estremamente chiara da E. Brown (cfr. Amer. Math. Montly, **88** (1981), 257-263). Altre semplici dimostrazioni sono state date da M. Gersternhaber (cfr. Amer. Math. Montly, **70** (1963), 397-398) e da J.S. Frame (cfr. Amer. Math. Montly, **85** (1978), 818-819).
Per un esame comparativo di varie dimostrazioni classiche della LRQ va infine segnalato un articolo di Frobenius del 1914 (cfr. Gesamm. Abh., **3** (1914), 628-647; Springer, 1968).

Teorema 6.21. (Legge di Reciprocità Quadratica). *Siano p, q due primi dispari distinti. Allora:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Dimostrazione. Nel piano cartesiano consideriamo il rettangolo di vertici $(0,0), (\frac{p}{2}, 0), (0, \frac{q}{2}), (\frac{p}{2}, \frac{q}{2})$.



e denotiamo con R l'interno di tale rettangolo. L'idea della dimostrazione consiste nel contare, in due modi distinti, i punti a coordinate intere giacenti in R.

Sia (n, m) un punto del piano a coordinate intere: è chiaro che $(n, m) \in R$ se, e soltanto se, risulta

$$1 \leqslant n \leqslant \frac{p-1}{2} \quad \text{e} \quad 1 \leqslant m \leqslant \frac{q-1}{2}$$

essendo $\frac{p-1}{2} = \left[\frac{p}{2}\right]$ e $\frac{q-1}{2} = \left[\frac{q}{2}\right]$. Pertanto i punti cercati sono in numero di $\left(\frac{p-1}{2}\right) \cdot \left(\frac{q-1}{2}\right)$.

Procediamo, ora, al calcolo degli stessi punti seguendo un altro metodo. La diagonale del rettangolo (condotta dal vertice $(0, 0)$) ha equazione:

$$Y = \frac{q}{p}X$$

e si verifica subito che nessun punto di R a coordinate intere (n, m) giace su tale diagonale. In caso contrario, risulterebbe $m = \frac{q}{p}n$, dunque $pm = qn$ e pertanto $p \mid n$ e $q \mid m$. Ciò è in contrasto con le limitazioni $1 \leqslant n \leqslant \frac{p-1}{2}$ e $1 \leqslant m \leqslant \frac{q-1}{2}$.

Se denotiamo allora con T_1 (rispettivamente T_2) il sottoinsieme triangolare di R giacente al di sotto (rispettivamente al di sopra) della diagonale, è evidente che i punti cercati sono quelli giacenti in T_1 più quelli giacenti in T_2. Ora, se k è un intero tale che $1 \leqslant k \leqslant \frac{p-1}{2}$, il numero degli interi y tali che $0 < y < \frac{qk}{p}$ è dato da $[qk/p]$ e pertanto i punti di T_1 a coordinate intere

e con ascissa k sono esattamente $[qk/p]$. Ne segue che i punti a coordinate intere in T_1 sono:

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right].$$

Analogamente, i punti a coordinate intere in T_2 sono:

$$\sum_{h=1}^{\frac{q-1}{2}} \left[\frac{ph}{q}\right].$$

In definitiva, abbiamo:

$$\left(\frac{p-1}{2}\right)\cdot\left(\frac{q-1}{2}\right) = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right] + \sum_{h=1}^{\frac{q-1}{2}} \left[\frac{ph}{q}\right].$$

Applicando due volte la Proposizione 6.19, abbiamo:

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\sum_{h=1}^{\frac{q-1}{2}}\left[\frac{ph}{q}\right]}\cdot(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{qk}{p}\right]} = (-1)^{(\frac{p-1}{2})\cdot(\frac{q-1}{2})}. \ \square$$

Corollario 6.22. *Siano p, q due primi dispari distinti. Allora:*

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 \pmod 4 \text{ o/e } q \equiv 1 \pmod 4, \\ -1 & \text{se } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Dimostrazione. Basta osservare che $(\frac{p-1}{2})\cdot(\frac{q-1}{2})$ è pari se, e soltanto se, almeno uno dei due primi p, q è congruente a $1 \pmod 4$. $\square$

Corollario 6.23. *Siano p, q due primi dispari distinti. Allora:*

$$\left(\frac{p}{q}\right) = \begin{cases} (\frac{q}{p}) & \text{se } p \equiv 1 \pmod 4 \text{ o/e } q \equiv 1 \pmod 4, \\ -(\frac{q}{p}) & \text{se } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Dimostrazione. Basta moltiplicare per $(\frac{q}{p})$ ambo i membri dell'uguaglianza del Corollario 6.22, tenendo conto del fatto che $(\frac{q}{p})^2 = 1$ $\square$

Algoritmo per il calcolo del simbolo di Legendre. A questo punto è opportuno chiarire come i risultati precedenti possono essere utilizzati per calcolare $(\frac{a}{p})$, dove p è un primo dispari ed a un intero tale che $\mathrm{MCD}(a, p) = 1$. Se $a = \pm 2^{e_0} p_1^{e_1} \dots p_r^{e_r}$ (con $p_1, \dots, p_r$ primi dispari distinti), dal Corollario 6.9 segue che:

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{e_0}\left(\frac{p_1}{p}\right)^{e_1}\cdots\left(\frac{p_r}{p}\right)^{e_r}.$$

La LRQ permette di ricondurre il calcolo di ogni $(\frac{p_i}{p})$ al calcolo di $(\frac{p}{p_i})$ (nel caso in cui $p_i < p$), rinviando quindi al calcolo del simbolo di Legendre con "denominatore" più piccolo di quello di partenza. Dividendo p per p_i si ha:

$$p = h_i p_i + r_i, \text{ con } h_i, r_i \in \mathbb{N} \quad \text{e} \quad 1 \leqslant r_i \leqslant p_i,$$

dunque $p \equiv r_i \pmod{p_i}$ e pertanto $(\frac{p}{p_i}) = (\frac{r_i}{p_i})$. A questo punto si fattorizza r_i nel prodotto di primi e si itera il procedimento sopra esposto. In questo modo, per il calcolo di un qualsiasi simbolo di Legendre $(\frac{p_i}{p})$, ci si riduce, in ultima analisi, al calcolo di simboli di Legendre del tipo:

$$(\frac{1}{q}), \quad (\frac{-1}{q}), \quad (\frac{2}{q})$$

dove q è un qualunque primo dispari; i valori di tali simboli di Legendre sono stati già calcolati.

Esemplifichiamo le considerazioni ora svolte.

Esempio 6.24. Calcolo di $(\frac{3}{p})$ con p primo dispari, $p > 3$.
Si ha, ponendo $r \equiv p \pmod{3}, 1 \leqslant r \leqslant 2$:

$$\begin{aligned}
\left(\frac{3}{p}\right) &= \begin{cases} (\frac{p}{3}) = (\frac{r}{3}) & \text{se } p \equiv 1 \pmod 4, \\ -(\frac{p}{3}) = -(\frac{r}{3}) & \text{se } p \equiv 3 \pmod 4, \end{cases} \\
&= \begin{cases} (\frac{1}{3}) = 1 & \text{se } p \equiv 1 \pmod 4 \text{ e } p \equiv 1 \pmod 3, \\ -(\frac{1}{3}) = -1 & \text{se } p \equiv 3 \pmod 4 \text{ e } p \equiv 1 \pmod 3, \\ (\frac{2}{3}) = -1 & \text{se } p \equiv 1 \pmod 4 \text{ e } p \equiv 2 \pmod 3, \\ -(\frac{2}{3}) = 1 & \text{se } p \equiv 3 \pmod 4 \text{ e } p \equiv 2 \pmod 3, \end{cases} \\
&= \begin{cases} 1 & \text{se } p \equiv 1, 11 \pmod{12}, \\ -1 & \text{se } p \equiv 5, 7 \pmod{12}. \end{cases}
\end{aligned}$$

Esempio 6.25. Calcolo di $(\frac{4}{p})$ con p primo dispari.
Risulta, ovviamente:

$$\left(\frac{4}{p}\right) = \left(\frac{2}{p}\right)^2 = 1.$$

Esempio 6.26. Calcolo di $(\frac{5}{p})$ con p dispari, $p \neq 5$.
Se $p = 3$, $(\frac{5}{3}) = (\frac{2}{3}) = -1$. Sia $p > 5$: in tal caso $(\frac{5}{p}) = (\frac{p}{5})$ e risulta:

$$p = 5k + r \text{ con } k, r, \in \mathbb{N} \quad \text{e} \quad 1 \leqslant r \leqslant 4.$$

Pertanto:

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{r}{5}\right) = \begin{cases} (\frac{1}{5}) = 1 & \text{se } p \equiv 1 \pmod 5, \\ (\frac{2}{5}) = -1 & \text{se } p \equiv 2 \pmod 5, \\ (\frac{3}{5}) = (\frac{5}{3}) = (\frac{2}{3}) = -1 & \text{se } p \equiv 3 \pmod 5, \\ (\frac{4}{5}) = (\frac{2}{5})^2 = 1 & \text{se } p \equiv 4 \pmod 5, \end{cases}$$

$$= \begin{cases} 1 & \text{se } p \equiv 1, 4 \pmod 5, \\ -1 & \text{se } p \equiv 2, 3 \pmod 5. \end{cases}$$

Esempio 6.27. Calcolo di $(\frac{6}{p})$ con $p \geqslant 5$, p primo.
Poiché $(\frac{6}{p}) = (\frac{2}{p}) \cdot (\frac{3}{p})$, allora, $(\frac{6}{p}) = -1$ se, e soltanto se, uno soltanto tra i simboli $(\frac{2}{p})$ e $(\frac{3}{p})$ vale -1. A partire dai valori già noti di $(\frac{2}{p})$ e $(\frac{3}{p})$ si ottiene facilmente che:

$$\left(\frac{6}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1, 5, 19, 23 \pmod{24}, \\ -1 & \text{se } p \equiv 7, 11, 13, 17 \pmod{24}. \end{cases}$$

Esempio 6.28. Calcolo di $(\frac{7}{p})$ con p primo dispari, $p \neq 7$.
Se $p = 3$, $(\frac{7}{3}) = (\frac{1}{3}) = 1$; se $p = 5$, $(\frac{7}{5}) = (\frac{2}{5}) = -1$. Sia ora $p > 7$; in tal caso si ha:

$$\left(\frac{7}{p}\right) = \begin{cases} (\frac{p}{7}) & \text{se } p \equiv 1 \pmod 4, \\ -(\frac{p}{7}) & \text{se } p \equiv 3 \pmod 4. \end{cases}$$

Ora, $p = 7k + r$ con $k, r \in \mathbb{N}$ e $1 \leqslant r \leqslant 6$; conseguentemente:

$$\left(\frac{p}{7}\right) = \begin{cases} (\frac{1}{7}) = 1 & \text{se } p \equiv 1 \pmod 7, \\ (\frac{2}{7}) = 1 & \text{se } p \equiv 2 \pmod 7, \\ (\frac{3}{7}) = -1 & \text{se } p \equiv 3 \pmod 7, \\ (\frac{4}{7}) = 1 & \text{se } p \equiv 4 \pmod 7, \\ (\frac{5}{7}) = -1 & \text{se } p \equiv 5 \pmod 7, \\ (\frac{6}{7}) = -1 & \text{se } p \equiv 6 \pmod 7. \end{cases}$$

Ne segue che:

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}, \\ -1 & \text{se } p \equiv 5, 11, 13, 15, 17, 23 \pmod{28}. \end{cases}$$

Concludiamo questo paragrafo studiando la risolubilità di congruenze quadratiche di tipo:

$$X^2 \equiv a \pmod n \tag{4}$$

dove n è un intero arbitrario $\geqslant 2$ ed a un intero tale che $\mathrm{MCD}(a,n)=1$. Tenuto conto delle considerazioni svolte all'inizio del Paragrafo 4 e supposto che n ammetta la seguente fattorizzazione in numeri primi distinti:

$$n = 2^{e_0} p_1^{e_1} \cdots p_r^{e_r},$$

la risolubilità di (4) equivale alla risolubilità del sistema:

$$\begin{cases} X^2 \equiv a \pmod{2^{e_0}}, \\ X^2 \equiv a \pmod{p_i^{e_i}}, \\ 1 \leqslant i \leqslant r \end{cases}$$

Ci occuperemo quindi separatamente dei seguenti problemi:

I Problema: studio della risolubilità di congruenze del tipo:

$$X^2 \equiv a \pmod{p^e}$$

con p primo dispari, $e > 1$ ed a intero tale che $\mathrm{MCD}(a,p)=1$.

II Problema: studio della risolubilità di congruenze del tipo:

$$X^2 \equiv a \pmod{2^e}$$

con $e > 1$ ed a intero dispari.

Veniamo al I Problema:

Teorema 6.29. *Sia p primo dispari ed a un intero tale che* $\mathrm{MCD}(a,p)=1$. *Allora la congruenza:*

$$X^2 \equiv a \pmod{p^e} \text{ con } e \geqslant 1 \tag{5}$$

è risolubile se, e soltanto se, $\left(\frac{a}{p}\right) = 1$.

Dimostrazione. Se la congruenza (5) è risolubile, ogni sua soluzione risolve anche la congruenza $X^2 \equiv a \pmod{p}$: dunque $\left(\frac{a}{p}\right) = 1$.

Viceversa, assumiamo che $\left(\frac{a}{p}\right) = 1$ e procediamo per induzione su e. Il caso $e = 1$ è assunto per ipotesi. Sia $e \geqslant 2$ e supponiamo che la congruenza $X^2 \equiv a \pmod{p^{e-1}}$ sia risolubile. Se y ne è una soluzione, esiste $b \in \mathbb{Z}$ tale che $y^2 = a + bp^{e-1}$. Poiché $\mathrm{MCD}(p, 2y) = 1$, la seguente congruenza lineare nell'indeterminata T:

$$2yT \equiv -b \pmod{p}$$

ammette un'unica soluzione t. Poniamo allora

$$x := x_t := y + tp^{e-1}$$

e verifichiamo che x è soluzione di (5). Infatti, si ha:

$$x^2 = a + bp^{e-1} + 2ytp^{e-1} + t^2 p^{2e-2} \equiv a + bp^{e-1} - bp^{e-1} \pmod{p^e}$$

in quanto $2ytp^{e-1} \equiv -bp^{e-1} \pmod{p^e}$ e $2e - 2 \geqslant e$, per $e \geqslant 2$. $\square$

Osservazione 6.30. Facendo uso del Teorema 4.6 possiamo riottenere in maniera più rapida la seconda implicazione del teorema precedente. Sia infatti $f(X) := X^2 - a$ e y una soluzione di $f(X) \equiv 0 \pmod{p^{e-1}}$. Poichè p è dispari, si dimostra per induzione su $e \geqslant 2$ che $f'(y) = 2y \not\equiv 0 \pmod{p}$ e dunque si è nella situazione descritta nel I Caso del Teorema 4.6 (cioè che y è una soluzione non singolare; cfr. anche Esercizio 4.1). Ne segue che (5) è risolubile.
Si noti che questo ragionamento non si può ripetere nel caso del successivo Teorema 6.32(3), per il quale sarà necessario sviluppare una dimostrazione "ad hoc".

Corollario 6.31. *Con le notazioni del Teorema 6.29, se la congruenza* (5) *è risolubile, essa ammette esattamente due soluzioni distinte (cioè non congruenti* $\pmod{p^e}$*).*

Dimostrazione. Alla conclusione si può pervenire (ragionando come nell'Osservazione 6.30), applicando il Teorema 4.6. Diamo, comunque, una dimostrazione esplicita (ispirata a quella del Teorema 4.6), che poi tornerà utile per dimostrare il successivo Corollario 6.34.
Se x_0 è una soluzione di (5), è chiaro che x_0 e $x_1 := p - x_0$ sono due soluzioni distinte di (5). Proviamo, per induzione su e, che (5) ammette soltanto due soluzioni distinte. Se $e = 1$, l'asserto è vero (cfr. Proposizione 6.1). Supponiamo che $e \geqslant 2$ e che la congruenza:

$$X^2 \equiv a \pmod{p^{e-1}} \tag{6}$$

ammetta soltanto due soluzioni y_0, y_1. Dalla dimostrazione del Teorema 6.29 segue che y_i $(0 \leqslant i \leqslant 1)$ determina la soluzione $x_i := y_i + t_i p^{e-1}$ di (5), dove $y_i^2 = a + b_i p^{e-1}$ per un qualche $b_i \in \mathbb{Z}$ e t_i è la soluzione della congruenza lineare $2y_i T \equiv -b_i \pmod{p}$.

Per concludere basta verificare che se x è una soluzione della congruenza (5), allora $x \equiv x_0 \pmod{p^e}$ oppure $x \equiv x_1 \pmod{p^e}$. Poiché x è una soluzione di (6), allora $x \equiv y_i \pmod{p^{e-1}}$, con $i = 0$ oppure $i = 1$. Posto $x = y_i + \tau p^{e-1}$ per un qualche $\tau \in \mathbb{Z}$, dalla congruenza $x^2 \equiv a \equiv (x_i)^2 \pmod{p^e}$ discende che:

$$y_i^2 + 2y_i \tau p^{e-1} + \tau^2 p^{2e-2} \equiv y_i^2 + 2y_i t_i p^{e-1} + t_i^2 p^{2e-2} \pmod{p^e}.$$

Da ciò di ricava facilmente che $\tau \equiv t_i \pmod{p}$ e quindi si conclude che $x \equiv x_i \pmod{p^e}$. □

Veniamo ora al II Problema:

Teorema 6.32. *Sia a un intero dispari. Allora:*

(1) *La congruenza $X^2 \equiv a \pmod{2}$ è sempre risolubile;*

(2) *La congruenza* $X^2 \equiv a \pmod 4$ *è risolubile se, e soltanto se,* $a \equiv 1 \pmod 4$*;*

(3) *La congruenza* $X^2 \equiv a \pmod{2^e}$*,* $e \geqslant 3$ *è risolubile se, e soltanto se,* $a \equiv 1 \pmod 8$*.*

Dimostrazione. (1). È del tutto ovvio. **(2).** Sia $x_0 \in \mathbb{Z}$ una soluzione della congruenza $X^2 \equiv a \pmod 4$. Essendo a dispari, anche x_0 è dispari e poichè il quadrato di ogni intero dispari è congruente ad 1 (mod 4), si ha $a \equiv x_0^2 \equiv 1 \pmod 4$. Viceversa, se $a \equiv 1 \pmod 4$, allora 1 e 3 sono soluzioni della congruenza in questione. **(3).** È facile verificare che il quadrato di ogni intero dispari è congruente ad 1 (mod 8) (cfr. Esercizio 1.3(b)). Se, quindi, la congruenza $X^2 \equiv a \pmod{2^e}$ $(e \geqslant 3)$ è risolubile, anche la congruenza $X^2 \equiv a \pmod 8$ è risolubile e pertanto, procedendo come sopra, si ottiene che $a \equiv 1 \pmod 8$. Viceversa, assumiamo che $a \equiv 1 \pmod 8$ e procediamo per induzione su e. Se $e = 3$, la congruenza $X^2 \equiv a \pmod 8$ è certamente risolubile. Supponiamo ora che $e \geqslant 4$ e che $X^2 \equiv a \pmod{2^{e-1}}$ sia risolubile. Se y ne è una soluzione, si ha $y^2 = a + b2^{e-1}$, per un qualche $b \in \mathbb{Z}$. Poichè a è dispari, anche y è dispari e, pertanto, la seguente congruenza lineare nell'indeterminata T:

$$yT \equiv -b \pmod 2$$

ammette un'unica soluzione $t \pmod 2$. Si pone allora:

$$x := x_t := y + t2^{e-2}$$

e si verifica, facilmente, che x è una soluzione della congruenza $X^2 \equiv a \pmod{2^e}$. Infatti, si ha $yt2^{e-2} \equiv -b \cdot 2^{e-1} \pmod{2^e}$, $2e - 4 \geqslant e$ e dunque $x^2 = a + b2^{e-1} + yt2^{e-1} + t^2 2^{2e-4} \equiv a \pmod{2^e}$. □

Osservazione 6.33. Si noti che nella dimostrazione del punto (3) del Teorema 6.32 si ha che se b è pari allora risulta $t \equiv 0 \pmod 2$; se b è dispari, $t \equiv 1 \pmod 2$. Ne primo caso $x = y$ e nel secondo $x = y + 2^{e-2}$.

Corollario 6.34. *Sia* a *un intero dispari. Allora:*

(1) *La congruenza* $X^2 \equiv a \pmod 2$ *ha un'unica soluzione;*

(2) *Se la congruenza* $X^2 \equiv a \pmod 4$ *è risolubile, allora ha esattamente due soluzioni distinte (cioè incongruenti (modulo* 4*));*

(3) *Se la congruenza* $X^2 \equiv a \pmod{2^e}$*,* $e \geqslant 3$ *è risolubile, allora ha esattamente quattro soluzioni distinte (cioè incongruenti (modulo* 2^e*)).*

Dimostrazione. (1) e **(2)** sono del tutto evidenti. Dimostriamo **(3)** seguendo la linea dimostrativa del Corollario 6.31.

Innanzitutto, se x_0 è una soluzione di

$$X^2 \equiv a \pmod{2^e} \quad e \geqslant 3, \tag{7}$$

si verifica subito che:

$$x_0, \quad -x_0, \quad x_0 + 2^{e-1}, \quad -x_0 + 2^{e-1}$$

sono quattro soluzioni distinte di (7). Proviamo, per induzione su e, che (7) ammette soltanto quattro soluzioni distinte. Se $e = 3$, allora possiamo porre $a = 1$ (in quanto, $a \equiv 1 \pmod 8$, cfr. Teorema 6.32(3)), ed è evidente che $X^2 \equiv 1 \pmod 8$ ha soltanto quattro soluzioni distinte (cioè: $1, 3, 5, 7 \pmod 8$). Sia $e \geqslant 4$ e supponiamo che l'asserto sia vero per l'esponente $e - 1$. Denotiamo con y_0, y_1, y_2, y_3 le quattro soluzioni distinte di

$$X^2 \equiv a \pmod{2^{e-1}} \tag{8}$$

Procedendo come nel Teorema 6.32, y_i $(0 \leqslant i \leqslant 3)$ determina la soluzione di (7):

$$x_i := y_i + t_i 2^{e-2},$$

dove si è posto $y_i^2 = a + b_i 2^{e-1}$ $(b_i \in \mathbb{Z})$ e t_i soluzione della congruenza $y_i T \equiv -b_i \pmod 2$. A partire da una qualsiasi scelta di i, con $0 \leqslant i \leqslant 3$, gli interi $x_i, -x_i, x_i + 2^{e-1}, -x_i + 2^{e-1}$ sono quattro soluzioni distinte di (7) (cfr. anche Osservazione 6.33). Per concludere basta verificare che se x è una soluzione di (7), allora x è congruente (modulo 2^e) ad una di tali soluzioni. Poiché x è anche soluzione di (8), esiste un unico intero i $(0 \leqslant i \leqslant 3)$ tale che $x \equiv y_i \pmod{2^{e-1}}$. Inoltre non è restrittivo assumere che $1 \leqslant x < 2^e$ e $1 \leqslant y_i < 2^{e-1}$ e quindi risulta necessariamente $x = y_i$ oppure $x = y_i + 2^{e-1}$. Nel primo caso, $y_i^2 \equiv a \pmod{2^e}$, quindi si vede facilmente che $x_i = y_i$ e, pertanto, $x \equiv x_i \pmod{2^e}$. Nel secondo caso si hanno due alternative:

(a) se $x_i = y_i$, allora $x \equiv x_i + 2^{e-1} \pmod{2^e}$;

(b) se $x_i = y_i + 2^{e-2}$, allora dal fatto che $x^2 \equiv (x_i)^2 \pmod{2^e}$ si ricava facilmente che $y_i \equiv 0 \pmod 2$ e ciò è assurdo in quanto a (e, quindi, y_i) è dispari. $\square$

Osservazione 6.35. Vogliamo commentare la dimostrazione del teorema precedente, anche alla luce del Teorema 4.6.
Innanzitutto, osserviamo che, con le notazioni sopra introdotte, per ogni j fissato, con $0 \leqslant j \leqslant 3$, risulta:

$$\{x_j, -x_j, x_j + 2^{e-1}, -x_j + 2^{e-1}\} = \{x_i, -x_i, x_i + 2^{e-1}, -x_i + 2^{e-1} : 0 \leqslant i \leqslant 3\}.$$

Inoltre $\{x_0, x_1, x_2, x_3\}$ non coincide, in generale, con l'insieme $\{x_j, -x_j, x_j + 2^{e-1}, -x_j + 2^{e-1}\}$ delle soluzioni distinte di $X^2 \equiv a \pmod{2^e}$.
Per esemplificare quanto osservato sopra, descriviamo più dettagliatamente, il passaggio dalla congruenza $X^2 \equiv a \pmod 8$ alla congruenza $X^2 \equiv a \pmod{16}$.
Nel caso risolubile, cioè $a \equiv 1 \pmod 8$, denotiamo con $\{y_0 = 1, y_1 = 3, y_2 = 5, y_3 = 7\}$ le soluzioni della congruenza $X^2 \equiv 1 \pmod 8$. Quindi se $a \equiv 1 \pmod 8$ abbiamo due congruenze risolubili $\pmod{16}$.

Caso 1: $X^2 \equiv 1 \pmod{16}$.
Conserviamo le notazioni della dimostrazione del Corollario 6.34. Allora, $b_0 = 0, b_1 = 1, b_2 = 3, b_3 = 6$, quindi $t_0 = 0, t_1 = 1, t_2 = 1, t_3 = 0$, pertanto $x_0 = 1, x_1 = 7, x_2 = 9, x_3 = 7$. Mentre l'insieme delle soluzioni distinte $X^2 \equiv 1 \pmod{16}$ è dato da:

$$\{1, -1, 9, -9\} = \{1, 15, 9, 7\} = \{x_j, -x_j, x_j + 8, -x_j + 8\}$$

per ogni scelta di j, con $0 \leqslant j \leqslant 3$. Inoltre, esaminando il problema con l'ottica del Teorema 4.6, abbiamo che $y_0 = 1$ e $y_3 = 7$ sono anche soluzioni della congruenza $\pmod{2^4}$ e quindi ciascuna di queste determina due soluzioni $\pmod{2^4}$ date da:

$$y_0 = 1, y_0 + 2^3 = 8, y_1 = 7, y_1 + 2^3 = 15$$

(II Caso del Teorema 4.6). Mentre $y_1 = 3$ e $y_2 = 5$ non sono soluzioni della congruenza $\pmod{2^4}$ e, quindi, non determinano alcuna soluzione della congruenza $\pmod{2^4}$ (III Caso del Teorema 4.6).

Caso 2: $X^2 \equiv 9 \pmod{16}$.
In questo caso, $b_0 = 1, b_1 = 0, b_2 = 2, b_3 = 5$, quindi $t_0 = 1, t_1 = 0, t_2 = 0, t_3 = 1$, pertanto $x_0 = 5, x_1 = 3, x_2 = 5, x_3 = 11$. Mentre l'insieme delle soluzioni distinte $X^2 \equiv 9 \pmod{16}$ è dato da:

$$\{3, -3, 11, -11\} = \{3, 13, 11, 5\} = \{x_j, -x_j, x_j + 8, -x_j + 8\}$$

per ogni scelta di j, con $0 \leqslant j \leqslant 3$. Inoltre le soluzioni $y_1 = 3$ e $y_2 = 5$ della congruenza $X^2 \equiv 1 \pmod{8}$ determinano ciscuna due soluzioni della congruenza $X^2 \equiv 9 \pmod{16}$ e cioè

$$y_1 = 3, y_1 + 2^3 = 11, y_2 = 5, y_2 + 2^3 = 13.$$

Mentre le soluzioni y_0 e y_3 non determinano soluzioni della congruenza $X^2 \equiv 9 \pmod{16}$.

Possiamo riassumere nel seguente teorema i risultati sopra ottenuti.

Teorema 6.36. *Sia n un intero $\geqslant 2$ che ammette la seguente fattorizzazione in primi distinti:*

$$n = 2^{e_0} p_1^{e_1} \dots p_r^{e_r}.$$

Sia a un intero tale che $\mathrm{MCD}(a, n) = 1$. *Allora, la congruenza*

$$X^2 \equiv a \pmod{n} \tag{4}$$

è risolubile se, e soltanto se, le seguenti due condizioni sono soddisfatte:
(1) $(\frac{a}{p_1}) = \dots = (\frac{a}{p_r}) = 1$;
(2) $\begin{cases} a \text{ dispari}, & \text{se } e_0 = 1; \\ a \equiv 1 \pmod{4}, & \text{se } e_0 = 2 \ (\text{cioè se } 4 \mid n \text{ e } 8 \nmid n); \\ a \equiv 1 \pmod{8}, & \text{se } e_0 \geqslant 3 \ (\text{cioè se } 8 \mid n). \end{cases}$

Dimostrazione. È una semplice congruenza dei Teoremi 4.1, 6.29, 6.32. □

Corollario 6.37. *Con le notazioni del Teorema 6.36, se la congruenza* (4) *è risolubile, il numero delle sue soluzioni distinte (cioè, incongruenti* (mod n)*) è dato da:*

$$\begin{cases} 2^r & \text{se } e_0 \leqslant 1, \\ 2^{r+1} & \text{se } e_0 = 2, \\ 2^{r+2} & \text{se } e_0 \geqslant 3. \end{cases}$$

Dimostrazione. È una semplice conseguenza dell'Osservazione 4.2 e dei Corollari 6.31 e 6.34. □

Osservazione 6.38. Come applicazione del Teorema 6.36, vogliamo studiare la risolubilità dell'equazione diofantea in due indeterminate X e Y:

$$aX^2 + bY + c = 0 \quad \text{con } a, b, c \in \mathbb{Z} \tag{9}$$

Se $a = 0$ (e $b \neq 0$), (9) è risolubile se, e soltanto se, $b \mid c$; se $b = 0$ (e $a \neq 0$), (9) è risolubile se, e soltanto se, $\frac{-c}{a}$ è il quadrato di un numero intero. Supponiamo, ora, che $a \neq 0$ e $b \neq 0$. In tal caso (9) è risolubile se, e soltanto se,

$$aX^2 \equiv -c \pmod{b} \tag{10}$$

è risolubile.
Supponiamo allora che la congruenza quadratica (10) sia risolubile e poniamo $d :=\text{MCD}(a, b)$. Allora risulta che $d \mid c$ e perciò, indicati con $\bar{a}, \bar{b}, \bar{c}$ gli interi tali che

$$a = \bar{a}d, \qquad b = \bar{b}d, \qquad c = \bar{c}d,$$

è immediato che la risolubilità di (9) equivale alla risolubilità di:

$$\bar{a}X^2 + \bar{b}Y + \bar{c} = 0 \quad \text{con MCD}(\bar{a}, \bar{b}) = 1. \tag{11}$$

In tal caso, la risolubilità di (11) equivale alla risolubilità della congruenza: $\bar{a}X^2 \equiv -\bar{c} \pmod{\bar{b}}$. Denotiamo, allora, con $\bar{a}^*$ un inverso aritmetico di $\bar{a}$ (mod $\bar{b}$) e posto $-\bar{c} \cdot \bar{a}^* =: e$, questa ultima congruenza è equivalente alla congruenza:

$$X^2 \equiv e \pmod{\bar{b}} \tag{12}$$

e per stabilire se (12) è risolubile basta applicare il Teorema 6.36.

In particolare, l'equazione diofantea:

$$X^2 - pY - c = 0,$$

con p primo dispari e $c \in \mathbb{Z}$, è risolubile se, e soltanto se, $(\frac{c}{p}) = 1$. Ad esempio, quindi, l'equazione diofantea $X^2 - 3Y + 1 = 0$ non è risolubile;

mentre $X^2 + pY - 5 = 0$ è risolubile per un primo p dispari se e soltanto se, $p \equiv 1, 4 \pmod 5$.

"Geometricamente" questo fatto si traduce nell'esistenza di parabole del piano che non contengono alcun punto a coordinate intere (ad esempio $X^2 + 3Y - 5 = 0$) oppure che ne contengono infiniti (ad esempio $X^2 + 11Y - 5 = 0$).

Il matematico tedesco C.G. Jacobi (1804 - 1851) ha introdotto un simbolo (noto come simbolo di Jacobi) che generalizza il simbolo di Legendre e ne estende alcune proprietà.

Definizione 6.39. Siano a, n interi tali che $n > 1$ e $\mathrm{MCD}(a, n) = 1$. Posto $n = p_1 p_2 \dots p_r$, con $p_1, p_2, \dots, p_r$ primi non necessariamente a due a due distinti, si chiama *simbolo di Jacobi* il simbolo così definito:

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)$$

dove $(\frac{a}{p_i})$ per $1 \leqslant i \leqslant r$ è l'usuale simbolo di Legendre.

Proposizione 6.40. *Siano n, m interi dispari tali che $n > 1, m > 1$; siano inoltre a, b interi relativamente primi con n e con m. Risulta:*

(a) $a \equiv b \pmod n \Rightarrow (\frac{a}{n}) = (\frac{b}{n})$;

(b) $(\frac{ab}{n}) = (\frac{a}{n}) \cdot (\frac{b}{n})$;

(c) $(\frac{a}{nm}) = (\frac{a}{n}) \cdot (\frac{a}{m})$;

(d) $(\frac{a}{n^2}) = (\frac{a^2}{n}) = 1$;

(e) $(\frac{1}{n}) = 1$;

(f) $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$;

(g) $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$. *In particolare,* $(\frac{2}{n}) = 1$ *se, e soltanto se* $n \equiv \pm 1 \pmod 8$.

(h) (Legge di Reciprocità Quadratica; forma generalizzata). *Siano n, m interi dispari tali che $n > 1, m > 1$ e $\mathrm{MCD}(n, m) = 1$. Allora:*

$$\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}}.$$

Dimostrazione. Per verificare **(a), ... , (e)** basta utilizzare la definizione del simbolo di Jacobi e le proprietà del simbolo di Legendre.
(f). Sia $n = p_1 \cdots p_r$. Tenuto conto della Proposizione 6.6(h), basta verificare che

$$\frac{n-1}{2} \equiv \frac{p_1 - 1}{2} + \frac{p_2 - 1}{2} + \cdots + \frac{p_r - 1}{2} \pmod 2.$$

Infatti, risulta $n = [(p_1-1)+1]\dots[(p_r-1)+1] = 4k+1+(p_1-1)+\cdots+(p_r-1)$ per un qualche $k \in \mathbb{N}$, perché $4 \mid (p_i-1)(p_j-1))$, con $1 \leqslant i \neq j \leqslant r$. Da ciò segue banalmente la congruenza voluta. **(g)**. Si procede come in (f). Tenuto conto del Corollario 6.14, basta verificare che:

$$\frac{n^2-1}{8} \equiv \frac{p_1^2-1}{8} + \cdots + \frac{p_r^2-1}{8} \pmod 2.$$

Infatti $n^2 = [(p_1^2-1)+1]\dots[(p_r^2-1)+1] = 16h+1+(p_1^2-1)+\cdots+(p_r^2-1)$ per un qualche $h \in \mathbb{N}$, perché $4 \mid (p_i^2-1)$ e quindi $16 \mid (p_i^2-1)(p_j^2-1)$, con $1 \leqslant i \neq j \leqslant r$. Da ciò segue l'asserto. **(h)**. Sia $n = p_1 \cdots p_r$ e $m = q_1 \cdots q_s$. Tenuto conto del Teorema 6.21, si ha:

$$\begin{aligned}\left(\frac{n}{m}\right)\cdot\left(\frac{m}{n}\right) &= \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right)\cdot\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)\cdot\left(\frac{q_j}{p_i}\right) = \\ &= \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{(\frac{p_i-1}{2}\cdot\frac{q_j-1}{2})} = \\ &= (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}(\frac{p_i-1}{2}\cdot\frac{q_j-1}{2})} = \\ &= (-1)^{(\sum_{i=1}^{r}(\frac{p_i-1}{2}))\cdot(\sum_{j=1}^{s}(\frac{q_j-1}{2}))}.\end{aligned}$$

Per concludere basta osservare (cfr. dimostrazione di (f)) che:

$$\sum_{i=1}^{r}(\frac{p_i-1}{2}) \equiv \frac{n-1}{2} \pmod 2 \quad \text{e} \quad \sum_{j=1}^{s}(\frac{q_j-1}{2}) \equiv \frac{m-1}{2} \pmod 2. \ \square$$

Osservazione 6.41. Si consideri la congruenza:

$$X^2 \equiv a \pmod n \tag{13}$$

con n dispari, $n > 1$ e $\mathrm{MCD}(a,n) = 1$. È chiaro che (cfr. Teorema 6.36) se (13) è risolubile, allora $(\frac{a}{n}) = 1$. Il viceversa è invece falso (anche se n è un intero per il quale esiste una radice primitiva $\pmod n$). Basta porre $n = 9$ (cfr. Teorema 5.17) ed osservare che $(\frac{2}{9}) = (\frac{2}{3^2}) = 1$, mentre $X^2 \equiv 2 \pmod 9$ non è risolubile (in quanto $(\frac{2}{3}) = -1$, cfr. Teorema 6.29).

Si noti la parziale analogia tra queste considerazioni e quelle svolte nell'Osservazione 6.11.

Possiamo, ora, applicare il simbolo di Jacobi e le sue proprietà per dimostrare il seguente risultato:

Proposizione 6.42. (S. Chowla). *L'equazione diofantea quadratica in una indeterminata X*

$$X^2 = a, \quad \textit{con } a \in \mathbb{Z} \tag{14}$$

è risolubile se, e soltanto se, per ogni primo p la congruenza

$$X^2 \equiv a, \pmod{p} \tag{15}$$

è risolubile.

Dimostrazione. È chiaro che se (14) è risolubile, ogni (15) è risolubile. Viceversa, ammettiamo per assurdo che $a \neq b^2$, per ogni $b \in \mathbb{Z}$. Verificheremo che esiste un intero dispari n tale che $(\frac{a}{n}) = -1$ (e, dunque, che esiste un primo dispari p con $p \mid n$ e tale che $(\frac{a}{p}) = -1$).

Distinguiamo tre casi, che insieme coprono tutte le possibilità per le quali a non è quadrato:

(a) Sia $a = \pm 2^e b$, con b, e interi positivi dispari. Sia n una soluzione del sistema:

$$\begin{cases} X \equiv 5 \pmod{8} \\ X \equiv 1 \pmod{b} \end{cases}$$

Si verifica con facilità che $(\frac{\pm 2}{n}) = -1$ (Proposizione 6.40(f) e (g)), $(\frac{2^{e-1}}{n}) = 1$ e $(\frac{b}{n}) = (\frac{n}{b}) = (\frac{1}{b}) = 1$. Allora $(\frac{a}{n}) = -1 \cdot 1 \cdot 1 = -1$.

(b) Sia $a = \pm 2^{2h} q^k b$, con q, k, b interi dispari, q primo e $q \nmid b$. Sia n una soluzione del sistema:

$$\begin{cases} X \equiv 1 \pmod{4b} \\ X \equiv c \pmod{q} \end{cases}$$

dove c è un intero tale che $(\frac{c}{q}) = -1$. Allora si ha: $(\frac{\pm 1}{n}) = 1$, $(\frac{2^{2h}}{n}) = 1$, $(\frac{b}{n}) = (\frac{n}{b}) = 1$, $(\frac{q^k}{n}) = (\frac{q}{n}) = (\frac{n}{q}) = (\frac{c}{q}) = -1$ e pertanto $(\frac{a}{n}) = -1$.

(c) sia $a = -b^2$, con b intero dispari. Scelto $n \equiv 3 \pmod{4}$ tale che $\mathrm{MCD}(a, n) = 1$, è chiaro che $(\frac{a}{n}) = (\frac{-1}{n}) = -1$. □

Osservazione 6.43. (1) Più generalmente, si dimostra che *l'equazione diofantea $X^n = a$ è risolubile se, e soltanto se, $X^n \equiv a \pmod{p^k}$ è risolubile per ogni p primo e per ogni $k \geqslant 1$.* Anzi, più precisamente è noto che *se $X^n \equiv a \pmod{p}$ è risolubile per ogni p primo, due casi sono possibili:*

1. *Se $8 \nmid n$, allora $X^n = a$ è risolubile;*

2. *Se $8 \mid n$, allora $X^n = a$ è risolubile, oppure $2^{\frac{n}{2}} X^n = a$ è risolubile.*

Il secondo caso, nell'enunciato precedente, si presenta effettivamente, come mostra il seguente esempio: $X^8 \equiv 16 \pmod{p}$ è risolubile, per ogni primo p, però l'equazione diofantea $X^8 = 16$ non è risolubile, mentre è ovviamente risolubile $2^4 X^8 = 16$.

Per maggiori dettagli si veda: E. Trost, Niew Arch. Wisk. **18** (1934), 58-61 od, anche, N.C. Ankeny - C.A. Rogers, Ann. Math. **53** (1951), 541-550. Una prova più algebrica di un caso particolare di tale risultato è stata data

più recentemente da J. Kraft e M. Rosen, Amer. Math. Montly, **88** (1981), 269-270.

(2) Si osservi che, in generale, se

$$aX^2 + bX + c \equiv 0 \pmod{n}$$

è risolubile per ogni $n \geqslant 2$, non è detto che l'equazione diofantea:

$$aX^2 + bX + c = 0$$

sia risolubile. (Ad esempio, $6X^2 + 5X + 1 = 0$ non ha soluzioni intere, mentre $6X^2 + 5X + 1 = (2X + 1)(3X + 1) \equiv 0 \pmod{n}$ è risolubile per ogni $n \geqslant 2$ perché $2X + 1 \equiv 0 \pmod{p}$ oppure $3X + 1 \equiv 0 \pmod{p}$ è risolubile per ogni primo p cioè, perché $p - 1$ è un multiplo di 2 oppure è un multiplo di 3.)

6. Esercizi e Complementi

6.1. Siano $a, b, c \in \mathbb{Z}, a \equiv 1 \pmod 2$. Determinare quando la congruenza $aX^2 + bX + c \equiv 0 \pmod 2$ è risolubile.
[Soluzione. La tabella seguente descrive i vari casi possibili:

b	c	x
0	0	0
0	1	1
1	0	$0, 1$
1	1	$-$

.]

6.2. Verificare che, per ogni primo p, la congruenza $X^2 \equiv 0 \pmod p$ ha un'unica soluzione (mod p).

6.3. Sia a un intero positivo che scriviamo nella forma $a = b^2 d$, con $b, d \in \mathbb{Z}$ e d privo di fattori quadratici. Mostrare che, per ogni p primo dispari tale che $p \nmid a$, risulta $(\frac{a}{p}) = (\frac{d}{p})$.

6.4. (a). Se q è un primo dispari ed r è una radice primitiva (mod q), si ha $(\frac{r}{q}) = -1$.
(b). Siano p, q primi dispari tali che $q = 2p + 1$ e si consideri l'insieme $T := \{a \in \mathbb{Z} : 1 \leqslant a \leqslant q - 1 \text{ e } (\frac{a}{q}) = -1\}$. Verificare che $\#(T) = p$, che $p - 1$ elementi di T sono radici primitive (mod q) e infine che $2p$ è l'unico elemento di T che non è radice primitiva (mod q).
(c). Utilizzando (b), calcolare le radici primitive modulo $7, 11, 23, 47$.
(Si noti che 11 e 23 sono gli unici primi q, tra 7 e 47, del tipo $q = 2p + 1$, con p primo.)
(d). Con le notazioni di (b), dimostrare che $2(-1)^{\frac{p-1}{2}}$ è una radice primitiva (mod q).
(e). Verificare che 2 è una radice primitiva modulo $11, 59$, e 107, mentre -2 è una radice primitiva modulo $7, 23, 47, 159$ e 167.
[Suggerimento. **(a)** segue dalle Proposizioni 6.6(d) e 5.22(d). **(b)** Il primo asserto è conseguenza della Proposizione 6.3 e del fatto che $\frac{q-1}{2} = p$. Per il secondo, cfr. (a) e la Proposizione 5.8. Infine, per il terzo si verifichi che, necessariamente, $q \equiv 3 \pmod 4$ da cui segue che $(\frac{q-1}{q}) = -1$ e $\mathrm{ord}_q(q-1) = 2$. **(c)** Se $q = 7$, $T = \{3, 5, 6\}$, $r = 3, 5$. Se $q = 11$, $T = \{2, 6, 7, 8, 10\}$, $r = 2, 6, 7, 8$. Se $q = 23$, $T = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$, $r = 5, 7, 10, 11, 14, 15, 17, 19, 20, 21$. Se $q = 47$, $T = \{5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45, 46\}$, $r = 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45$. **(d)** Se $p \equiv 1 \pmod 4$, $\frac{p-1}{2}$ è pari e bisogna quindi provare che $\mathrm{ord}_q(2) = 2p$. A priori, $\mathrm{ord}_q(2) = 1, 2, p, 2p$ e bisogna pertanto escludere le prime tre eventualità. Per le prime due è ovvio essendo $q \geqslant 7$, per la terza, si ha $2^p = 2^{\frac{q-1}{2}} \equiv (\frac{2}{q}) \pmod q$ e, essendo $p \equiv 1 \pmod 4$ allora $q \equiv 3 \pmod 8$, dunque $2^p \equiv -1 \pmod q$. Se invece $p \equiv 3 \pmod 4$, bisogna provare che $\mathrm{ord}_q(-2) = 2p$. Procedendo come sopra, essendo $q \equiv 7 \pmod 8$, si ha: $(-2)^p \equiv (\frac{-2}{q}) = (\frac{-1}{q}) \cdot (\frac{2}{q}) \equiv -1 \pmod q$, e da ciò segue l'asserto. **(e)** È una semplice conseguenza di (d).]

6.5. Sia p un primo dispari ed a un intero tale che $\mathrm{MCD}(a,p)=1$. Se $(\frac{a}{p})=1$, allora

$$\left(\frac{p-a}{a}\right)=\begin{cases}1 & \text{se } p\equiv 3 \pmod 4,\\ -1 & \text{se } p\equiv 1 \pmod 4.\end{cases}$$

[Suggerimento: $(\frac{p-a}{a})\equiv(p-a)^{\frac{p-1}{2}}\equiv(-a)^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{2}} \pmod p$.]

6.6. Sia p un primo dispari ed a un intero tale che $\mathrm{MCD}(a,p)=1$. Mostrare che:

$$(p-1)!\equiv-\left(\frac{a}{p}\right)a^{\frac{p-1}{2}} \pmod p.$$

[Suggerimento. Dal Criterio di Eulero segue che $(\frac{a}{p})\equiv a^{\frac{p-1}{2}} \pmod p$, quindi $(\frac{a}{p})a^{\frac{p-1}{2}}\equiv 1 \pmod p$; la conclusione è conseguenza del Lemma di Wilson.]

6.7. Sia p un primo dispari e siano $a,b\in\mathbb{Z}$ tali che $\mathrm{MCD}(a,p)=\mathrm{MCD}(b,p)=1$. Se $(\frac{a}{p})=(\frac{b}{p})$, allora $aX^2\equiv b \pmod p$ è risolubile.
[Suggerimento. Se a^* è l'inverso aritmetico di $a \pmod p$, allora $X^2\equiv a^*b \pmod p$ è risolubile $\iff$ $(\frac{a^*b}{p})=1$ $\iff$ $(\frac{a}{p})=(\frac{b}{p})$.]

6.8. Mostrare che esistono infiniti primi di tipo $4k+1$.
[Suggerimento. Per assurdo, siano $p_1,\dots,p_n$ i soli primi di tipo $4k+1$. L'intero $N:=4(p_1\cdots p_n)+1$ è divisibile per un primo dispari p. Utilizzando la Proposizione 6.6(h), si verifica che $p\equiv 1 \pmod 4$ e che da ciò segue un assurdo.]

6.9. Mostrare che esistono infiniti primi di tipo $8k-1$.
[Suggerimento. Per assurdo, siano $p_1,\dots,p_n$ i soli primi di tipo $8k-1$. L'intero $N:=(4p_1\cdots p_n)^2-2$ ammette certamente un divisore primo p dispari. Ne segue che $(\frac{2}{p})=1$, quindi $p\equiv 1,7 \pmod 8$. Se tutti i divisori primi dispari di N fossero della forma $8k+1$, siccome N è pari risulterebbe $N\equiv 2 \pmod{16}$, mentre $N\equiv -2 \pmod{16}$. Se invece fosse $p\equiv 7\equiv -1 \pmod 8$, allora $p\mid(N-(4p_1\cdots p_n)^2)=2$ e ciò è ugualmente assurdo.]

6.10. Mostrare che esistono infiniti primi del tipo:

(a) $8k+3$;

(b) $8k+5$;

(c) $8k+7$;

(d) $6k+1$.

[Suggerimento. Per ciascuna parte si assuma che esistano un numero finito di primi del tipo indicato. Per la parte **(a)** prendere in esame $N:=(4p_1\cdots p_n)^2-2$, per la parte **(b)** prendere in esame $N:=(p_1\cdots p_n)^2+2$, per la parte **(d)** $N:=(2p_1\cdots p_n)^2+3$. Per **(c)** si noti che $8k+7\equiv 8k-1 \pmod 8$ (cfr. Esercizio 6.9).]

6.11. Sia n un intero dispari ed a un intero tale che $\mathrm{MCD}(a,n)=1$. Mostrare che la risolubilità della congruenza $aX^2+bX+c\equiv 0 \pmod n$ può essere ricondotta alla risolubilità di una congruenza del tipo: $Y^2\equiv d \pmod n$.
[Suggerimento. Si proceda come già fatto all'inizio del Paragrafo 6 per ogni fattore primo p (necessariamente dispari) di n e si tenga conto del Teorema 6.36.]

6.12. Determinare se le seguenti congruenze sono risolubili:

(a) $2X^2 - 5X + 7 \equiv 0 \pmod{21}$

(b) $X^2 + X - 2 \equiv 0 \pmod{35}$

[Soluzione. **(a)** Sia $a = 2, b = -5, c = 7, d = b^2 - 4ac = -31, Y = 2aX + b = 4X - 5$. Poiché $21 = 3 \cdot 7$ è dispari, allora le soluzioni della congruenza data si determinano dalle soluzioni della congruenza

$$Y^2 \equiv -31 \pmod{21} \quad \text{cioè} \quad Y^2 \equiv 11 \pmod{21}.$$

Poiché $(\frac{11}{21}) = (\frac{21}{11}) = (\frac{10}{11}) = (\frac{2}{11})(\frac{5}{11}) = -(\frac{11}{5}) = -(\frac{1}{5}) = -1$, $Y^2 \equiv 11 \pmod{21}$ non è risolubile, pertanto non è risolubile la congruenza data. **(b)** In tal caso $d = 9, Y = 2X + 1, Y^2 \equiv 9 \pmod{35}$ è risolubile in quanto $(\frac{9}{5}) = 1$ e $(\frac{9}{7}) = 1$. Precisamente le soluzioni sono $x = 1, 8, 26, 33 \pmod{35}$.]

6.13. Sia p primo, $p \neq 3$ ed a un intero tale che $\text{MCD}(a, p) = 1$. Mostrare che la congruenza: $aX^3 + bX^2 + cX + d \equiv 0 \pmod{p}$ può essere ricondotta ad una congruenza del tipo: $Y^3 + eY + f \equiv 0 \pmod{p}$.
[Suggerimento. Si moltiplichi la congruenza assegnata per a^* e si ponga $X = Y - 3^* a^* b$.]

6.14. Mostrare che p è un qualsiasi primo dispari, allora:

$$\left(\frac{2}{p}\right) = \left(\frac{8-p}{p}\right) = \left(\frac{p}{p-8}\right) = \left(\frac{2}{p-8}\right).$$

[Suggerimento. Utilizzando la Proposizione 6.40 si ha: $(\frac{8-p}{p}) = (\frac{8}{p}) = (\frac{2 \cdot 4}{p}) = (\frac{2}{p})$, $(\frac{p}{p-8}) = (\frac{8}{p-8}) = (\frac{2}{p-8})$, $(\frac{2}{p}) = (\frac{2}{p-8})$ perché $p \equiv p - 8 \pmod{8}$.]

6.15. Sia $k \geqslant 2$ e sia $p = 4k + 3$ un numero primo. Mostrare che:

(a) $2p + 1$ è primo $\iff 2^p \equiv 1 \pmod{(2p+1)}$.

(b) Se $2p+1$ è primo, il numero $M_p := 2^p - 1$ (detto *p-esimo numero di Mersenne*) è composto.

[Suggerimento. **(a, $\Rightarrow$)**. Basta osservare che $2^p = 2^{\frac{2p+1-1}{2}} \equiv (\frac{2}{2p+1}) = 1$ (modulo $2p + 1$) per il Criterio di Euler, essendo $2p + 1 \equiv 7 \pmod{8}$. **(a, $\Leftarrow$)**. Poniamo $n := 2p + 1$. Se $2^p \equiv 1 \pmod{n}$, allora necessariamente $p = \text{ord}_n(2)$ e quindi $p \mid \varphi(n)$. Se $n = p_1^{e_1} \cdots p_r^{e_r}$ allora $p \mid \big(\prod_{i=1}^r p_i^{e_i - 1} \cdot (p_i - 1)\big)$. Poiché si vede subito che $p \nmid p_i$, per ogni i, allora $p \mid (p_i - 1)$, per qualche i. D'altro lato $2p + 1 = p_i \cdot n'$ dove $n' := \frac{n}{p_i}$. Se $n' > 1$, allora è subito visto che deve essere $n' > 2$, e quindi si avrebbe che $p \nmid (p_i - 1)$, poché avremmo che $p > p_i - 1$, e ciò è assurdo. Pertanto $n' = 1$, cioè $2p + 1 = p_i$ è un primo. **(b)**. È una semplice conseguenza di (a).]

6.16. Sia p un primo dispari. Mostrare che $X^4 \equiv -4 \pmod{p}$ è risolubile se e soltanto se $p \equiv 1 \pmod{4}$.
[Suggerimento. Si noti che $X^4 + 4 = ((X+1)^2 + 1)((X-1)^2 + 1)$. Pertanto $X^4 \equiv -4 \pmod{p}$ è risolubile se e soltanto se almeno una delle congruenze $((X+1)^2 + 1) \equiv 0 \pmod{p}$ oppure $((X-1)^2 + 1) \equiv 0 \pmod{p}$ è risolubile. È subito che entrambe sono risolubili se e soltanto se $(\frac{-1}{p}) = 1$.]

6.17. Calcolare i seguenti simboli di Jacobi:

$$\textbf{(a)}\ \left(\frac{713}{1009}\right); \qquad \textbf{(b)}\ \left(\frac{111}{991}\right); \qquad \textbf{(c)}\ \left(\frac{313}{367}\right).$$

[Soluzione. **(a)** Si noti che $1009 \equiv 1 \pmod 4$ ed è primo e che $713 = 23 \cdot 31$.

$$\begin{aligned}
\left(\frac{23}{1009}\right) &= \left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) = \\
&= \left(\frac{4}{23}\right)\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1, \\
\left(\frac{31}{1009}\right) &= \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \\
&= \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = \\
&= -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1
\end{aligned}$$

quindi $(\frac{713}{1009}) = 1$. **(b)**: -1. **(c)**: 1.]

6.18. Determinare il numero delle soluzioni della congruenza

$$X^2 \equiv 4 \pmod{105}.$$

[Soluzione. Poiché $105 = 3 \cdot 5 \cdot 7$ e ciascuna delle congruenze $X^2 \equiv 4 \pmod 3, X^2 \equiv 4 \pmod 5, X^2 \equiv 4 \pmod 7$ ha due soluzioni, allora la congruenza data ha 2^3 soluzioni (mod 105): $2, 23, 37, 47, 58, 68, 82, 103$.]

6.19. (Gauss).Sia p un primo dispari. Siano $n, n+1$ due interi consecutivi nel sistema ridotto di residui $S^* := \{1, 2, \ldots, p-1\}$. Denotiamo con (RR) (rispettivamente: (RN); (NR); (NN)) il numero delle coppie di interi consecutivi $(n, n+1)$ di S^* tali che $(\frac{n}{p}) = 1$ e $(\frac{n+1}{p}) = 1$ (rispettivamente: $(\frac{n}{p}) = 1$ e $(\frac{n+1}{p}) = -1$; $(\frac{n}{p}) = -1$ e $(\frac{n+1}{p}) = 1$; $(\frac{n}{p}) = -1$ e $(\frac{n+1}{p}) = -1$). I seguenti enunciati mostrano che la distribuzione dei residui e dei non residui quadratici è essenzialmente casuale, in quanto ciascuna delle quattro possibilità si presenta con una frequenza pressoché uguale (cioè $\left[\frac{1}{4}(p-1)\right]$).
Poniamo $\varepsilon := (-1)^{\frac{p-1}{2}} = (\frac{-1}{p}) = (\frac{p-1}{p})$. Mostrare che:

(1) (RR) + (RN) $= \frac{1}{2}(p - 2 - \varepsilon)$;

(2) (NR) + (NN) $= \frac{1}{2}(p - 2 + \varepsilon)$;

(3) (RR) + (NR) $= \frac{1}{2}(p-1) - 1 = \frac{1}{2}(p-3)$;

(4) (RN) + (NN) $= \frac{1}{2}(p-1)$;

(5) $\sum_{n=1}^{p-2}(\frac{n(n+1)}{p}) = -1$;

(6) (RR) + (NN) - (RN) - (NR) $= -1$;

(7) (RR) + (NN) $= \frac{1}{2}(p-3)$;

(8) (RR) - (NN) $= -\frac{1}{2}(1+\varepsilon)$;

(9) (RR) = $\frac{1}{4}(p-4-\varepsilon)$;

(10) (NN) = $\frac{1}{4}(p-2+\varepsilon)$;

(11) (RN) + (NR) = $\frac{1}{2}(p-1)$;

(12) (RN) - (NR) = $1-\frac{1}{2}(1+\varepsilon)=\frac{1}{2}(1-\varepsilon)$;

(13) (RN) = $\frac{1}{4}(p-\varepsilon)$;

(14) (NR) = $\frac{1}{4}(p-2+\varepsilon)$.

[Suggerimento. **(1)** Il numero (RR) + (RN) è il numero delle coppie $(n, n+1)$ per cui n è un residuo quadratico, dove n varia tra 1 e $p-2$. Quindi tale numero dipende dal valore di

$$\left(\frac{p-1}{p}\right)=\left(\frac{-1}{p}\right)=\varepsilon.$$

Se $p-1$ è un non residuo quadratico, cioè se $\varepsilon=-1$, allora i residui quadratici sono tutti tra gli interi $\{1,2,\ldots,p-2\}$ e quindi (RR) + (RN) = $\frac{1}{2}(p-1)$. Se $p-1$ è un residuo quadratico, cioè $\varepsilon=1$, allora i residui quadratici tra gli interi $\{1,2,\ldots,p-2\}$ sono $\frac{1}{2}(p-1)-1=\frac{1}{2}(p-3)$.
Similmente si dimostrano **(2)**, **(3)** e **(4)**.
(5) Se n^* è un inverso aritmentico di n allora:

$$n(n+1)=n^2+n\equiv n^2(1+n^*) \pmod{p}$$

e quindi

$$\sum_{n=1}^{p-2}\left(\frac{n(n+1)}{p}\right)=\sum_{n=1}^{p-2}\left(\frac{1+n^*}{p}\right)=\sum_{n=2}^{p-1}\left(\frac{n}{p}\right).$$

Poichè

$$\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)=0,$$

allora

$$\sum_{n=2}^{p-1}\left(\frac{n}{p}\right)=-\left(\frac{1}{p}\right)=-1.$$

(6) segue da (5).
(7) e **(8)** sono semplici conseguenze di (6), (1), e (2).
(9) e **(10)** seguono da (7) e (8).
(11) e **(12)** seguono da (3) e (4) e dal fatto che (RN) - (NR) + (NN) - (RR) =1.
(13) e **(14)** seguono immediatamente da (11) e (12).]

Parte II

L'utilizzo di *Mathematica* nella teoria delle congruenze

1 Proprietà elementari delle congruenze

1.1 Congruenze e Calendario

Le congruenze possono essere trattate anche da un punto di vista "geometrico". Generalmente, per rappresentare (geometricamente) i numeri interi ($\mathbb{Z}$), si sceglie un segmento con lunghezza unitaria e lo si prolunga verso destra e verso sinistra mediante multipli del segmento di partenza (cfr. Figura 1). In tal modo si può trovare sulla retta un punto corrispondente a ciascuno dei numeri interi.

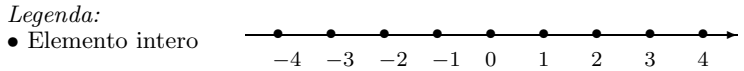


Figura 1: rappresentazione geometrica di $\mathbb{Z}$

Ma quando si tratta di numeri interi (modulo d), due numeri congrui sono considerati identici per quanto riguarda il loro comportamento nella divisione per d, poiché danno lo stesso resto. Per rappresentare questo geometricamente, useremo una circonferenza divisa in d parti uguali (cfr. Figura 2 per $d = 4$).
Un qualsiasi numero intero diviso per d dà come resto uno dei d numeri $0, 1, 2, \ldots, d-1$, situati ad intervalli uguali sulla circonferenza. Ogni altro numero intero è congruo modulo d a uno di questi numeri, e perciò è rappresentato geometricamente da uno di questi punti; due numeri sono congrui se sono rappresentati dallo stesso punto.

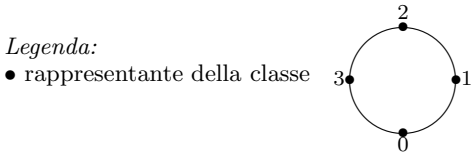


Figura 2: rappresentazione geometrica degli interi (modulo 4)

Il quadrante dell'orologio è un altro esempio tratto dalla vita di tutti i giorni. Se si devono calcolare i minuti sul quadrante corrispondenti a 40 minuti più 35 minuti, quello che facciamo non è altro che risolvere la seguente congruenza: $40 + 35 \equiv x \pmod{60}$ dove $x = 15$ minuti.
Anche nel calcolo delle ore pomeridiane su un quadrante di un orologio applichiamo le congruenze. Se aggiungiamo, infatti, 5 ore alle 10 a.m. otteniamo le 15 che nella congruenza (modulo 12) risultano essere le 3 p.m.

Un'applicazione pratica delle congruenze è il *calcolo del giorno della settimana corrispondente alla data assegnata.*
Per prima cosa ricordiamo le regole che si utilizzano per la definizione degli anni bisestili. Nel *Calendario Gregoriano*, gli anni con 366 giorni sono quelli che risultano divisibili per 4, fanno eccezione tutti gli inizi di secolo (divisibili per 100) che non siano a loro volta divisibili per 400. Per esempio il

1900 ha 365 giorni, mentre il 2000 è bisestile.
È opportuno ricordare che *il numero dei naturali minori di* $n \in \mathbb{N}$ *divisibili per un naturale* d *è pari al più grande intero* u *tale che* $ud \leqslant n$ *cioè* $u = \frac{n}{d}$ *(indicheremo* $u = \left[\frac{n}{d}\right]$*).* [2]

Consideriamo quindi il seguente problema: calcolare il giorno della settimana a cui corrisponde una data assegnata.
Indichiamo con $n+1$ l'anno preso in considerazione e con m il numero corrispondente al giorno che stiamo considerando (per convenzione: il Primo Gennaio dell'anno 1 si è fissato uguale a Lunedì) così che risulti $1 \leqslant m \leqslant 366$.
Applichiamo ora le seguente formula:

$$H = n \cdot 365 + \left(\left[\frac{n}{4}\right] - \left[\frac{n}{100}\right] + \left[\frac{n}{400}\right]\right) + m.$$

dove

$$\left[\frac{n}{4}\right] - \left[\frac{n}{100}\right] + \left[\frac{n}{400}\right] =$$

$=$ numero degli anni bisestili precedenti all'anno preso in esame.

Calcoliamo quale valore assume $H \pmod 7$ ed associamo al risultato il giorno della settimana come dalla seguente tabella:

0	Domenica
1	Lunedì
2	Martedì
3	Mercoledì
4	Giovedì
5	Venerdì
6	Sabato

Per semplificare il calcolo osserviamo che $365 \equiv 1 \pmod 7$.

Esempio. *Calcolare a che giorno della settimana corrisponde il* 5 *Giugno* 2000.
I valori che associamo alle incognite in questo caso sono:

$$n = 1999 \quad \text{e} \quad m = 157.$$

Visto che $n \equiv 4 \pmod 7$ otteniamo:

$$\begin{aligned} H &= 4 \cdot 1 + \left[\frac{1999}{4}\right] - \left[\frac{1999}{100}\right] + \left[\frac{1999}{400}\right] + 157 \equiv \\ &\equiv 4 + 499 - 19 + 4 + 157 = \\ &= 645 \equiv 1 \pmod 7, \end{aligned}$$

Quindi il 5 Giugno 2000 sarà un Lunedì.

[2] Si tratta della definizione di *parte intera*

1.2 Congruenze e mcm

Nella Proposizione *1.9* abbiamo dato una proprietà delle congruenze legata al MCD. Diamone ora una legata al mcm.
Prima però è opportuno ricordare la seguente caratterizzazione del mcm.

Teorema 1. *Siano a, b interi non nulli, allora:*

$$\text{mcm}(a,b) = \frac{ab}{\text{MCD}(a,b)}.$$

Dimostrazione. Se $\text{MCD}(a,b) = 1$ cioè se a, b sono coprimi, la conclusione è ovvia.
Se $\text{MCD}(a,b) = d \neq 1$ allora sappiamo che se $a = \prod_p p^{e_p}$ e $b = \prod_p p^{f_p}$:

$$d = \prod_p p^{\min\{e_p, f_p\}}$$

da cui:

$$\frac{ab}{\text{MCD}(a,b)} = \frac{\prod_p p^{e_p+f_p}}{\prod_p p^{\min\{e_p,f_p\}}} = \prod_p p^{\max\{e_p,f_p\}} = \text{mcm}(a,b). \square$$

Proposizione 2. *Se $a \equiv b \pmod{m_1}$ e $a \equiv b \pmod{m_2}$ allora:*

$$a \equiv b \pmod{\text{mcm}(m_1, m_2)}.$$

Dimostrazione. Le due congruenze di partenza ci dicono che $a - b = k_i m_i$ con $i = 1, 2$. Se indichiamo con $d :=\text{MCD}(m_1, m_2)$ abbiamo che:

$$\text{mcm}(m_1, m_2) = \frac{m_1 m_2}{d}$$

A questo punto, tenuto conto che $\text{MCD}(\frac{m_1}{d}, \frac{m_2}{d}) = 1$, applicando il Lemma di Euclide [3] otteniamo che $\frac{m_i}{d} \mid k_j$ con $i \neq j$ e quindi esiste un intero k tale che:

$$a = b + \frac{k m_1 m_2}{d} \equiv b \pmod{\text{mcm}(m_1, m_2)}. \square$$

1.3 Ulteriori criteri di divisibilità

Abbiamo visto già come le congruenze possano aiutare nel determinare alcuni criteri di divisibilità. Diamo qui di seguito ulteriori criteri.

Teorema 3. *Sia $n \in \mathbb{N}$ tale che $n = d_k \cdot 10^k + \cdots + d_1 \cdot 10 + d_0$. Avremo che:*

$$n \equiv d_k + \cdots + d_1 + d_0 \pmod{9}.$$

[3] **Lemma di Euclide**
Siano $a, b, c \in \mathbb{Z}$ tali che $\text{MCD}(a,b) = 1$ e $a \mid bc$ allora $a \mid c$.

Dimostrazione. Discende banalmente dal criterio di divisibilità per 9 (cfr. Teorema *1.17*).
Sia $n \in \mathbb{N}$ e con la seguente scrittura decimale: $n = d_k \dots d_1 d_0$. Passiamo alla congruenza (modulo 9) ed otteniamo:

$$n = d_k \cdot 10^k + \cdots + d_1 \cdot 10 + d_0 \equiv d_k + \cdots + d_1 + d_0 \pmod 9$$

visto che $10 \equiv 1 \pmod 9$ e quindi $10^m \equiv 1^m \equiv 1 \pmod 9$. □

Il teorema appena enunciato è alla base della cosìdetta "prova del nove" che fornisce una condizione necessaria ma non sufficiente per la validità di uguaglianze numeriche.

Esempio. *Verificare se* $(314) \cdot (159) = 49826$ *senza effettuare la moltiplicazione.*
Calcoliamo le due congruenze (modulo 9).

$$\begin{aligned}(314) \cdot (159) &\equiv (3+1+4) \cdot (1+5+9) = 8 \cdot 15 \equiv \\ &\equiv 8 \cdot (1+5) = 8 \cdot 6 = 48 \equiv 4+8 = 12 \equiv \\ &\equiv 1+2 = 3 \pmod 9\end{aligned}$$

mentre

$$\begin{aligned}49826 &\equiv 4+9+8+2+6 = 29 \equiv \\ &\equiv 2+9 = 11 \equiv 1+1 = 2 \pmod 9\end{aligned}$$

Risulta quindi che i due numeri non sono uguali.
Si ha infatti che $(314) \cdot (159) = 49926$.

Esempio. *Utilizzando lo stesso procedimento dell'esempio precedente trovare la cifra che manca affinché si abbia:*

$$(31415) \cdot (92653) = 2910\diamond 93995.$$

Calcoliamo le due congruenze (modulo 9).

$$\begin{aligned}(31415) \cdot (92653) &\equiv (3+1+4+1+5) \cdot (9+2+6+5+3) = \\ &= 14 \cdot 25 \equiv (1+4) \cdot (2+5) = 5 \cdot 7 = \\ &= 35 \equiv 3+5 = 8 \pmod 9\end{aligned}$$

mentre

$$\begin{aligned}2910\diamond 93995 &\equiv 2+9+1+0+\diamond+9+3+9+9+5 = \diamond + 47 \equiv \\ &\equiv \diamond + 4 + 7 = \diamond + 11 \equiv \diamond + 1 + 1 = \diamond + 2 \pmod 9\end{aligned}$$

Quindi perché valga l'uguaglianza si deve porre $\diamond = 6$.

Utilizzando il criterio di Pascal, diamo ora altre caratterizzazioni per quanto riguarda i criteri di divisibilità.

Considerando le ipotesi del Teorema *1.17* si ha:

Criterio di divisibilità per 6. Osserviamo che:

$$10 \equiv -2 \pmod 6,\ 10^2 \equiv -2 \pmod 6, \dots, 10^n \equiv -2 \pmod 6$$

quindi:

$$N = a_0 + 10a_1 + \cdots + 10^n a_n \equiv a_0 - \sum_{i=1}^{n} a_i =: r$$

da cui:

$$\boxed{6 \mid N \iff 6 \mid r \iff a_0 \text{ pari e } 3 \mid N}$$

Infatti, visto che $6 = 2 \cdot 3$, se $6 \mid N$ si avrà che $2 \mid N$ (cioè a_0 è pari) e $3 \mid N$. Se invece N è tale che a_0 è pari (cioè $2 \mid N$) e $3 \mid N$ si ha che $2 \cdot 3 = 6 \mid N$.

Criterio di divisibilità per 7. Osserviamo:

$$\begin{aligned} 10^1 &\equiv 3 \pmod 7, & 10^2 &\equiv 2 \pmod 7, & 10^3 &\equiv -1 \pmod 7, \\ 10^4 &\equiv -3 \pmod 7, & 10^5 &\equiv -2 \pmod 7, & 10^6 &\equiv 1 \pmod 7. \end{aligned}$$

da cui si ottiene:

$$N \equiv r := (a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5) + (a_6 + \dots) + \dots \pmod 7$$

e quindi

$$\boxed{7 \mid N \iff 7 \mid r}$$

Criterio di divisibilità per 8.

$$\begin{aligned} 10^1 &\equiv 2 \pmod 8, & 10^2 &\equiv 4 \pmod 8, \\ 10^3 &\equiv 0 \pmod 8, & 10^n &\equiv 0 \pmod 8. \end{aligned}$$

da cui si ottiene che:

$$N \equiv r := a_0 + 2a_1 + 4a_2 \pmod 8$$

e quindi:

$$\boxed{8 \mid N \iff 8 \mid r}$$

Criterio di divisibilità per 10. Dato che $10 \equiv 0 \pmod{10}$ si ha che

$$\boxed{10 \mid N \iff a_0 = 0}$$

Criterio di divisibilità per 12.

$$10^1 \equiv -2 \pmod{12},\ 10^2 \equiv 4 \pmod{12},\ 10^3 \equiv 4 \pmod{12}.$$

Da cui si ottiene che:

$$N \equiv r := a_0 - 2a_1 + 4(a_2 + \dots) \pmod{12}$$

e quindi:

$$\boxed{12 \mid N \iff 12 \mid r \iff 3 \mid N \text{ e } 4 \mid N}$$

Criterio di divisibilità per 13.

$$10^1 \equiv -3 \pmod{13},\quad 10^2 \equiv -4 \pmod{13},\quad 10^3 \equiv -1 \pmod{13},$$
$$10^4 \equiv 3 \pmod{13},\quad 10^5 \equiv 4 \pmod{13},\quad 10^6 \equiv 1 \pmod{13}.$$

da cui si ottiene che:

$$N \equiv r := (a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 4a_5) + (a_6 - \dots) + \dots \pmod{13}$$

e quindi:

$$\boxed{13 \mid N \iff 13 \mid r}$$

1.4 Soluzioni di alcuni esercizi proposti

1.3. **(a)** Sappiamo che necessariamente $a \equiv x \pmod 4$ con x elemento del sistema completo di residui (modulo 4). Controlliamo come si comportano gli elementi del Sistema Completo di Residui elevati al quadrato.

elemento	valore (mod 4)
0^2	0
1^2	1
2^2	0
3^2	1

(b) Sappiamo che necessariamente $a \equiv x \pmod 8$ con x elemento del sistema completo di residui (modulo 8). Controlliamo come si comportano gli elementi del Sistema Completo di Residui elevati al quadrato.

elemento	valore (mod 8)
0^2	0
1^2	1
2^2	4
3^2	1
4^2	0
5^2	1
6^2	4
7^2	1

(c) Procediamo per assurdo.
Supponiamo che si possa scrivere $n = a^2 + b^2 \equiv 3 \pmod 4$. Nel punto (a) abbiamo già visto come si comportano gli elementi del Sistema Completo di Residui (modulo 4) e osserviamo che non è quindi possibile formare coppie tali che la somma sia congrua a $3 \pmod 4$.

(d) Procediamo per assurdo.
Supponiamo che si possa scrivere $n = a^2 + b^2 + c^2 \equiv 7 \pmod 8$. Nel punto (b) abbiamo già visto come si comportano gli elementi del Sistema Completo di Residui (modulo 8) e osserviamo che non è quindi possibile formare terne tali che la somma sia congrua a $7 \pmod 8$.

1.4. Prendiamo $ar_i + b$ e $ar_j + b$.
Per assurdo supponiamo che $ar_i + b \equiv ar_j + b$ comunque preso $i \neq j$
Allora avremo: $ar_i - ar_j \equiv 0 \pmod n$ e, visto che $\text{MCD}(a, n) = 1$ si ha che $aa^*(r_i - r_j \equiv 0 \pmod n$, conseguentemente $r_i - r_j \equiv 0 \pmod n$ e cioè $r_i \equiv r_j \pmod n$. Il che è assurdo.
Essendo $ar_i + b$, $i = 1, \dots n$ in numero n ed incongruenti devono formare un Sistema Completo di Residui.

1.5 Esercizi aggiuntivi con soluzioni

★ 1. Un numero *palindromo* è un numero che rimane invariato sia che si legga da destra che da sinistra.

(a) Dimostrate che tutti i numeri palindromi di 4 cifre sono divisibili per 11.

(b) Cosa si può dire per i palindromi di 6 cifre?

Soluzione. (a) Sia $n = abba$. Sappiamo che:

$$11 \mid n \iff 11 \mid \sum_{i=0}^{3} (-1)^i a_i = A(n)$$

Calcoliamo dunque $A(n) = a - b + b - a = 0 \Rightarrow 11 \mid n$.

(b) Sia $n = abccba$. Ricordiamo che per determinare criteri di divisibilità di un numero si può fare ricorso a due quantità particolari: $S(n)$ ed $A(n)$ (cfr. Proposizione *1.17*). In questo caso abbiamo:
$S(n) = 2a + 2b + 2c = 2(a + b + c)$;
$A(n) = a - b + c - c + b - a = 0$.
Otteniamo quindi che: $11 \mid n$ comunque preso n di 6 cifre.

★ **2.** Dimostrare che se $n \equiv 4 \pmod 9$ allora n non può essere scritto come somma di tre cubi.

Soluzione. Procediamo per assurdo. Supponiamo che si possa scrivere $n = a^3 + b^3 + c^3$. Controlliamo come si comportano gli elementi del Sistema Completo di Residui elevati al cubo.

elemento	valore (mod 9)
0^3	0
1^3	1
2^3	8
3^3	0
4^3	1
5^3	8
6^3	0
7^3	1
8^3	8

Non è quindi possibile trovare una combinazione di tre cubi tali che la loro somma sia congrua a 4 (mod 9).

1.6 Il software *Mathematica* e la Teoria delle congruenze

1.6.1 Divisibilità e MCD

Abbiamo parlato della divisibilità per un dato numero. In *Mathematica* è esistente una funzione **Divisors[n]** che ci restituisce tutti i divisori di un dato numero n.

Divisors[123]

{1, 3, 41, 123}

Con il comando **Intersection[lista1, lista2]** possiamo calcolare i divisori comuni a più numeri. Nell'esempio che stiamo per dare abbiamo usato un metodo alternativo di scrittura della funzione Intersection[lista1, lista2]: **lista1** ESC **Inter** ESC **lista2** dove ESC indica il pulsante ESC che si trova in alto a sinistra sulla tastiera. Il risultato è il seguente:

Divisors[4519229] ∩ **Divisors[1574573]**

{1, 11, 13, 121, 143, 169, 1573, 1859, 20449}

Con questo comando è anche possibile definire una funzione per il calcolo del MCD in modo diverso da quello definito nella funzione built-in **GCD[n, m]**.

MCD[m_, n_] := Max[Intersection[Divisors[m], Divisors[n]]]

Tale funzione (MCD[m, n]) però non è efficace quanto la funzione GCD[m, n], visto che quest'ultima si basa sull'algoritmo Euclideo delle divisioni successive.
Confrontiamo i tempi delle due funzioni[4].

GCD[10^50+342, 10^50+435]//Timing

{0.018 Second, 1}

Cioè in 0.018 secondi calcola il MCD che risulta essere 1.

MCD[10^50+342, 10^50+435]//Timing

{2102.06 Second, 1}

Cioè in 2102.06 secondi calcola il MCD che risulta essere 1.

Possiamo adesso utilizzare la funzione **algEuclide[a, b]** da noi definita per il calcolo dell'Algoritmo Euclideo (per i dettagli sulla definizione di tale funzione vedere il paragrafo successivo 1.6.3.2).

algEuclide[4519229,1574573]

4519229 = 2 * 1574573 + 1370083
1574573 = 1 * 1370083 + 204490
1370083 = 6 * 204490 + 143143
204490 = 1 * 143143 + 61347
143143 = 2 * 61347 + 20449
61347 = 3 * 20449 + 0

Osservando attentamente i resti (positivi) dell'algoritmo se ne vede la decrescita costante. Questa tendenza viene confermata da un punto di vista teorico, il che permette di affermare la finitezza dell'algoritmo. Applicando tale algoritmo a due numeri di Fibonacci consecutivi, possiamo dare una stima non migliorabile sulla sua lunghezza.

Nel grafico seguente viene rappresentato l'andamento dell'algoritmo euclideo. Precisamente sull'ascissa la lunghezza dell'algoritmo euclideo e sulle ordinate la grandezza dei resti nelle divisioni successive.

ListPlot[restiDivisione[121, 102], PlotStyle − > PointSize[0.015], RGBColor[0.726574, 0.0937514, 0.00390631]];

[4]Si osservi che la differenza di risultato tra più prove con gli stessi numeri è dovuta alla memoria del computer e alle operazioni contemporanee che si effettuano.

Figura 1: Andamento resti per la divisione tra 121 e 102

Il seguente esempio potrebbe sembrare in contraddizione con l'andamento strettamente decrescente dei resti. Ma si deve osservare che il numero maggiore della divisione è il secondo, quindi il "primo" punto (resto) va nascosto .

```
ListPlot[restiDivisione[12134, 16523],
PlotStyle -> PointSize[0.015],
RGBColor[0.14844, 0.0195315, 0.882826]];
```

Figura 2: Andamento resti per la divisione tra 12134 e 16523

1.6.2 *Mathematica* e le congruenze (mod m)

Prendendo in considerazione ora alcuni elementi, osserviamo il valore che assume il resto nella divisione per un m assegnato.
Poniamo $m = 8$ e a che varia tra 100 e 115:

```
t=creaTabella[100, 115, 8];
stampaTabella[t, 8]
```

	a	q	r
	100	12	4
	101	12	5
	102	12	6
	103	12	7
	104	13	0
	105	13	1
	106	13	2
m = 8	107	13	3
	108	13	4
	109	13	5
	110	13	6
	111	13	7
	112	14	0
	113	14	1
	114	14	2
	115	14	3

Osserviamo che i resti hanno tutti valori tra 0 ed $m-1$, infatti (poniamo $m = 13$ e a che varia tra 143 e 168):

t=creaTabella[143, 168, 13];
stampaTabella[t, 13]

	a	q	r
	143	11	0
	144	11	1
	145	11	2
	146	11	3
	147	11	4
	148	11	5
	149	11	6
	150	11	7
	151	11	8
	152	11	9
	153	11	10
	154	11	11
m = 13	155	11	12
	156	12	0
	157	12	1
	158	12	2
	159	12	3
	160	12	4
	161	12	5
	162	12	6
	163	12	7
	164	12	8
	165	12	9
	166	12	10
	167	12	11
	168	12	12

Scegliamo ora nella tabella per a che varia tra 1 e 100 i valori che danno un determinato resto nella divisione per 7 (nel caso esaminato sotto: resto = 4):

```
t=creaTabella[1, 100, 7];
First/@Select[t, #1[[3]]==4&]
```

{4, 11, 18, 25, 32, 39, 46, 53, 60, 67, 74, 81, 88, 95}

Quali sono i valori di a in tale tabella che hanno come resto 3?

```
First/@Select[t, #1[[3]]==3&]
```

{3, 10, 17, 24, 31, 38, 45, 52, 59, 66, 73, 80, 87, 94}

Quindi possiamo caratterizzare i numeri a seconda del resto che danno nella divisione modulo m. Tale caratteristica è detta classe di congruenza. Osserviamo la tabella cromatica che "classifica" i numeri da 0 a 100 modulo 7. A colore uguale corrisponde resto uguale (Rosso → 0; Giallo → 1; Verde chiaro → 2; Verde scuro → 3; Celeste → 4; Blu → 5; Viola → 6)

```
mostraCongruenza[7];
```

Figura 3: Classi congruenza modulo 7.

Osserviamo che in questa tabella *Mathematica* usa 7 colori.
Possiamo quindi dire che i numeri corrispondenti ai primi quadretti, fino a che non riappaia nuovamente il colore Rosso, formano un *Sistema Completo di Residui*. Osserviamo altre tabelle:

mostraCongruenza[5];

Figura 4: Classi congruenza modulo 5.

mostraCongruenza[10];

Figura 5: Classi congruenza modulo 10.

mostraCongruenza[9];

Figura 6: Classi congruenza modulo 9.

Questa ultima tabella ha come caratteristica di avere dello stesso colore i quadretti sulla diagonale opposta a quella che si ha ponendo $m = 11$.

mostraCongruenza[11];

Figura 7: Classi congruenza modulo 11.

mostraCongruenza[1];

Figura 8: Classi congruenza modulo 1.

Dall'ultima tabella osserviamo la proprietà che è anche descritta nell'Osservazione 1.2(a): modulo 1 tutti i numeri sono congruenti.

Nell'Osservazione 1.2(c) abbiamo visto che la congruenza modulo m è identica alla congruenza modulo $-m$. Verifichiamolo visivamente confrontando le tabelle qui di seguito con quelle già calcolate con i valori positivi.

mostraCongruenza[-5];

Figura 9: Classi congruenza modulo -5.

mostraCongruenza[-10];

Figura 10: Classi congruenza modulo -10.

Osserviamo che l'unica differenza tra queste tabelle sta nel colore che il computer sceglie ogni volta per la rappresentazione della classe di congruenza, ma se si osserva la distribuzione, sono uguali. Questo perché il resto di una divisione non dipende dal segno (l'algoritmo Euclideo richiede infatti che il modulo del resto sia minore del modulo del divisore!).

Per calcolare i valori della congruenza, *Mathematica* ha una funzione built-in: **Mod[a, m]** che determina il valore del resto r di a, $0 \leqslant r \leqslant m-1$, nella divisione per m.

Mod[-7, 6]

5

Mod[213, 6]

3

Possiamo anche definire una funzione **testCongruenza[a, b, m]** (cfr. 1.6.3.7) che ci permette di verificare se due numeri a e b, sono congruenti modulo m.
Diamone alcuni esempi con verifica.

testCongruenza[-19, 5, 6]

True

Mod[-19, 6]

5

Mod[5, 6]

5

testCongruenza[-4, 9, 6]

False

Mod[-4, 6]

2

Mod[9, 6]

3

Nella Proposizione 1.3, inoltre abbiamo dato alcune proprietà delle congruenze. "Verifichiamole" sperimentalmente.

Abbiamo visto:

$$a \equiv b \pmod{m} \Rightarrow a + c \equiv c + b \pmod{m} \; \forall c \in \mathbb{Z}$$

Verifichiamo con la funzione **verificaSomma[m]** da noi definita (cfr. 1.6.3.11):

verificaSomma[12]

	a	b	c	a + c ≡ b + c (mod 12)?
	7536	0	8722	True
	7537	1	4160	True
	7538	2	1062	True
	7539	3	2434	True
	7540	4	8576	True
	7541	5	6117	True
m = 12	7542	6	7723	True
	7543	7	1424	True
	7544	8	8997	True
	7545	9	8343	True
	7546	10	5275	True
	7547	11	2071	True
	7548	0	8660	True

Abbiamo visto anche:

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m} \Rightarrow a + c \equiv d + b \pmod{m}$$

Verifichiamolo con la funzione **verificaSomma1[m]** (cfr. 1.6.3.11):

verificaSomma1[10]

	a	b	c	d	a + c ≡ b + d (mod 10)?
	8655	5	1058	8	True
	8656	6	8000	0	True
	8657	7	2236	6	True
	8658	8	6147	7	True
	8659	9	985	5	True
m = 10	8660	0	6827	7	True
	8661	1	6074	4	True
	8662	2	4913	3	True
	8663	3	2701	1	True
	8664	4	8647	7	True
	8665	5	6411	1	True

Abbiamo che:

$$a \equiv b \pmod{m} \Rightarrow a * c \equiv c * b \pmod{m} \; \forall c \in \mathbb{Z}$$

Verifichiamo con la funzione **verificaProdotto[m]** (cfr. 1.6.3.9):

verificaProdotto[12]

	a	b	c	a * c ≡ b * c (mod 12)?
	4004	8	7527	True
	4005	9	6351	True
	4006	10	723	True
	4007	11	3697	True
	4008	0	8494	True
	4009	1	4644	True
m = 12	4010	2	8170	True
	4011	3	2458	True
	4012	4	1427	True
	4013	5	4416	True
	4014	6	2265	True
	4015	7	3629	True
	4016	8	386	True

Diamo ora alcune osservazioni per quanto riguarda invece la "regola di cancellazione". Vogliamo vedere se vale la seguente proprietà:

$$a * b \equiv a * c \pmod{m},\ a \not\equiv 0 \pmod{m} \Rightarrow b \equiv c \pmod{m}?$$

leggeCancellazione[11]

m=11	a	b	c	a*b	a*c	a*b ≡ a*c (mod m)?	b ≡ c (mod m)?
	0	1	2	0	0	True	False
	1	1	12	1	12	True	True
	2	1	12	2	24	True	True
	3	1	12	3	36	True	True
	4	1	12	4	48	True	True
	5	1	12	5	60	True	True
	6	1	12	6	72	True	True
	7	1	12	7	84	True	True
	8	1	12	8	96	True	True
	9	1	12	9	108	True	True
	10	1	12	10	120	True	True

Osserviamo che la "regola di cancellazione" vale solo per i moduli primi (cfr. Proposizione *1.9*).

leggeCancellazione[6]

m = 6	a	b	c	a*b	a*c	a*b ≡ a*c (mod m)?	b ≡ c (mod m)?
	0	1	2	0	0	True	False
	1	1	7	1	7	True	True
	2	1	4	2	8	True	False
	3	1	3	3	9	True	False
	4	1	4	4	16	True	False
	5	1	7	5	35	True	True

Si analizzi in particolare la riga per $a = 2$. Abbiamo:

testCongruenza[2*4, 2*1 , 6]

True

testCongruenza[2, 0, 6]

False

testCongruenza[4, 1, 6]

False

Abbiamo definito, all'inizio del paragrafo, una relazione tra le congruenze ed i giorni della settimana. Applichiamo tale "formula" a *Mathematica* e definiamo una funzione appropriata **giornosettimana[g, m, a]** (cfr. 1.6.3.12):

giornosettimana[5, 6, 2000]

Monday

1.6.3 Funzioni utilizzate

Diamo ora la descrizione e la spiegazione delle funzioni definite per questa parte.
Per prima cosa dobbiamo "pulire" da funzioni eventualmente in memoria residua.

```
Off[General::"spell"];
Off[General::"spell1"];
```

♦ **1.6.3.1.** La funzione **listaGCD[a, b]** crea una lista di $\{r_i, r_j, q, r\}$ con $r_i = qr_j + r$ che rappresentano i passi dell'Algoritmo Euclideo delle divisioni successive.

```
Clear[listaGCD];

listaGCD[a_,b_]:=Module[{dividendo,divisore,resto,risultato},
     dividendo=Max[a,b];
     divisore=Min[a,b];
     quoziente=Quotient[dividendo,divisore];
     resto=Mod[dividendo,divisore];
     risultato={dividendo,divisore,quoziente,resto};
     While[resto!=0,
         dividendo=divisore;
         divisore=resto;
         quoziente=Quotient[dividendo,divisore];
 resto=Mod[dividendo,divisore];
         AppendTo[risultato,{dividendo,divisore,quoziente,resto}]];
    Return[risultato]]
```

♦ **1.6.3.2.** La funzione **algEuclide[a, b]** descrive esplicitamente, in una tabella, l'Algoritmo Euclideo.

```
Clear[algEuclide];

algEuclide[a_,b_]:=Module[{lista=listaGCD[a,b]},
TableForm[(ToString[#1 [[1]] ]<>" = "<>
                   ToString[#1 [[3]]]<>" * "<>
                   ToString[#1 [[2]] ]<>" + "<>
                   ToString[#1 [[4]] ]&)/@
                   lista, TableSpacing->{0,2}]]
```

♦ **1.6.3.3.** Per avere, invece, una lista con i soli resti dell'Algoritmo Euclideo si è definita la funzione **restiDivisione[a, b]**.

```
Clear[restiDivisione, passiresti];

restiDivisione[a_, b_]=passiresti[a, b, {a}];

passiresti[a_, b_, r_]:=passiresti[b, Mod[a,b], Append[r,b]];

passiresti[a_, 0, r_]:=r;
```

♦ **1.6.3.4.** Dovendo creare tabelle e "scacchiere" è stato necessario definire una funzione **newtickf[min, max]** che crea una tabella composta da coppie del tipo $\{i + \frac{1}{2}, i\}$ con i che varia tra **Floor[min]** e **Ceiling[max]** .

```
Clear[newtickf,min,max];

newtickf[min_,max_]:=Table[{i+1/2,i},{i,Floor[min],Ceiling[max]}];
```

♦ **1.6.3.5.** Diamo qui di seguito alcune funzioni secondarie che ci sono servite per la definizione delle principali altre funzioni.

```
Clear[pow, scomposizioneInteri];

pow[x_, y_]:=x^y;

scomposizioneInteri[n_] := Times@@Apply[pow, FactorInteger[n], 1]

Clear[creaTabella,l,u,m];

creaTabella[l_,u_,m_]:=Table[{a,Quotient[a,m],Mod[a,m]},{a,l,u}];

Clear[stampaTabella,t,m];

stampaTabella[t_,m_]:=
   "m = "<>ToString[m]
   TableForm[t,TableSpacing->{0,1},
   TableHeadings->{None,{"a","q","r"}}]
```

♦ **1.6.3.6.** Per poter visualizzare la tabella delle congruenze è stata definita la funzione **mostraCongruenza[n]** .

```
Clear[mostraCongruenza, m, maxTens];

mostraCongruenza[m_, maxTens_: 10] :=
        Module[{matrix},
          matrix = Table[
            Table[Mod[10 i + j, m], {j, 0, 9}],
            {i, 0, maxTens - 1}];
          ListDensityPlot[matrix, FrameTicks -> newtickf,
          FrameLabel -> {"unita'", "decine"},
          ColorFunction -> (Hue[(#1 (m))) / (m + 2)]),
          RotateLabel -> False]]
```

♦ **1.6.3.7.** Per sapere se due numeri a e b sono congrui modulo m si può usare, oltre che la funzione **Mod[a, m]** anche la funzione da noi definita **testCongruenza[a,b,m]** .

```
Clear[testCongruenza,a,b,m];

testCongruenza[a_,b_,m_]:=Mod[a-b,m]==0
```

Sono state poi create delle funzioni che permettano di verificare le proprietà delle congruenze descritte.

♦ **1.6.3.8.** La funzione **leggeCancellazione[m]** illustra le proprietà che devono essere soddisfatte da a per avere: $ab \equiv ac \pmod{m} \Rightarrow b \equiv c \pmod{m}$.

```
Clear[leggeCancellazione, m];

leggeCancellazione[m_] :=
    Module[{c},
      TableForm[
        Table[{"<>", a, 1, c = 1 + m/GCD[a, m], a, a c,
            testCongruenza[a, a c, m],
            testCongruenza[1, c, m]}, {a, 0, m - 1}],
        TableHeadings -> {None, {"m = "<>ToString[m], "a", "b", "c",
              "ab", "ac", "ab = ac?",
              "b = c?"}}, TableSpacing -> {0, 2},
        TableAlignments -> {Center, Bottom}]]
```

♦ **1.6.3.9.** La funzione **verificaProdotto[m]** verifica che valga la proprietà del prodotto: $a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$ prendendo la prima volta a a caso tra gli interi 1 e 10000, b tale che $a \equiv b \pmod{m}$ e c a caso con lo stesso criterio di a. Successivamente si incrementa a di uno fino a utilizzare tutti gli elementi del sistema completo di residui modulo m.

```
Clear[verificaProdotto, verificaprodotto];

verificaProdotto[m_]:=
  "m = "<>ToString[m]
  TableForm[verificaprodotto[m],TableSpacing->{0,1},
  TableHeadings->{None,{"a","b","c", "a*c = b*c ?"}}];

verificaprodotto[n_]:=Module[{a, b, c, test, verifica},
    a=Random[Integer, {1, 10000}];
    b=Mod[a,n];
    c=Random[Integer, {1,10000}];
    test=testCongruenza[a*c, b*c, n];
    verifica={{a, b, c,test}};
    For[j=0, j<n, {a= a+1;
          b=Mod[a,n];
          c=Random[Integer, {1,10000}];
  test=testCongruenza[a*c, c*b, n];
  AppendTo[verifica,{a, b, c, test}]};
          j++];
    Return[verifica]]
```

♦ **1.6.3.10.** La funzione **verificaSomma1[m]** verifica che valga la proprietà della somma: $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m} \Rightarrow a+c \equiv b+d \pmod{m}$ prendendo a, b e c con gli stessi criteri della funzione *verificaProdotto[m]* mentre d è preso tale che $c \equiv d \pmod{m}$.

```
Clear[verificaSomma1, verificasomma1];

verificaSomma1[m_]:=
  "m = "<>ToString[m]
    TableForm[verificasomma1[m],TableSpacing->{0,1},
      TableHeadings
        ->{None,{"a","b","c", "d", "a+c = b+d ?"}}];

verificasomma1[n_]:=Module[{a, b, c,d, test, verifica},
a=Random[Integer, {1, 10000}];
        b=Mod[a,n];
c=Random[Integer, {1,10000}];
        d=Mod[c, n];
        test=testCongruenza[a+c, d+b, n];
        verifica={{a, b, c, d,test}};
For[j=0, j<n,{a= a+1 ;
           b=Mod[a,n];
           c=Random[Integer, {1,10000}];
           d=Mod[c, n];
   test=testCongruenza[a+c, d+b, n];
           AppendTo[verifica,{a, b, c, d,test}]};
           j++];
        Return[verifica]]
```

♦ **1.6.3.11.** La funzione **verificaSomma[m]** verifica che valga la proprietà della somma: $a \equiv b \pmod{m} \Rightarrow a + c \equiv b + c \pmod{m}$ prendendo a, b e c con gli stessi criteri della funzione *verificaProdotto[m]*.

```
Clear[verificaSomma, verificasomma];

verificaSomma[m_]:=
  "m = "<>ToString[m]
    TableForm[verificasomma[m],TableSpacing->{0,1},
      TableHeadings->{None,{"a","b","c", "a+c  b+c ?"}}];

verificasomma[n_]:=Module[{a, b, c,test, verifica},
        a=Random[Integer, {1, 10000}];
        b=Mod[a,n];
c=Random[Integer, {1,10000}];
test=testCongruenza[a+c, b+c, n];
        verifica={{a, b, c,test}};
For[j=0, j<n,{a= a+1 ;
            b=Mod[a,n];
            c=Random[Integer, {1,10000}];
    test=testCongruenza[a+c, b+c, n];
    AppendTo[verifica,{a, b, c,test}]};
            j++];
        Return[verifica]]

Clear[testCancellazione];
```

```
testCancellazione[a_,b_,c_,m_]:=
  If[testCongruenza[a b,a c,m],
    TableForm[Table[{testCongruenza[b,c,m-i],m-i},{i,0,m-1}],
      TableHeadings
        ->{None,{ToString[b]<>" = "<>ToString[c]<>" mod m?","m"}},
      TableSpacing->{0,1}],
    ToString[a b]<>" != "<>ToString[a c]<>" mod "<>ToString[m]]
```

♦ **1.6.3.12.** Per concludere definiamo la funzione che ci permette di applicare quanto descritto all'inizio del paragrafo: **giornosettimana[gg, mm, aa]**.

```
Clear[giornosettimana, h, giorno, giornomese, bisestile];

bisestile[x_]:=
  If[FractionalPart[(x/400)]==0, 1,
    If[FractionalPart[(x/100)]==0, 0,
If[FractionalPart[(x/4)]==0, 1, 0]]];

giornomese[1,z_]=0; giornomese[2,z_]=1;
giornomese[3,z_]:=If[bisestile[z]==1, 60, 59];
giornomese[4,z_]:=giornomese[3,z]+31;
giornomese[5,z_]:=giornomese[4,z]+30;
giornomese[6,z_]:=giornomese[5,z]+31;
giornomese[7,z_]:=giornomese[6,z]+30;
giornomese[8,z_]:=giornomese[7,z]+31;
giornomese[9,z_]:=giornomese[8,z]+31;
giornomese[10,z_]:=giornomese[9,z]+30;
giornomese[11,z_]:=giornomese[10,z]+31;
giornomese[12,z_]:=giornomese[11,z]+30;
giorno[x_,y_,z_]:=giornomese[y,z]+x;

h[x_, y_, z_]:=
     (z-1) +
        (IntegerPart[(z-1)/4]-IntegerPart[(z-1)/100]+
IntegerPart[(z-1)/400])+
    giorno[x,y,z];

giornosettimana[x_,y_,z_]:=
  If[Mod[h[x,y,z],7]==0, Print["Sunday"],
    If[Mod[h[x,y,z],7]==1, Print["Monday"],
      If[Mod[h[x,y,z],7]==2, Print["Tuesday"],
        If[Mod[h[x,y,z],7]==3, Print["Wednsday"],
          If[Mod[h[x,y,z],7]==4, Print["Thursday"],
            If[Mod[h[x,y,z],7]==5, Print["Friday"],
              If[Mod[h[x,y,z],7]==6, Print["Saturday"]]]]]]];
```

2 Congruenze lineari ed equazioni diofantee lineari

2.1 Frazioni continue ed equazioni diofantee

Le equazioni diofantee[5] sono legate, da un punto di vista storico, alla risoluzione di alcuni problemi di vita quotidiana.
L'esempio classico che viene riportato in molti testi è quello delle *pecore* e delle *galline*:

In un recinto ci sono delle galline ed un numero dispari di pecore per un totale di 20 zampe. Quante sono le pecore?

L'equazione che descrive la situazione, ponendo x il numero delle pecore e y il numero delle galline, assume la seguente forma:

$$4x + 2y = 20$$

Per il principio di equivalenza:

$$2x + y = 10$$

cioè

$$x = \frac{10 - y}{2}$$

con soluzioni razionali:

x	$\frac{9}{2}$	4	$\frac{7}{2}$	3	$\frac{5}{2}$	2	$\frac{3}{2}$	1	$\frac{1}{2}$	0
y	1	2	3	4	5	6	7	8	9	10

Visto che x ed y si ricercano tra i numeri interi ed entrambi positivi (in più x deve essere dispari), i risultati accettabili risultano essere: $(3, 4)$ e $(1, 8)$.

Questo particolare tipo di equazione si dice Equazione Diofantea Lineare (in due indeterminate) ed esiste un semplice metodo per calcolarne la soluzione. Per quanto riguarda, invece, equazioni diofantee di grado superiore al primo, non esiste un metodo generale per determinare la soluzione. Per risolvere un problema lineare sono stati trovati molti metodi. Il metodo di Euler (cfr. Esercizio 2.5) è quello più usato e deve il suo nome a Euler che fu il primo ad usarlo nel suo libro *Algebra* del 1770. Un altro metodo che riteniamo interessante da studiare è quello che fa uso delle *Frazioni Continue*.

[5] Il nome deriva dal matematico greco Diofanto vissuto ad Alessandria intorno al 250 d. C. e che scrisse un trattato sull'argomento.

Definizione 4. Una *frazione continua* è un'espressione del tipo:

$$x = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{a_5 + \dots}}}}$$

dove gli $a_i \in \mathbb{N}$ sono detti *quozienti*.
Una *frazione continua* si dirà *finita* se il numero dei quozienti è finito.

La forma tipografica più pratica e di uso comune per scrivere una frazione continua è:

$$[a_1, a_2, \dots, a_n, \dots].$$

Diamo alcune caratterizzazioni delle frazioni continue che ci serviranno per la definizione del metodo di risoluzione delle equazioni diofantee.

Le frazioni continue finite sono utilizzate per la scrittura dei numeri razionali del tipo $\frac{p}{q}$ con $\mathrm{MCD}(p, q) = 1$.

Esempio. *Scrivere* $\frac{67}{29}$ *con le frazioni continue.*
Per prima cosa si applica l'Algoritmo Euclideo ai termini della frazione:

$$\begin{aligned} 67 &= 2 \cdot 29 + 9 \\ 29 &= 3 \cdot 9 + 2 \\ 9 &= 2 \cdot 4 + 1 \end{aligned}$$

Da cui si ottiene:

$$\begin{aligned} \frac{67}{29} &= 2 + \frac{9}{29} = 2 + \cfrac{1}{\cfrac{29}{9}} = \\ &= 2 + \cfrac{1}{3 + \cfrac{2}{9}} = 2 + \cfrac{1}{3 + \cfrac{1}{\cfrac{9}{2}}} = \\ &= 2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}} = [2, 3, 4, 2] \end{aligned}$$

Osserviamo che avremmo potuto scrivere anche $\frac{67}{29} = [2, 3, 4, 1, 1]$ ponendo $2 = 1 + \frac{1}{1}$.
Questo perché vale il seguente risultato:

Teorema 5. *Ogni numero razionale*[6] *si può scrivere in frazione continua sia con un numero pari che con un numero dispari di quozienti, modificando soltanto l'ultimo termine.*

Dimostrazione. Se $q \in \mathbb{Q}$, allora $q = \frac{m}{n}$ con $m, n \in \mathbb{Z}$ e sappiamo che l'Algoritmo Euclideo tra due numeri interi è un algoritmo finito. In più sappiamo che si può sempre scrivere q in modo tale che $\mathrm{MCD}(m, n) = 1$ e quindi, applicando l'osservazione che abbiamo fatto alla fine dell'Esempio, abbiamo la tesi. □

Definizione 6. Se $\frac{p}{q} = [a_1, \ldots, a_N]$, le seguenti quantità

$$c_1 := \frac{a_1}{1}, \qquad c_2 := a_1 + \frac{1}{a_2}, \qquad c_3 := a_1 + \frac{1}{a_2 + \dfrac{1}{a_3}}, \qquad \ldots$$

sono dette *convergenti* della frazione continua con $c_N := [a_1, \ldots, a_N]$.

Teorema 7. *Se* $c_i = \frac{p_i}{q_i}$, *allora* $p_i \cdot q_{i-1} - p_{i-1} \cdot q_i = (-1)^i$.

Dimostrazione. Si tratta di una semplice applicazione del principio di induzione alla seguente relazione che intercorre tra i convergenti:

$$\begin{aligned} p_1 &= a_1 & q_1 &= 1 \\ p_2 &= a_1 \cdot a_2 + 1 & q_2 &= a_2 \\ p_i &= a_i \cdot p_{i-1} + p_{i-2} & q_i &= a_i \cdot q_{i-1} + q_{i-2} \end{aligned}$$ □

Mostriamo ora come usare le frazioni continue per risolvere le equazioni diofantee lineari (in due indeterminate).

Cominciamo con lo studiare

$$aX - bY = \pm 1 \quad \text{con } a, b \in \mathbb{N} \quad \text{e} \quad \mathrm{MCD}(a, b) = 1 \tag{1}$$

L'ipotesi che a e b siano primi tra loro implica che le soluzioni sono infinite.

Il seguente teorema che dimostreremo, oltre a provare l'esistenza di soluzioni per questo particolare tipo di equazione, determina un metodo generale per il calcolo di una soluzione.

[6] Anche i numeri irrazionali si possono scrivere come frazioni continue **infinite** questo perché nell'Algoritmo Euclideo non abbiamo più un insieme di quozienti e resti interi in numero finito.
Alcuni esempi sono calcolati in [O]:

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \ldots}}}} \qquad e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \ldots}}}}}$$

Teorema 8. *L'equazione* (1) *ha infinite soluzioni intere.*

Dimostrazione. Sviluppiamo la frazione $\frac{a}{b}$ in frazioni continue.

$$\frac{a}{b} = [a_1, \ldots, a_n]$$

Se consideriamo p_j e q_j come definiti nella dimostrazione del Teorema 7, otteniamo i seguenti convergenti:

$$c_1 = \frac{p_1}{q_1}; \qquad c_2 = a_1 + \frac{1}{a_2} = \frac{a_1 \cdot a_2 + 1}{a_2};$$

$$c_3 = [a_1, a_2, a_3] = a_1 + \frac{1}{\frac{a_3 \cdot a_2 + 1}{a_3}} = \frac{a_3 \cdot (a_1 \cdot a_2 + 1) + a_1}{a_3 \cdot a_2 + 1} = \frac{a_3 p_2 + p_1}{a_3 q_2 + q_1} = \frac{p_3}{q_3}$$

e per $3 \leqslant i \leqslant n$:

$$c_i = [a_1, \ldots, a_i] = \frac{p_i}{q_i}$$

Per il Teorema 7 si ha:

$$p_n \cdot q_{n-1} - p_{n-1} \cdot q_n = (-1)^n$$

e visto che $a = p_n$ e $b = q_n$, ne segue:

$$a \cdot q_{n-1} - p_{n-1} \cdot b = (-1)^n$$

Prendiamo ora in considerazione l'equazione $aX - bY = (-1)^n$ che ha tra le soluzioni: $x_0 = q_{n-1}$ e $y_0 = p_{n-1}$. Ricordando quanto enunciato nel Teorema 5 siamo in grado di trovare altre soluzioni particolari di (1). Con questo il teorema è dimostrato.
Cerchiamo ora di scrivere in modo esplicito la soluzione generale.
Sia (x, y) la soluzione generale per $aX - bY = 1$ e sia (x_0, y_0) una particolare fissata. Sottraendo, si ottiene:

$$a(x - x_0) - b(y - y_0) = 0.$$

$b \mid b(y - y_0) \Rightarrow b \mid a(x - x_0)$ e dalle ipotesi su a e b ne segue che $b \mid (x - x_0) \Rightarrow (x - x_0) = tb,\ t \in \mathbb{Z}$.
Sostituendo si ottiene: $a(tb) = b(y - y_0)$ cioè le soluzioni sono della forma

$$\begin{cases} x = x_0 + tb \\ y = y_0 - ta \end{cases}$$

Inoltre, se (x, y) è del tipo sopra descritto, allora è subito verificato che è una soluzione dell'equazione $aX - bY = 1$ essendo $ax_0 - by_0 = 1$. A prima vista potrebbe sembrare si sia fatto un lavoro eccessivo. In realtà, dopo aver

stabilito la condizione **necessaria** affinchè la coppia (x, y) sia soluzione, abbiamo dimostrato che avere tale caratteristica è **sufficiente** per essere una soluzione.
In modo del tutto analogo si ottiene una soluzione per $aX - bY = -1$ sviluppando $\frac{a}{b}$ in una frazione continua con un numero dispari di quozienti. □

Esempio. *Trovare la soluzione generale di* $205X - 93Y = 1$.
Sviluppiamo $\frac{205}{93}$ in frazione continua:

$$\frac{205}{93} = [2, 4, 1, 8, 2] = [2, 4, 1, 8, 1, 1].$$

I convergenti sono:

$$c_1 = 2, \qquad c_2 = \frac{9}{4}, \qquad c_3 = \frac{11}{5},$$

$$c_4 = \frac{97}{44}, \qquad c_5 = \frac{108}{49}, \qquad c_6 = \frac{205}{93}.$$

Quindi:

$$x_0 = 49 \qquad y_0 = 108$$

è una soluzione particolare mentre quella generale si otterrà al variare di $t \in \mathbb{Z}$ ponendo:

$$x = x_0 + tb = 49 + 93t$$

$$y = y_0 + ta = 108 + 205t.$$

Studiamo ora il caso:

$$aX - bY = c \quad \text{con MCD}(a, b) = 1 \tag{2}$$

Ripercorrendo i passi della dimostrazione del Teorema 8, arriviamo a scrivere l'equazione:

$$a \cdot q_{n-1} - p_{n-1} \cdot b = (-1)^n.$$

Moltiplicando ambo i membri per $(-1)^n \cdot c$ otteniamo:

$$(-1)^n \cdot c \cdot a \cdot q_{n-1} - (-1)^n \cdot c \cdot p_{n-1} \cdot b = c$$

Con soluzioni particolari:

$$\begin{cases} x_0 = (-1)^n \cdot c \cdot q_{n-1} \\ y_0 = (-1)^n \cdot c \cdot p_{n-1} \end{cases}$$

e conseguenti soluzioni generali al variare di $t \in \mathbb{Z}$

$$\begin{cases} x = x_0 + tb \\ y = x_0 + ta \end{cases}$$

Per concludere studiamo:

$$aX + bY = c \quad \text{con MCD}(a, b) = 1 \tag{3}$$

Ci si può ricondurre alle precedenti equazioni scrivendo: $aX - b(-Y) = 1$ e cercando la soluzione per le coppie $(x, -y)$ così da ottenere:

$$\begin{cases} x = cq_{n-1} + tb \\ y = -cp_{n-1} - ta \end{cases}$$

dove (q_{n-1}, p_{n-1}) è soluzione di $aX - bY = 1$.

Esempio. *Calcolare le soluzioni della congruenza* $30X \equiv 7 \pmod{37}$.
Le soluzioni della congruenza data determinano soluzioni dell'equazione diofantea $30X - 37Y = 7$. Abbiamo che:

$$\frac{30}{37} = [0, 1, 4, 3, 2]$$

con, di conseguenza, $q_1 = 1$, $q_2 = 1$, $q_3 = 4 \cdot 1 + 1 = 5$, $q_4 = 3 \cdot 5 + 1 = 16$ e $p_1 = 0$, $p_2 = 0 \cdot 1 + 1 = 1$, $p_3 = 4 \cdot 1 + 0 = 4$, $p_4 = 3 \cdot 4 + 1 = 13$.
L'equazione diofantea $30X - 37Y = 7$ avrà una soluzione particolare del tipo:

$$\begin{cases} x_0 = (-1)^5 \cdot 7 \cdot 16 = -112 \\ y_0 = (-1)^5 \cdot 7 \cdot 13 = -91 \end{cases}$$

In generale, le soluzioni sono date dalle seguenti espressioni, al variare di $t \in \mathbb{Z}$.

$$\begin{cases} x = -112 + 37 \cdot t \\ y = -91 + 37 \cdot t \end{cases}$$

2.2 La funzione φ di Euler

La definizione di tale funzione è stata data nel Paragrafo 2 (parte 1) a cui facciamo riferimento. Non si sono però analizzate in dettaglio le principali proprietà di tale funzione.

Definizione 9. Una funzione $f : \mathbb{N} \longrightarrow \mathbb{C}$ si dice *moltiplicativa* se:

$$\text{MCD}(a, b) = 1 \Rightarrow f(a \cdot b) = f(a) \cdot f(b).$$

Se l'ipotesi sul MCD risultasse superflua (cioè se $f(a \cdot b) = f(a) \cdot f(b)$, presi comunque $a, b \in \mathbb{N}$), la f si dirà *completamente moltiplicativa*.

Osserviamo che una funzione moltiplicativa non identicamente nulla verifica sempre la proprietà che $f(1) = 1$.
Diamo ora alcuni esempi di funzioni moltiplicative:

$$\tau(n) := \text{ numero dei divisori positivi di } n$$
$$\sigma(n) := \text{ somma dei divisori positivi di } n.$$

Torniamo ora a parlare della *funzione di Euler*.

Lemma 10. *Preso comunque $n > 0$ si ha:*

$$\varphi(p^n) = p^{n-1}(p-1).$$

Dimostrazione. I numeri positivi $s \leqslant p^n$ che **non** sono primi con p^n sono i multipli di p:

$$1 \cdot p,\ 2 \cdot p,\ \ldots,\ (p^{n-1}) \cdot p,$$

e sono esattamente p^{n-1}. I restanti (che sono dunque primi con p^n) risultano quindi essere in numero:

$$\varphi(p^n) = p^n - p^{n-1} = (p^{n-1}) \cdot (p-1). \qquad \square$$

Per dimostrare in maniera semplice che φ è moltiplicativa (senza far uso della funzione di Moebius) ci occorre il seguente (banale) risultato:

Lemma 11. *Se* $\mathrm{MCD}(a, m) = 1$ *e* $a \equiv b \pmod{m}$, *allora* $\mathrm{MCD}(b, m) = 1$

Ora possiamo dimostrare:

Teorema 12. *La funzione φ è una funzione moltiplicativa.*

Dimostrazione. Supponiamo $\mathrm{MCD}(m, n) = 1$ e scriviamo tutti i numeri tra 1 e mn nella seguente tabella:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \ldots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \ldots & (n-1)m+2 \\ & & \cdot & & \cdot \\ & & \cdot & & \cdot \\ m & 2m & 3m & \ldots & mn \end{array}$$

Supponiamo di prendere ora r tale che $\mathrm{MCD}(m, r) = d > 1$. È chiaro che nessun elemento delle r-esima riga è primo con mn visto che si tratta dei seguenti elementi:

$$r\ m+r\ 2m+r\ \ldots\ km+r\ \ldots\ (n-1)m+r.$$

Questo perché se $d \mid m$ e anche $d \mid r$, allora $d \mid (km + r)$ comunque preso k.
Cerchiamo dunque i numeri primi con mn.
Supponiamo di aver dimostrato che ci sono esattamente $\varphi(n)$ elementi primi

con mn nelle righe il cui primo elemento è primo con m. Si hanno quindi $\varphi(m)$ righe di questo tipo e quindi si ha che gli elementi relativamente primi con mn sono esattamente $\varphi(m) \cdot \varphi(n)$.

Studiamo ora gli elementi della r-esima riga (dove $\text{MCD}(m, r) = 1$). Abbiamo quindi:

$$r \; m + r \; 2m + r \; \ldots \; km + r \; \ldots \; (n-1)m + r. \qquad (\circ)$$

Dimostriamo che i loro residui (mod n) sono una permutazione di:

$$0, \; 1, \; 2, \; \ldots, \; (n-1).$$

basta cioè dimostrare che non ci sono coppie di elementi in $(\circ)$ congruenti (mod n).
Supponiamo che:

$$km + r \equiv jm + j \pmod{n},$$

con $0 \leqslant k, j < n$. Quindi (Proposizione 1.3(6)) si ha $km \equiv jm \pmod{n}$ e dato che $\text{MCD}(m, n) = 1$ si ha (Corollario 1.11(a)): $k \equiv j \pmod{n}$. Di conseguenza $k = j$. Quindi se $k \neq j$ i due elementi non sono congrui.
Inoltre, per la Proposizione 2.10 abbiamo che $(\circ)$ ha esattamente $\varphi(n)$ elementi primi con n, in più, per il Lemma 11 tutti gli elementi nella r-esima riga sono primi con m. Si è visto così che la r-esima riga ha esattamente $\varphi(n)$ elementi primi con mn. Questo completa la dimostrazione. □

Proposizione 13. *Se f è una funzione moltiplicativa ed $n = p_1^{e_1} \cdots p_r^{e_r}$, con $p_i \neq p_j$ per $1 \leqslant i \neq j \leqslant r$ allora:*

$$f(n) = f(p_1^{e_1}) \cdots f(p_r^{e_r}).$$

Dimostrazione. Procediamo per induzione su $r \geqslant 1$.
La proposizione è ovviamente vera per $r = 1$. Supponiamola vera per $r = k$, dimostriamola per $r = k + 1$.
Visto che $\text{MCD}(p_1^{e_1} \cdots p_k^{e_k}, p_{k+1}^{e_{k+1}}) = 1$, e f è moltiplicatica:

$$f(p_1^{e_1} \cdots p_{k+1}^{e_{k+1}}) = f(p_1^{e_1} \cdots p_k^{e_k}) \cdot f(p_{k+1}^{e_{k+1}}).$$

Applicando l'ipotesi induttiva abbiamo la tesi. □

Cerchiamo ora delle formule per descrivere $\varphi(m)$.

Teorema 14. *Sia $n = p_1^{e_1} \cdots p_r^{e_r}$ (come nella Proposizione 13), allora*

$$\varphi(n) = p_1^{e_1 - 1}(p_1 - 1) \cdots p_r^{e_r - 1}(p_r - 1).$$

Dimostrazione. Visto che φ è moltiplicativa, per la Proposizione 13 si ha:

$$\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r}).$$

Dal Lemma 10 discende la tesi. □

Esempio. *Calcolare* $\varphi(72)$.
Visto che $72 = 2^3 \cdot 3^2$, abbiamo:

$$\varphi(72) = \varphi(2^3) \cdot \varphi(3^2) = 2^2 \cdot 1 \cdot 3^1 \cdot 2 = 24.$$

Teorema 15. *Sia* $n = p_1^{e_1} \cdots p_r^{e_r}$ *(come nella Proposizione 13), allora*

$$\varphi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Dimostrazione. Prendiamo prima il caso $n = p^a$ con p primo ed $a \geqslant 1$. Si avrà (Lemma 10):

$$\varphi(n) = p^a - p^{a-1} = p^a \left(1 - \frac{1}{p}\right).$$

Quindi, per la Proposizione 13:

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r}) \\
&= p_1^{e_1} \left(1 - \frac{1}{p_1}\right) \cdots p_r^{e_r} \left(1 - \frac{1}{p_r}\right) \\
&= p_1^{e_1} \cdots p_r^{e_r} \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \\
&= n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \qquad \square
\end{aligned}$$

2.3 Applichiamo il software *Mathematica*

2.3.1 Le equazioni diofantee lineari

Equazioni in due indeterminate. Le equazioni diofantee sono particolari equazioni di cui cerchiamo soluzioni intere, scartando quindi eventuali altre soluzioni non intere.
La seguente funzione ci restituisce il grafico della funzione $4x + 6y = 4$ nell'intervallo $[-6,\ 6]$ e per vederne le soluzioni intere basta controllarne le intersezioni con il reticolo.

linearPlot[4, 6, 4, -6, 6];

Figura 11: Grafico della funzione $4x + 6y = 4$ nell'intervallo dell'asse x $[-6, 6]$

Per controllare, più precisamente, se un elemento è soluzione, basta utilizzare la seguente funzione **soluzioneQ[a, b, c, x, y]**(cfr. 2.3.4.2):

soluzioneQ[4, 6, 4, 1, 0];

True

Che restituisce *True* se la coppia (x, y) posta agli ultimi due posti, è soluzione.

soluzioneQ[4, 6, 4, -5, 4];

True

soluzioneQ[4, 6, 4, -1, 1];

False

Il caso in cui si debba studiare $ax + by = c$ dove $a = 0$ e $b = 0$ è particolare.

linearPlot[0, 0, 4, -6, 6];

- Power::infy : Infinite expression $\frac{1}{0}$ encountered.

- Plot::plnr : ComplexInfinity is not a machine-size real number at $x = -6\ldots$

- Plot::plnr : ComplexInfinity is not a machine-size real number at $x = -5.5132$.

- Plot::plnr : ComplexInfinity is not a machine-size real number at $x = -4.98229$.

- General::stop : Further output of Plot :: plnr will be suppressed during this calculation.

Figura 12: Grafico della funzione $0x + 0y = 4$

Stesso identico risultato si ha per $0X = 0Y = 0$
In entrambi i casi il computer restituisce un segnale di errore visto che, nel caso in cui $c = 0$, tutte le coppie sono soluzioni, mentre nel caso $c \neq 0$ non esistono soluzioni.

Studiamo ora, invece, la funzione $4x + 6y = 9$ per $-6 \leqslant x \leqslant 6$.

linearPlot[4, 6, 9, -6, 6];

Figura 13: Grafico della funzione $4x + 6y = 9$ nell'intervallo dell'asse x $[-6, 6]$

Già dalla figura vediamo che non ci sono soluzioni (almeno nella regione $-6 \leqslant x \leqslant 6$). Ad esempio facendo delle prove:

soluzioneQ[4, 6, 9, 4, -1];

False

La scelta dell'intervallo può essere modificata. Si consiglia, per una buona visione delle intersezioni con il reticolo, di non superare un "range" di 12 tra il minimo ed il massimo (l'ideale è 10).

linearPlot[4, 6, 9, 10, 20];

Figura 14: Grafico della funzione $4x+6y = 9$ nell'intervallo dell'asse delle x $[10, 20]$

linearPlot[4, 6, 9, -10, 10];

Figura 15: Grafico della funzione $4x + 6y = 9$ nell'intervallo dell'asse delle x $[-10, 10]$

Abbiamo quindi osservato che, al solo variare di c, due equazioni lineari si comportano in maniera completamente diversa:
$4x + 6y = 4$ ha soluzioni mentre $4x + 6y = 9$ non ne ha.

Osserviamo nuovamente il grafico della funzione $4x+6y = 4$. Per cercare una regola (Teorema 2.2) determiniamo qual'è la prima soluzione fuori dal grafico (cfr. Figura 11).
Osserviamo che la retta ha un'inclinazione pari a $-\frac{2}{3}$ e quindi le successive intersezioni (da ambo le parti del grafo) sono $(7, -4)$ e $(-8, 6)$ come è facilmente verificabile.

soluzioneQ[4, 6, 4, 7, -4];

True

soluzioneQ[4, 6, 4, -8, 6];

True

Verifichiamo che l'osservazione fatta è applicabile anche a $-5x + 2y = 4$.

linearPlot[5, 2, 4, -4, 4];

Figura 16: Grafico della funzione $5x+2y = 4$ nell'intervallo dell'asse delle x $[-4, 4]$

Avviene infatti che $(0, 2)$ e $(2, 7)$ sono due soluzioni "consecutive" dell'equazione.
Per concludere osserviamo che l'equazione $4x + 6y = 4$ può essere semplificata nel seguente modo: si possono dividere ambo i membri per $2 = \text{MCD}(4, 6, 4)$ ed ottenere così $2x + 3y = 2$ che ha le stesse soluzioni della precedente.
Questo, visto che non ci sono metodi semplici per la risoluzione di tali equazioni, non ci semplifica il compito della determinazione delle soluzioni di $2x + 3y = 2$. Sappiamo, comunque, che tramite l'Algoritmo Euclideo, esiste un metodo algoritmico per calcolare x ed y tali che: $2x + 3y = \text{MCD}(2, 3)$ (relazione di Bézout). Visto che $\text{MCD}(2, 3) = 1$, possiamo trovare dei valori per x ed y per i quali sia soddisfatta l'equazione $2x + 3y = 1$.

linearPlot[2, 3, 1, -4, 4];

Figura 17: Grafico della funzione $2x+3y = 1$ nell'intervallo dell'asse delle x $[-4, 4]$

Abbiamo creato una funzione per determinare i valori di x ed y in questi casi: **identitaBezout[a, b]**(cfr. 2.3.4.3).

identitaBezout[2,3]

{ -1, 1 }

Vediamo ora come possiamo trovare una soluzione dell'equazione diofantea $2X + 3Y = 2$ partendo dalla soluzione $x = -1$, $y = 1$ di $2X + 3Y = 1$.
Se moltiplichiamo $2(-1) + 3(1) = 1$ per 2 otteniamo $2(-2) + 3(2) = 2$, e $x = -2$, $y = 2$ è una soluzione di $2X + 3Y = 2$ come possiamo facilmente verificare.

soluzioneQ[2,3,2,-2,2]

True

Trovata quindi una soluzione, come possiamo trovarne altre?
Se (x_0, y_0) è una soluzione dell'equazione $aX + bY = \text{MCD}(a, b)$, avremo che $(x_0 - bt, y_0 + at)$, comunque preso t intero, è soluzione di $aX + bY = c$.

Algoritmo per la risoluzione delle Equazioni Diofantee lineari in due indeterminate:
Se $AX + BY = C$ ha soluzione, ricapitoliamo i passi da seguire per trovarle esplicitamente:

1. Semplificare l'equazione dividendo ambo i membri per $\text{MCD}(A, B, C)$ ed ottenendo $aX + bY = c$.
2. Trovare una soluzione per $aX + bY = 1$ usando l'Algoritmo Euclideo e poi usare tale risultato per determinare una soluzione di $aX + bY = c$.
3. Da questa soluzione, tramite le formule generali, determinare le altre soluzioni.

Questo algoritmo è stato implementato nella funzione **solEqDiofanto2[a, b, c, max, min]**(cfr. 2.3.4.5).
Usando tale metodo risolviamo: $39401X + 52111Y = 113119$ al variare di t tra -5 e 5.

solEqDiofanto2[39401, 52111, 113119, -5, 5]

Soluzioni dell'equazione sono: {{ 151,-112 }, { 192,-143 },
{ 233,-174 }, { 274,-205 }, { 315,-236 }, { 356,-267 }, { 397,-298 },
{ 438,-329 }, { 479,-360 }, { 520,-391 }, { 561,-422 } }

ottenute a partire dalla soluzione particolare { 356, -267 }

Poco sopra abbiamo trovato alcune soluzioni di $4X + 6Y = 4$. L'equazione $4X + 6Y = 9$ invece, risulta priva di soluzioni nonostante sia già ridotta.
Cerchiamo di applicare ora l'algoritmo descritto sopra a questa equazione:

$$4X + 6Y = \text{MCD}(4, 6) = 2.$$

identitaBezout[4,6]

{ -1,1 }

Ed otteniamo come soluzione $4(-1) + 6(1) = 2$.
Ciò però non ci aiuta a trovare una soluzione dell'equazione diofantea $4X + 6Y = 9$. Infatti, moltiplicando ambo i membri per $\frac{9}{2}$, una soluzione dell'equazione polinomiale data risulta: $x = -\frac{9}{2}$, $y = \frac{9}{2}$ e non essendo intera non possiamo accettarla.

Il fatto che l'algoritmo sopra descritto non sia efficace in questo caso, a priori non ci garantisce della non risolubilità dell'equazione.
Proviamo da un punto di vista teorico che l'equazione diofantea $4X+6Y = 9$ non è risolubile.
Supponiamo che (a, b) sia una soluzione dell'equazione $4X + 6Y = 9$. Allora $4a + 6b = 9$. Se $g = \text{MCD}(4, 6)$, si ha $g \mid 4$ e $g \mid 6$, quindi $g \mid 4a + 6b$. Ma $g \nmid 9$. Il che è assurdo (Teorema 2.2).

solEqDiofanto2[4, 6, 9, -10, 10]

Non ci sono soluzioni

Algoritmo per la risoluzione delle Equazioni Diofantee lineari in tre indeterminate:
Per questo argomento facciamo riferimento all'Esercizio 2.5 (c).
L'algoritmo lavora nel seguente modo:

1. Inseriamo l'equazione $aX + bY + cZ = d$;
2. Se $\text{MCD}(a, b, c) \mid d$ andiamo avanti, altrimenti l'equazione non ha soluzioni;
   Mod[GCD[a, b, c], d]
3. Risolviamo due equazioni:

$$a\xi_1 + \text{MCD}(b, c)\xi_2 = d \qquad \text{con solEqDiofanto2[a, MCD[b, c], d]}$$
$$b\zeta_1 + c\zeta_2 = \text{MCD}(b, c) \qquad \text{con identitaBezout[b, c]}$$

4. Determiniamo le soluzioni finali con le formule

$$x = \xi_1 + \frac{\text{MCD}(b, c)}{\text{MCD}(a, b, c)}t;$$
$$y = \zeta_1\xi_2 - \zeta_1\frac{a}{\text{MCD}(a, b, c)}t + \frac{c}{\text{MCD}(b, c)}s$$
$$z = \zeta_2\xi_2 - \zeta_2\frac{a}{\text{MCD}(a, b, c)}t - \frac{b}{\text{MCD}(b, c)}s$$

Verifichiamo dando le soluzioni per l'equazione $6X - 4Y + 8Z = 12$ in una regione delimitata dello spazio (Esercizio 2.5(d)) facendo riferimento alla funzione **solEqDiofanto3[a, b, c, d, min, max]** descritta in 2.3.4.6.

solEqDiofanto3[6, -4, 8, 12, 0, 2]

Soluzioni dell'equazione sono: {{{ 6,-6,-6 }, { 6,-4,-5 }, { 6,-2,-4 }},
{{ 8,-9,-9 }, { 8,-7,-8 }, { 8,-5,-7 }},
{{ 10,-12,-12 }, { 10,-10,-11 }, { 10,-8,-10}}}

ottenute a partire dai valori assunti da $\{\xi_1, \xi_2, \zeta_1, \zeta_2\}$ soluzioni delle equazioni descritte nel passo 3 dell'algoritmo: { 4, 8, 1, 1 }

2.3.2 Congruenze lineari

Le equazioni lineari sono le equazioni più semplici da risolvere.
Cerchiamo ora di studiare le soluzioni della congruenza $4X \equiv 2 \pmod 6$.
Tramite la funzione **soluzioni[a, b, m]**(cfr. 2.3.4.4) possiamo verificare quali elementi del SCR (Sistema Completo di Residui mod m) soddisfano la congruenza.

soluzioni[4, 2, 6]

$m = 6$	x	$4x$	$4x \equiv 2 \pmod 6$?
	0	0	False
	1	4	False
	2	8	True
	3	12	False
	4	16	False
	5	20	True

Le soluzioni (allargando il raggio di ricerca negli interi positivi minori di 20) risultano essere: $x = 2, 5, 8, 11, 14, 17,$ e 20.
Il seguente comando **visualizzaSol[a, b, m]**(cfr. 2.3.4.8) visualizza i numeri tra 0 e 99 in una scacchiera con in rosso i valori di x per cui $4x \equiv 2 \pmod 6$.

visualizzaSol[4, 2, 6]

Osserviamo che ogni 3 *quadretti* abbiamo una soluzione, cioè tutte le soluzioni sono congrue mod 3: $\{\dots 2, 5, 8, 11, 14, \dots\}$.
Possiamo anche controllare il valore delle soluzioni in un altro intervallo con la funzione **soluzioni[a, b, m, min, max]** 2.3.4.4:

soluzioni[4, 2, 6, 100, 110]

$m = 6$	x	$4x$	$4x \equiv 2 \pmod 6$?
	100	400	False
	101	404	True
	102	408	False
	103	412	False
	104	416	True
	105	420	False
	106	424	False
	107	428	True
	108	432	False
	109	436	False
	110	440	True

Anche qui resta la "regola" della congruenza mod 3.

Studiamo ora $4x \equiv 3 \pmod 6$.
Prima mettiamoci nell'intervallo $[0, 10]$ e poi allarghiamo la ricerca in $[0, 99]$.

soluzioni[4, 3, 6, 0, 10]

$m = 6$	x	$4x$	$4x \equiv 3 \pmod 6$?
	0	0	False
	1	4	False
	2	8	False
	3	12	False
	4	16	False
	5	20	False
	6	24	False
	7	28	False
	8	32	False
	9	36	False
	10	40	False

visualizzaSol[4, 3, 6]

Quindi, abbiamo appena visto che non tutte le congruenze lineari hanno soluzioni. Visualizziamo ora i vari comportamenti che ha la congruenza $2X \equiv b \pmod 6$ per tutti i possibili valori che può assumere $b \pmod 6$: $b = 0, 1, 2, 3, 4, 5$[7].

[7]Nel dischetto allegato al testo, quando si visualizzano tali grafici, si può cliccare con il mouse due volte sul primo grafico (oppure selezionarlo e premere CTRL+Y) per avere un'immagine in movimento.
Per questo bisogna partire il pacchetto di animazione con il comando:
≪ **Graphics'Animation'**

Do[visualizzaSol[2, b, 6], {b, 0, 5}]

Solo per $b = 0, 2, 4$ troviamo soluzioni.
Studiamo ora la congruenza $2X \equiv b \pmod 7$.

Do[visualizzaSol[2, b, 7], {b, 0, 6}]

Preso comunque b abbiamo soluzioni alla congruenza. Questo è quanto abbiamo infatti dimostrato nel Teorema 2.2.
Diamo, per finire, una prova "sperimentale" del Teorema 2.2.(b) sul numero delle soluzioni di una congruenza lineare:

TableForm[Table[soluzioni[a, 0, 7], {a, 1, 6}]]

$m=7$	x	$1x$	$1x \equiv 0 \pmod 7$?
	0	0	True
	1	1	False
	2	2	False
	3	3	False
	4	4	False
	5	5	False
	6	6	False

$m=7$	x	$2x$	$2x \equiv 0 \pmod 7$?
	0	0	True
	1	2	False
	2	4	False
	3	6	False
	4	8	False
	5	10	False
	6	12	False

$m=7$	x	$3x$	$3x \equiv 0 \pmod 7$?
	0	0	True
	1	3	False
	2	6	False
	3	9	False
	4	12	False
	5	15	False
	6	18	False

$m=7$	x	$4x$	$4x \equiv 0 \pmod 7$?
	0	0	True
	1	4	False
	2	8	False
	3	12	False
	4	16	False
	5	20	False
	6	24	False

$m=7$	x	$5x$	$5x \equiv 0 \pmod 7$?
	0	0	True
	1	5	False
	2	10	False
	3	15	False
	4	20	False
	5	25	False
	6	30	False

$m=7$	x	$6x$	$6x \equiv 0 \pmod 7$?
	0	0	True
	1	6	False
	2	12	False
	3	18	False
	4	24	False
	5	30	False
	6	26	False

Per la a, siamo partiti da 1 e non da 0 per evitare il caso banale in cui tutti i termini siano soluzioni.
Quindi abbiamo che $6x \equiv 4 \pmod{10}$ deve avere 2 soluzioni. Infatti:

soluzioni[6, 4, 10]

$m = 10$	x	$6x$	$6x \equiv 4 \pmod{10}$?
	0	0	False
	1	6	False
	2	12	False
	3	18	False
	4	24	True
	5	30	False
	6	36	False
	7	42	False
	8	48	False
	9	54	True

Algoritmo per la risoluzione delle congruenze lineari.
Per trovare una soluzione ad $aX \equiv b \pmod{m}$ con *Mathematica* :

1. Calcolare $d = \text{MCD}(a, m)$ tramite la funzione
   GCD[a,m];
2. Se $d \nmid b$, allora non ci sono soluzioni e quindi ci arrestiamo. Verificarlo con la funzione
   Mod[b,d]
   Se tale funzione dà risultato diverso da zero l'algoritmo si arresta.
3. Dividere a, b, e m per d per avere la congruenza $a'x \equiv b' \pmod{m'}$.
   Quotient[a,d]
   Quotient[b,d]
   Quotient[m,d]
4. Trovare c ed e per cui $a'c + m'e = 1$
   identitaBezout[a′, m′]
5. Moltiplicare per b' così da avere $a'(b'c) + m'(b'e) = b'$. E $b'c$ risulta soluzione dell'equazione ridotta.
6. Calcolare, $f \pmod{m'}$ con la funzione
   Mod[b′c, m′]
7. Tutte le soluzioni sono calcolabili tramite la funzione
   Table[f + km′, { k, 0, d-1 }].

Per la funzione **solCongLin[a, b, m]** vedere 2.3.4.7.

solCongLin[3, 5, 9]

Non ci sono soluzioni

solCongLin[360, 1656, 504]

{6, 13, 20, 27, 34, 41, 48, 55, 62, 69, 76, 83, 90, 97, 104, 111, 118, 125, 132,

139, 146, 153, 160, 167, 174, 181, 188, 195, 202, 209, 216, 223, 230, 237, 244, 251, 258, 265, 272, 279, 286, 293, 300, 307, 314, 321, 328, 335, 342, 349, 356, 363, 370, 377, 384, 391, 398, 405, 412, 419, 426, 433, 440, 447, 454, 461, 468, 475, 482, 489, 496, 503}

2.3.3 Le frazioni continue

In *Mathematica* esiste un pacchetto (Add-on Package) relativo alle Frazioni Continue.
Per richiamarlo occorre digitare il seguente comando:

<< NumberTheory‘ContinuedFractions‘

Abbiamo visto come le frazioni continue possono essere utilizzate per la scrittura di numeri razionali.
Ecco alcuni esempi:

ContinuedFraction[160/9]

$$17+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{2}}}$$

ContinuedFraction[23/37]

$$0+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2}}}}}}$$

La funzione inversa (cioè quella che a partire da una frazione continua restituisce un numero razionale) è la seguente:

Normal[ContinuedFractionForm[{ 3, 5, 4, 2, 7, 4, 2}]]

$\frac{10353}{3244}$

Verifichiamo “sperimentalmente” con questa funzione quanto dimostrato nel Teorema 6.

Normal[ContinuedFractionForm[{ 0, 5, 4, 5, 7, 7, 2 }]]

$\frac{2307}{12085}$

Normal[ContinuedFractionForm[{ 0, 5, 4, 5, 7, 7, 1, 1 }]]

$\frac{2307}{12085}$

Abbiamo poi parlato dei convergenti. Definiamo una funzione che permetta di calcolarli 2.3.4.9:

convergenti[23/37]

$\{0, 1, \frac{1}{2}, \frac{2}{3}, \frac{3}{5}, \frac{5}{8}, \frac{8}{13}, \frac{23}{37}\}$

Per concludere la discussione, verifichiamo come il metodo descritto nel Teorema 9 per la risoluzione delle equazioni diofantee tramite le frazioni continue (**solFraCon[a, b, c]** 2.3.4.10) dà (ovviamente) lo stesso risultato di quello sopra descritto.

solFraCon[205, 93, 1]

{ 49, 108}

Verifichiamo ora che si tratta di una soluzione:

soluzioneQ[205,-93,1,49,108]

True

2.3.4 Le funzioni utilizzate

Diamo ora una descrizione e la spiegazione delle funzioni definite in questo Paragrafo 2.
Per prima cosa dobbiamo "pulire" da funzioni eventualmente in memoria residua[8].

```
Off[General::"spell"];
Off[General::"spell1"];
```

♦ **2.3.4.1.** La funzione **linearPlot[a, b, c, min, max]** restituisce in verde il grafico della funzione $aX+bY = c$ nell'intervallo dell'asse x per x che varia tra [min, max] inserendo anche un reticolato blu per poter così determinare i punti a coordinate intere della funzione.
Per definirla occorre aprire il pacchetto *Colors* con il comando:

```
Needs["Graphics`Colors`"]

Clear[linearPlot];

linearPlot[a_, b_, c_, min_, max_, colore_:  Green] :=
    plot[(c - a x)/b, min, max, colore]

Clear[plot];
```

[8] Per le funzioni già definite nel precedente paragrafo vedere i riferimenti.

```
plot[f_, min_, max_, colore_:  Green] :=
    Plot[Evaluate[f], {x, min, max},
      PlotStyle-> {{colore, AbsoluteThickness[2]}},
      GridLines -> tickf,
      AxesStyle
        ->{{Red,  AbsoluteThickness[1.5]}, {Red,
            AbsoluteThickness[1.5]}}, Ticks -> tickf,
      AspectRatio -> 1/GoldenRatio,
      DisplayFunction -> DisplayFunction]

Clear[tickf];

tickf[m_,n_]:=Table[i,{i,Floor[m],Ceiling[n]}]
```

♦ **2.3.4.2.** La funzione **soluzioneQ[a, b, c, x, y]** restituisce la stringa *True* se x ed y risultano soluzioni dell'equazione $aX + bY = c$. Lavora solo se gli elementi inseriti in input risultano interi.

```
Clear[soluzioneQ];

soluzioneQ[a_Integer,b_Integer,c_Integer,x_Integer,y_Integer]:=
         a x+b y==c
```

♦ **2.3.4.3.** La funzione **identitaBezout[m, n]** restituisce una coppia $\{a, b\}$ che verifica $am + bn = \text{MCD}(m, n)$, calcolata applicando l'algoritmo euclideo in senso inverso, partendo dal risultato ottenuto con la funzione **listaGCD[m, n]** (1.6.3.1).

```
Clear[identitaBezout];

identitaBezout[m_,n_]:=
  Module[{l=listaGCD[m,n],
    coeff,
    a=1,
    b=0,
    appoggio,
    segno=1,
    risultato},
    coeff=Reverse[Drop[(#1[[3]]&)/@l,-1]];
    While[coeff != {},
        appoggio=a;
         a=appoggio First[coeff]+b;
         b=appoggio;
         coeff=Rest[coeff];
         segno=-segno];
    risultato={segno a,-segno b};
    Return[If[m>n,Reverse[risultato],
         risultato]]]
```

♦ **2.3.4.4.** La funzione **soluzioni[a, b, m]** elenca le x tra 0 ed $m - 1$ soluzioni di $aX \equiv b \pmod{m}$.

```
Clear[soluzioni];

soluzioni[a_,b_,m_, min_, max_]:=
  TableForm[Table[{"",x,a x,testCongruenza[a x,b,m]},{x,min,max}],
   TableHeadings ->{None,{"m = "<>ToString[m],"x",
    ToString[a]<>"x",
    ToString[a]<>"x = "<>ToString[b]<>" mod "<>ToString[m]<>"?"}},
   TableSpacing->{0,2}]

soluzioni[a_,b_,m_]:=
  TableForm[Table[{"",x,a x,testCongruenza[a x,b,m]},{x,0,m-1}],
   TableHeadings->
    {None,{"m = "<>ToString[m],"x",ToString[a]<>"x",
    ToString[a]<>"x = "<>ToString[b]<>" mod "<>ToString[m]<>"?"}},
  TableSpacing->{0,2}]
```

♦ **2.3.4.5.** La funzione **solEqDiofanto2[a, b, c, min, max]** restituisce la lista, per t che varia tra min e max, delle soluzioni di $aX + bY = c$ ottenute da una soluzione (x_0, y_0) calcolata utilizzando la funzione **identitaBezout[a, b]** (2.3.4.3).

```
Clear[diofanto2, solEqDiofanto2];

solEqDiofanto2[a_, b_, c_, min_, max_] :=
    If[Mod[c, GCD[a, b]] != 0,
      "Non ci sono soluzioni",
      diofanto2[a/GCD[a, b, c],
          b/GCD[a, b, c],
          c/GCD[a, b, c], min, max]];

diofanto2[a_, b_, c_, min_, max_] := Module[ {lista, prima},
    If[a <= 0,
      diofanto2[(-1)*a, (-1)*b, (-1)*c],
      lista= Table[{identitaBezout[a, b][[1]] c + b t,
          identitaBezout[a, b][[2]] c - a t},
          {t,  min,  max} ]];
    prima={identitaBezout[a, b][[1]] c,
           identitaBezout[a, b][[2]] c};
    Return[{Print["Soluzioni dell'equazione sono:", lista];
            Print["ottenute a partire
                  dalla soluzione particolare", prima]}]];
```

♦ **2.3.4.6.** La funzione **solEqDiofanto3[a, b, c, d, min, max]** restituisce la lista, per t ed s che variano tra min e max, delle soluzioni di $aX + bY + cZ = d$ ottenute a partire dai valori assunti dalle funzioni **x[i, a, b, c]** e **y[i, b, c]** calcolate utilizzando rispettivamente le funzioni **identitaBezout[a, b]** e **identitaBezout[b, c]** (2.3.4.3).

```
Clear[diofanto3, solEqDiofanto3, x, y];

solEqDiofanto3[a_, b_, c_, d_, min_, max_] :=
```

```
    If[Mod[d, GCD[a, b, c]] != 0,
       "Non ci sono soluzioni",
       diofanto3[a/GCD[a, b, c, d], b/GCD[a, b, c, d],
        c/GCD[a, b, c, d], d/GCD[a, b, c, d], min, max]];

diofanto3[a_,  b_,  c_, d_,  min_,  max_] := Module[{lista},
     lista= Table[{ x[1, a, GCD[b, c], d]  +
              (GCD[b, c]/GCD[a, b, c]) t,
              y[1, b, c] x[2, a, GCD[b, c], d] -
              y[1, b, c] (a/GCD[a, b, c]) t +
              (c/GCD[c, b]) s,
              y[2, b, c] x[2, a, GCD[b, c], d] -
              y[2, b, c] (a/GCD[a, b, c]) t  -
              (b/GCD[c, b]) s}, {t, min, max},
             {s, min, max}];
     Return[{Print["Soluzioni
                    dell'equazione sono: ", lista],
             Print["ottenute a partire dai valori assunti
                    da x1,x2,z1,z2 soluzioni delle
                    equazioni descritte nel passo 3
                    dell'algoritmo: ",
                    {x[1, a, b, c],  x[2, a, b, c],
                     y[1, b, c], y[2, b, c]}]}];]

x[i_, a_, b_, c_]:=identitaBezout[a, b][[i]] c;

y[i_,b_, c_]:=
  If[b<=0, identitaBezout[-(b), -(c)][[i]],
     identitaBezout[b, c][[i]]];
```

♦ **2.3.4.7.** La funzione **solCongLin[a, b, m]** restituisce la lista delle soluzioni di $aX \equiv b \pmod{m}$.

```
Clear[solCongLin];

solCongLin[a_, b_, m_]:=
  Module[{d=GCD[a,m]},
   If[Mod[b,d]!=0,
      "Non ci sono soluzioni",
       Module[{ap=Quotient[a,d],
           bp=Quotient[b,d],
           mp=Quotient[m,d],
           x,
           passoSucc,
           risultato},
         risultato=identitaBezout[ap,mp];
         x=risultato[[1]];
         passoSucc=Mod[bp x,mp];
         Table[passoSucc+mp k,{k,0,d-1}]]]]
```

♦ **2.3.4.8.** La funzione **visualizzaSol[a, b, m, max]** visualizza le soluzioni di $aX \equiv b \pmod{m}$ in rosso. Max indica il numero di righe da visualizzare[9].

```
Clear[visualizzaSol];

visualizzaSol[a_, b_, m_, maxTens_: 10] :=
    Module[{matrice},
      matrice =
        Table[If[Mod[a(10 i + j) - b, m] == 0, 0, 1], {i, 0,
            maxTens - 1}, {j, 0, 9}];
      ListDensityPlot[matrice, FrameTicks -> newtickf,
        FrameLabel -> {"unita'", "decine"},
        ColorFunction -> (Hue[#1\/4]&), RotateLabel -> False,
        PlotLabel ->
          FontForm[
            ToString[a]<>"x = "<>ToString[b]<>" mod "<>ToString[m],
              {"TimesRoman", 12}]]; ]
```

♦ **2.3.4.9.** La funzione **convergenti[a]** restituisce l'elenco di tutti i convergenti della scrittura in frazione continua di un numero a.

```
Clear[ convergente, convergenti, lunghezza, p, q];

convergenti[x_]:=
  Append[Append[convergenti1[x],
    p[lunghezza1[x], x] / q[lunghezza1[x], x]], x];

lunghezza[x_]:=Length[convergenti[x]];

convergente1[numero_, valore_]:= ContinuedFraction[valore, numero];

convergente[n_, x_]:=
  If[n < lunghezza1[x], convergente1[n, x],
    If[n == lunghezza1[x], (p[n-1, x]/q[n-1, x]) +
         (p[n-2, x]/q[n-2, x]),
      If[n == lunghezza1[x]+1, x]]];

lunghezza1[x_]:=Module[{i, j},
    i=1;
    j=1;
    While[j!=0,
     If[convergente1[i, x][[1]]!= convergente1[i+1, x][[1]],
       i++,
       j=0]];
    Return[i]];

convergenti1[x_]:=Table[p1[i, x]/ q1[i, x],
     {i, 1, lunghezza1[x]-1}];
```

[9] Per la funzione *newtickf* vedere 1.6.3.4.

```
p1[i_, x_]:=Numerator[Normal[ContinuedFractionForm[
           convergente1[i, x][[1]]]]];

q1[i_, x_]:=
  Denominator[Normal[ContinuedFractionForm[
           convergente1[i, x][[1]]]]];

p[i_, x_]:=If[i<lunghezza1[x], p1[i, x], p1[i-1, x] + p1[i-2, x]];

q[i_, x_]:=If[i<lunghezza1[x], q1[i, x], q1[i-1, x] + q1[i-2, x]];
```

♦ **2.3.4.10.** La funzione **solFraCon[a, b, c]** restituisce una soluzione dell'equazione $aX - bY = c$ applicando il metodo delle frazioni continue, nel caso che $\mathrm{MCD}(a, b) = 1$.

```
Clear[solFraCon, soluzioniFC, x];

solFraCon[a_Integer, b_Integer, c_Integer]:=
  If[GCD[a, b]!= 1,
     Print["Non possiamo applicare l'algoritmo"],
     soluzioniFC[a, b, c]];

soluzioniFC[a_, b_, c_]:=
    {(-1)^lunghezza[a/b]*c* q[lunghezza[a/b]-1, a/b],
      (-1)^lunghezza[a/b]*
         c* p[lunghezza[a/b]-1, a/b]};
```

3 Il "piccolo" Teorema di Fermat

3.1 I numeri di Carmichael

Nel Paragrafo 3 della prima parte (Definizione 3.6) sono stati introdotti i numeri di Carmichael. Questi particolari numeri sono oggetto di studio dal 1910 quando Robert Carmichael [C1] li descrisse per la prima volta definendoli *numeri pseudoprimi assoluti*[10].

Abbiamo detto che il più piccolo numero di Carmichael è 561. Nel suo articolo [C1] Carmichael definisce una funzione $\lambda(N)$ nel seguente modo:

$$\begin{aligned}
&\lambda(2^h) = \varphi(2^h) && \text{per } h = 0, 1, 2;\\
&\lambda(2^h) = \frac{1}{2}\varphi(2^h) && \text{per } h > 2;\\
&\lambda(q^h) = \varphi(q^h) && \text{per } q \text{ primo dispari;}\\
&\lambda(q_1^{h_1} \dots q_r^{h_r}) = \operatorname{mcm}(\lambda(q_1^{h_1}) \dots \lambda(q_r^{h_r})) && \text{per } q_j \text{ primi distinti.}
\end{aligned}$$

Tramite questa funzione Carmichael dimostrò che N è un numero pseudoprimo assoluto se e solo se:

$$N \equiv 1 \pmod{\lambda(N)}. \qquad (\star)$$

Da questo si deduce che quindi N e $\lambda(N)$ sono relativamente primi tra loro. Per quanto diremo in seguito dobbiamo premettere i seguenti risultati:

Teorema 16. *Ogni numero di Carmichael N si può scrivere come prodotto di primi dispari distinti (cioè $N = p_1 \cdots p_h$, $h > 2$) e $N-1 \equiv 0 \pmod{p_i - 1}$ con $1 \leqslant i \leqslant h$.*

Dimostrazione. Prendiamo in considerazione N tale che si abbia $a^{N-1} \equiv 1 \pmod{N}$.
Per prima cosa supponiamo che $N = 2^e$, con $e > 1$. Studiando $a^{2^e-1} \equiv 1 \pmod{2^e}$ ed osserviamo che per $a = 3$ ed $e \geqslant 2$ non è mai possibile; N deve, quindi, avere almeno un fattore dispari.

Supponiamo ora che $N = r \cdot p^e$ dove p è il primo con esponente e maggiore ed r è il prodotto dei restanti fattori.
Sia w una radice primitiva di p^e (Definizione 5.17), allora w, $w + 2 \cdot p^e$, $\dots$ sono primi e quindi esisterà s sufficientemente grande da avere che $x = w + s \cdot p^e$ è più grande di N.
x è primo con N e verifica:

$$x^{N-1} \equiv w^{N-1} \equiv 1 \pmod{p^e}.$$

[10] Il nome **numeri di Carmichael** è stato introdotto da N. G. W. H. Beerger in *On composite numbers n for which $a^{n-1} \equiv 1 \pmod{n}$ for every a prime to n*, Scripta Math. **16** (1950), pag 133 - 135.

Dato che w è una radice primitiva $N-1 \equiv 0 \pmod{p^e - p^{e-1}}$. Inoltre deve essere verificato che $N-1 = rp^e - 1$ è primo con p. L'unica possibilità è dunque che $e = 1$ e $N-1 \equiv 0 \pmod{p-1}$ e dato che $p-1$ è pari, allora N deve essere dispari.

Rimane da dimostrare che N è il prodotto di almeno tre primi ($h > 2$). Per assurdo scriviamo $N = p_1 \cdot p_2$ e, senza cadere in restrizioni, supponiamo $p_1 > p_2$.
Dato che $N-1 \equiv 0 \pmod{p-1}$ otteniamo:

$$p_1 \cdot p_2 - 1 \equiv p_2 - 1 \equiv 0 \pmod{p_1 - 1};$$

cioè, si dovrebbe avere che

$$\frac{p_1 p_2 - 1}{p_1 - 1} \in \mathbb{Z}$$

ma

$$\frac{p_1 p_2 - 1}{p_1 - 1} = p_2 + \frac{p_2 - 1}{p_1 - 1}.$$

dove il secondo termine risulterebbe intero se, e soltanto se, $p_2 \geqslant p_1$ per cui si arriva ad una contraddizione. □

Osservazione 17. Dal Teorema precedente e dalla definizione della funzione $\lambda(n)$ si ottiene che, per ogni N numero di Carmichael si avrà che $\lambda(N) = \text{mcm}(p_1 - 1, p_2 - 1, \ldots, p_k - 1)$.

Proposizione 18. *Sia N un numero di Carmichael e sia $\Lambda = \lambda(N)$. Se $p = \Lambda + 1$ è un primo e $N \not\equiv 0 \pmod{p}$, allora Np è un numero di Carmichael.*

Dimostrazione. Si tratta di un caso particolare del Teorema di Chernick (cfr. [Ch]) □

Corollario 19. *Non esistono due numeri $n, q \in \mathbb{N}$ tali che q ed $nq+1$ siano entrambi fattori primi di un numero di Carmichael.*

Dimostrazione. Per quanto abbiamo dimostrato nel Teorema 16, sappiamo che per essere fattori primi di un numero di Carmichael sia q che $nq+1$ devono essere primi **dispari**.
Supponendo quindi q primo dispari ($q = 2m+1$) abbiamo due possibilità che andiamo ad analizzare.
Sia n **dispari**. Allora $n = 2h+1$ con $h \in \mathbb{N}$. La quantità

$$nq = (2m+1) \cdot (2h+1) = 2(2mh + h + m) + 1$$

cioè risulta essere una quantità dispari e quindi $nq+1$ essendo pari non può essere un fattore primo di un numero di Carmichael.
Quindi dobbiamo supporre n **pari**. Ma allora $nq + 1 = 1 + 2h + 4mh$ che

può essere primo.
Supponiamo allora che $nq+1$ e q siano due fattori primi di N numero di Carmichael. Si avrebbe che $N-1 = s \cdot q \cdot (qn+1) \not\equiv 0 \pmod{qn}$ il che non è possibile per il Teorema 16. $\square$

Già Carmichael nel suo primo articolo presenta altri pseudoprimi assoluti (tutti con tre fattori).

Il ragionamento fatto per ottenerli era il seguente.
Partendo dall'idea che $N = pqr$ con p, q, r primi distinti (Teorema 16) e sapendo che deve essere verificato che $N-1 \equiv 0 \pmod{\lambda(N)}$, si ottengono:

$$\frac{pqr-1}{p-1}, \qquad \frac{pqr-1}{q-1}, \qquad \frac{pqr-1}{r-1};$$

sottraendo rispettivamente le quantità qr, rp, pq otteniamo così:

$$\frac{qr-1}{p-1}, \qquad \frac{pr-1}{q-1}, \qquad \frac{pq-1}{r-1} \tag{$\bullet$}$$

tutti interi.

Ponendo $p=3$ si verifica che le quantità sono intere per i seguenti valori di p, q, r: $3 \cdot 11 \cdot 17$.
Se invece poniamo $p=5$ si ottengono: $5 \cdot 13 \cdot 17,\ 3 \cdot 17 \cdot 29$.
Per finire, per $p=7$ si ottiene: $7 \cdot 13 \cdot 19,\ 7 \cdot 13 \cdot 31,\ 7 \cdot 19 \cdot 67,\ 7 \cdot 31 \cdot 73$.

Nell'articolo [Ch] Chernick introduce una formula universale per generare i numeri di Carmichael. Sia:

$$U_k(m) = (6m+1) \cdot (12m+1) \prod_{i=1}^{k-2} (9 \cdot 2^i m + 1),$$

allora $U_k(m)$ è un numero di Carmichael se tutti i suoi fattori sono primi.

Tramite l'utilizzo di questa funzione è stato possibile determinare i numeri di Carmichael con 101 cifre ($U_6(m)$), 321 e 1057 cifre ($U_3(m)$).
La difficoltà nell'utilizzo di questa funzione sta nel determinare il valore di k per cui i termini della produttoria siano simultaneamente primi.

La ricerca dei vari numeri di Carmichael ha occupato lo studio di molti matematici come Yorinaga che determinò nel 1978 due numeri di Carmichael con 18 fattori:

$$N = 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 73 \cdot 79 \cdot 89 \cdot 101 \cdot 109 \cdot 113 \cdot 127 \cdot 131 \cdot 1783$$

$$N = 19 \cdot 23 \cdot 29 \cdot 37 \cdot 41 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 89 \cdot 101 \cdot 103 \cdot 113 \cdot 127 \cdot 131 \cdot 137 \cdot 4421$$

3.1.1 Un algoritmo per calcolarli

L'algoritmo che andiamo a descrivere è stato sviluppato da Löh e Niebuhr [LN]. I risultati da loro ottenuti li presenteremo nel paragrafo 3.1.2.

Lo scopo dell'algoritmo è calcolare un numero di Carmichael N. Per prima cosa si determina un intero Λ per cui dovrà accadere che $\Lambda = \lambda(N)$ con N numero di Carmichael. A questo punto si determinano tutti i possibili fattori primi di N applicando l'Osservazione 17 ed il Corollario 19. Si ottiene così un insieme $\mathcal{S}$ con cardinalità κ. A questo punto si determinano gli elementi primi in $\mathcal{S}$ e se ne calcola il prodotto modulo Λ. Denotando tale valore con s si puó avere:
- $s = 1$: allora il prodotto di tali elementi è un numero di Carmichael per $(\star)$ (questo però è un caso raro);
- $s \neq 1$: costruiamo l'insieme $\mathcal{T} \subset \mathcal{S}$ minimo per cui il prodotto dei suoi elementi modulo Λ sia s. Se prendiamo ora in considerazione gli elementi restanti $\mathcal{F} = \mathcal{S} - \mathcal{T}$, i primi di $\mathcal{F}$ determinano un numero di Carmichael con $k = \kappa - \#\mathcal{T}$ fattori.

L'algoritmo, per come è sviluppato, non ci garantisce che alla fine si avrà $\lambda(N) = \Lambda$, ma di sicuro sarà che $\lambda(N) \mid \Lambda$. Questo perché, per come abbiamo costruito N, esso è un numero di Carmichael anche se $\lambda(N) \neq \Lambda$.
Quello che notiamo è che questa è una situazione patologica che può presentarsi nei casi in cui o $\#\mathcal{S}$ è piccola oppure $\#\mathcal{T}$ è grande.

Descriviamo schematicamente l'algoritmo:

A1 Determiniamo un intero Λ e scriviamone la fattorizzazione in primi $\Lambda = 2^e \prod_{i=1}^{r} q_i^{h_i}$.

A2 Costruiamo dei $p(\beta, \alpha_1, \ldots, \alpha_r) = 2^\beta \prod_{i=1}^{r} q_i^{\alpha_i} + 1$.

A3 $*$ Creiamo l'insieme $\mathcal{S}$ costituito da tutti i $p(\beta, \alpha_1, \ldots, \alpha_r)$ primi che non appartengano all'insieme $\{q_j\}_{j=1}^{r}$.
Se il valore $\Lambda + 1$ risulta essere uno di tali elementi ridefiniamo $\mathcal{S}$ come $\mathcal{S} \setminus \{\Lambda + 1\}$. In tal caso, infatti, per la Proposizione 18, ogni numero di Carmichael N ottenuto con tale algoritmo avente $\lambda(N) = \Lambda$, moltiplicato per $\Lambda + 1$ darebbe origine ed un altro numero di Carmichael.
$*$ Calcoliamo $s \equiv \prod_{p \in \mathcal{S}} p \pmod{\Lambda}$.
$*$ Se $s = 1$ allora $\mathcal{T} = \emptyset$ e vado al passo A5.

A4 Creo $\mathcal{T} \subset \mathcal{S}$ tale che $s \equiv \prod_{p \in \mathcal{T}} p \pmod{\Lambda}$.

A5 Calcolo:

$$N = \prod_{p \in \mathcal{S} - \mathcal{T}} p.$$

Per ottenere un numero di Carmichael con un elevato quantitativo di fattori primi, al passo A1 basta scegliere Λ in modo tale che $\kappa = \#\mathcal{S}$ sia molto grande.

Esempio. Scriviamo i dettagli di un particolare calcolo dell'algoritmo.

A1 Prendiamo $\Lambda = 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$.

A2 Otteniamo un totale di $4 \cdot 3 \cdot 2 \cdot 2$ possibilità per $p(\beta, \alpha_1, \ldots, \alpha_r)$.

A3 $\mathcal{S} = \{11, 13, 17, 19, 29, 31, 37, 41, 43, 61, 71, 73, 113, 127, 181, 211, 241, 281, 337, 421, 631, 1009, 2521\}$.
Si ha in questo modo che $\kappa = 23$.

A4 $s = 929 \pmod{\Lambda}$ per un totale di

$$\sum_{i=0}^{20} \binom{23}{i} = 8388331$$

possibili insiemi $\mathcal{T}$.

Come vediamo dall'esempio, la complessità dell'algoritmo sta nel calcolo di $\mathcal{T}$.
Descriviamo per sommi capi come hanno risolto il problema Löh e Niebuhr[11].

Si pone $t = s$ e a questo punto, tramite una scelta di elementi $p \in \mathcal{S}$, si divide t fino a giungere al valore $t = 1$.
Ponendo dunque $t_i \equiv t \pmod{q_i^{h_i}}$. Quindi si definisce $\mathcal{T} = p$ e se ne aggiungono altri fino a che:

$$\prod_{p \in \mathcal{T}} p \equiv s \pmod{\Lambda}.$$

Si è così costruito uno dei tanti possibili $\mathcal{T}$[12].

3.1.2 Risultati ottenuti dall'algoritmo

Il lavoro di Löh e Niebuhr è iniziato nel 1987 usando un computer IBM-compatibile e lavorando sotto DOS 3.1. Riportiamo qui di seguito tre risultati da loro ottenuti[13]:

[11] Per i dettagli rimandiamo all'articolo [LN, p. 828-829].

[12] Sempre nel loro articolo Löh e Niebuhr calcolano che ci sono ben

$$\mathcal{E}_{pos} = \frac{\sum_{i=0}^{\kappa-3} \binom{\kappa}{i}}{\varphi(\Lambda)}$$

possibili insiemi $\mathcal{T}$ per ogni $\mathcal{S}$ di cardinalità κ.

[13] Nello scrivere il valore di N si sono riscritte solo le prime 4 e le ultime 4 cifre.

Λ	N	cifre	Tempo
$2^6\,3^2\,5\,7\,11\,13\,17\,19$	$1185\ldots9441$	1504	30s
$2^8\,3^4\,5^2\,7^2\,11\,13\,17\,19\,23\,29\,31$	$2466\ldots9201$	81488	89m 57s
$2^{14}\,3^7\,5^4\,7^2\,11^2\,13^2\,17\,19\,23\,29\,31\,37\,41\,43\,47$	$7038\ldots0001$	16142049	9h 18m

Da come si vede i numeri calcolati sono molto elevati e anche il tempo per il calcolo risulta essere molto elevato. L'ultimo risultato è stato ottenuto nel 1992.

3.1.3 Stima sui numeri di Carmichael

Molte sono le proprietà dei numeri di Carmichael. Alcune di queste sono[14]:
- un numero di Carmichael è privo di fattori quadratici;
- un numero di Carmichael è il prodotto di almeno tre primi.

Nell'articolo in cui dimostrano che i numeri di Carmichael sono infiniti, Alfort, Granville e Pomerance danno anche una stima su quanti numeri di Carmichael si possono trovare al di sotto di un determinato valore:

$$C(x) = \#\{N \text{ di Carmichael } : N \leqslant x\} > x^{\frac{2}{7}}.$$

Se indichiamo con $C_k(x)$ il numero degli N minori di x con k fattori primi, abbiamo come problema aperto la non limitatezza di tale funzione per $k = 3$. Per il momento possiamo darne la seguente stima:

Teorema 20. *Per x sufficientemente grande, si ha:*

$$C_3(x) = \mathcal{O}(x^{\frac{5}{14}+o(1)}).$$

Dimostrazione. Sia N di Carmichael con tre fattori primi che denoteremo p, q ed r. Supponiamo $2 < p < q < r$. Si avrà che:

$$\begin{aligned} N - 1 &\equiv 0 \pmod{p-1} \\ N - 1 &\equiv 0 \pmod{q-1} \\ N - 1 &\equiv 0 \pmod{r-1}. \end{aligned}$$

Sia $g = \text{MCD}(p-1, q-1, r-1)$ e prendiamo a, b, c tali che siano verificate le seguenti identità:

$$p - 1 = ga \quad q - 1 = gb \quad r - 1 = gc.$$

[14]La dimostrazione di tali proprietà si trova in [K]

Di conseguenza (per l'ipotesi fatta su p, q, r) abbiamo che $a < b < c$. Abbiamo quindi che:

$$\begin{aligned} gbc + b + c &\equiv 0 \pmod{a} \\ gac + a + c &\equiv 0 \pmod{b} \\ gab + a + b &\equiv 0 \pmod{c} \end{aligned}$$

Che possono essere riassunte nella seguente congruenza:

$$g(ab + ac + bc) + a + b + c \equiv 0 \pmod{abc}$$

dato che a, b, c sono a due a due coprimi così che una volta determinati a, b, c anche $g \pmod{abc}$ è determinato.

Contiamo ora quante sono le quadruple (g, a, b, c) che soddisfano le condizioni sopra descritte e che in più $g^3abc \leqslant x$.
Abbiamo quindi che $C_3(x) \leqslant M$ con $M = M_1 + M_2 + M_3$ che sono rispettivamente[15]:
M_1 il numero delle quadruple (g, a, b, c) tali che $g > abc$;
M_2 il numero delle quadruple (g, a, b, c) tali che $x^{\frac{3}{14}} < g \leqslant abc$;
M_3 il numero delle quadruple (g, a, b, c) tali che $g \leqslant x^{\frac{3}{14}}$ e $g \leqslant abc$. □

3.2 Il software *Mathematica*

3.2.1 I sistemi di congruenze

Come abbiamo già visto nel paragrafo 2.3.2, con *Mathematica* è possibile calcolare la soluzione di congruenze lineari.
Risolviamo $7X \equiv 14 \pmod{50}$ facendo uso della funzione **congLineare[a, b, n]** (3.2.3.1) che a differenza di quella utilizzata nel paragrafo precedente (cfr. 2.3.4.7) fa uso della formula risolutiva.

congLineare[7, 14, 50]

{ 2 }

Risolviamo $15X \equiv 5 \pmod{40}$.

congLineare[15, 5, 40]

{ 27, 35, 3, 11, 19 }

In questo paragrafo però ci occuperemo in modo più ampio della risoluzione dei sistemi di r congruenze lineari.

$$\begin{cases} a_i X \equiv b_i \pmod{n_i} \\ 1 \leqslant i \leqslant r \end{cases}$$

[15] Per una stima più precisa di tali temini vedere [BN]

Per risolverli si è creata la funzione **sistemaCong[m]** (3.2.3.2) dove il sistema viene inserito sotto forma matriciale nel seguente modo:
$m = \{\{$ lista dei termini $a\}$, $\{$ lista dei termini $b\}$, $\{$ lista dei moduli $n\}\}$
La funzione da noi definita lavora nel seguente modo:

1. Data la matrice m il computer controlla che sia verificata la condizione necessaria e sufficiente per la risoluzione del problema (cfr. Esercizio 3.7) utilizzando la funzione **testCNS[m]** 3.2.3.3 e qualora non fosse verificata darebbe come output:

   m={{2, 2, 14, 54, 54, 34, 54}, {2, 3, 7, 65, 3, 65, 5}, {4, 8, 21, 8, 43, 5, 3}}

   {{ 2, 2, 14, 54, 54, 34, 54 }, { 2, 3, 7, 65, 3, 65, 5 }, { 4, 8, 21, 8, 43, 5, 3 }}

   sistemaCong[m];

   Il sistema dato in input $m = \begin{pmatrix} 2 & 2 & 4 \\ 2 & 3 & 8 \\ 14 & 7 & 21 \\ 54 & 65 & 8 \\ 54 & 3 & 43 \\ 34 & 65 & 5 \\ 54 & 5 & 3 \end{pmatrix}$

   non è risolubile.

2. Se la condizione necessaria e sufficiente risulta verificata si controlla che i moduli siano tutti relativamente primi a coppie (o come diremo brevemente "compatibili").
   testModuli[m] (3.2.3.4).
   Se questo non si verificasse:

   m={{2, 6, 2}, {2, 3, 6}, {8, 5, 12}}

   {{2, 6, 2}, {2, 3, 6}, {8, 5, 12}}

   sistemaCong[m];

   Il sistema dato in input $m = \begin{pmatrix} 2 & 2 & 4 \\ 6 & 3 & 5 \\ 2 & 6 & 12 \end{pmatrix}$

   non è trattabile con tale metodo.

3. Se, invece, i moduli risultano "compatibili", il computer trasforma il sistema di base m nel sistema m' applicando la funzione:
   sistemaTrasformato[m] (3.2.3.5)
   che semplifica le varie congruenze riducendole.

4. Si controlla quindi che il sistema abbia tutte congruenze risolubili tramite la funzione
   controlloModulo[m'] (3.2.3.6).
   Questa funzione verifica che nel ridurre le varie congruenze non si siano creati elementi razionali.

   m={{ 2, 2, 14, 7, 8 }, { 2, 3, 7, 9, 7 }, { 4, 5, 13, 7, 17 }}

   {{ 2, 2, 14, 7, 8 }, { 2, 3, 7, 9, 7 }, { 4, 5, 13, 7, 17 }}

   sistemaCong[m];

   Il sistema dato in input $m = \begin{pmatrix} 2 & 2 & 4 \\ 2 & 3 & 5 \\ 14 & 7 & 13 \\ 7 & 9 & 7 \\ 8 & 7 & 17 \end{pmatrix}$

   non è risolubile perché ha una congruenza non solubile.

5. A questo punto, superati questi controlli, il sistema m' viene ulteriormente semplificato con la funzione
   trasformoSistema[m'] (3.2.3.7)
   in modo da ottenere un sistema m'' con tutti termini 1 al posto dei termini a.

6. Ora si tratta di fare semplici calcoli:
   la funzione "built-in" **ChineseRemainderTheorem**[m''**(2),** m''**(3)**] mi restituisce la soluzione base;
   divisori[m] (3.2.3.9) mi restituisce il numero di soluzioni da calcolare;
   moduloFinale[m] (3.2.3.8) mi restituisce il modulo per cui vengono calcolate le varie soluzioni.

   m={{2, 2, 14}, {2, 3, 7}, {4, 5, 21}}

   {{2, 2, 14}, {2, 3, 7}, {4, 5, 21}}

   sistemaCong[m];

   Le soluzioni del sistema dato in input $m = \begin{pmatrix} 2 & 2 & 4 \\ 2 & 3 & 5 \\ 14 & 7 & 21 \end{pmatrix}$

   sono: {29, 59, 89, 119, 149, 179, 209, 239, 269, 299, 329, 359, 389, 419}
   Modulo 420

3.2.2 Numeri primi

Nel paragrafo 3 della prima parte, facciamo riferimento a vari tipi di numeri. Per prima cosa abbiamo parlato di un "test" sulla primarità di un numero

che però per numeri maggiori di 340 può sbagliare.
Per analizzare l'errore che commette tale criterio facciamo uso di alcune funzioni quali:

testPrimi[n] **3.2.3.18** verifica se il valore n soddisfa la condizione $2^n \equiv 2 \pmod{n}$. Qualora infatti tale condizione fosse verificata sappiamo che n è primo (Osservazione 3.4).

listaPrimi1[n] **3.2.3.19** determina una lista di tutti i primi (secondo il criterio dato dalla funzione **testPrimi[n]**) minori di n.

listaPrimi[n] **3.2.3.19** determina la lista di tutti i primi minori di n.

Nel grafico qui di seguito vediamo in rosso viene tracciata la linea che unisce i punti corrispondenti ai numeri primi mentre in blu i punti che risultano essere "primi" con il test descritto nell'Osservazione 3.4.

```
p1=ListPlot[ listaPrimi[400], PlotJoined − >True,
PlotStyle − > { PointSize[0.01],
RGBColor[1, 0, 0] }];
p2=ListPlot[listaPrimi1[400],
PlotStyle− > {PointSize[0.011], RGBColor[0, 0, 1]}];
Show[p1, p2];
```

Per osservare meglio la differenza tra le due liste utilizziamo la funzione **differenzaListe[lista1, lista2]** 3.2.3.22 in modo da avere un grafico più chiaro:

```
p1=ListPlot[differenzaListe[listaPrimi1[500], listaPrimi1[300]],
PlotJoined − > True,
PlotStyle− > { PointSize[0.015], RGBColor[1, 0, 0]}];
p2=ListPlot[differenzaListe[listaPrimi[500], listaPrimi[300]],
PlotStyle− > {PointSize[0.015], RGBColor[0, 0, 1]}];
Show[p1, p2];
```

Per continuare osserviamo la distribuzione dei primi (minori di 100) con la funzione **visualizzaPrimi[min, max]** 3.2.3.21 che ci restituisce una tabella 10×10 segnando in rosso i numeri che risultano effettivamente primi compresi tra i valori min e max.

visualizzaPrimi[1, 100]

Per confrontare ora i numeri primi con quelli calcolati applicando il Teorema di Wilson (pag. 29) ricorriamo ad un altro tipo di grafico.
I numeri primi li otteniamo tramite il crivello di Eratostene graficandolo tramite la funzione **eseguiCrivelloA[max]** 3.2.3.11 che visualizza in sei grafici i vari passaggi del crivello.
Applichiamo la funzione ai numeri minori di 150.

eseguiCrivelloA[150]

Visualizziamo ora i Primi secondo il Teorema di Wilson e confrontiamoli con l'ultima tabella ottenuta dalla funzione precedente.

s=calcolaCrivelloB[inCrivelloB[150]];
visualizzaCrivelloB[s]

Osserviamo che le due tabelle coincidono (si noti che la prima ha una riga in più). Questo conferma quanto già abbiamo dimostrato nell'osservazione 3.9(b) e cioè che i numeri che verificano il Teorema di Wilson sono tutti e soli i numeri primi.

3.2.3 Funzioni utilizzate

♦ **3.2.3.1.** La funzione **congLineare[a, b, n]** restituisce una lista di tutte le possibili soluzioni non congrue della congruenza lineare $aX \equiv b \pmod{n}$. Utilizza la funzione **conglineare[a, b, n, k]** ponendo i limiti di k tra 0 e $\mathrm{MCD}(a, n) - 1$.

```
Clear[congLineare, conglineare];

conglineare[a_, b_, n_, k_]:=
    Mod[(a/GCD[a, n])^(EulerPhi[n/GCD[a,n]]-1) (b/GCD[a,n]) +
       k(n/GCD[a, n]), n];

congLineare[a_, b_, n_]:=
  If[Mod[b, GCD[a, n]]==0,
    Table[conglineare[a, b, n, k], {k, 0, GCD[a, n]-1}],
    "Non ci sono soluzioni"];
```

♦ **3.2.3.2.** La funzione **sistemaCong[m]** restituisce le soluzioni del sistema di congruenze inserito in input nel seguente modo:
$m = \{\{\text{lista dei coefficienti}\}, \{\text{lista dei termini noti}\}, \{\text{lista dei moduli}\}\}$.
Per fare ciò fa uso di varie funzioni secondarie, nel seguente modo:
calcola il valore della funzione **testCNS[m]** per il sistema dato in input, se tale valore risulta essere pari ad ∞ restituisce l'output già descritto in precedenza, altrimenti continua il calcolo.
A questo punto effettua un'altro test per vedere se il sistema è compatibile. Una volta esauriti i test, trasforma il sistema in modo da ottenere un sistema risolubile con la funzione built-in **ChineseRemainderTheorem** A questo

punto, a partire da tale soluzione, applica la formula descritta nella prima parte.

```
Clear[sistemaCong ];

<<NumberTheory‘NumberTheoryFunctions‘

sistemaCong[m_]:=
  Module[{test, m1, controllo, m2, z, x, y, m3},
    test=testCNS[m];
    m3=Transpose[m];
    If[test==Infinity,
       Return[{Print["Il sistema dato in input: m= ",
                     MatrixForm[m3]],
            Print["non e’ risolubile."]}]];
    test=testModuli[m];
    If[test==Infinity,
        Return[{Print["Il sistema dato in input: m= ",
                      MatrixForm[m3]],
          Print["non e’ trattabile con tale metodo."]}]];
    m1=sistemaTrasformato[m];
    controllo=controlloModulo[m1];
    If[controllo==Infinity,
           Return[{Print["Il sistema dato in input: m= ",
                         MatrixForm[m3]],
                   Print["non e’ risolubile perche’ ha una
                            congruenza non solubile."]}]];
    m2=trasformoSistema[m1];
    x=ChineseRemainderTheorem[m2[[2]], m2[[3]]];
    z=divisori[m];
    y=Table[Mod[x+k moduloFinale[m2], moduloFinale[m]],{k, 0, z-1}];
    Return[{Print["Le soluzioni del sistema dato in input: m= ",
                MatrixForm[m3]],
             Print["sono: ", y],
             Print["Modulo ", moduloFinale[m]]}]];
```

♦ **3.2.3.3.** La funzione **testCNS[matrice]** verifica che sia soddisfatta la condizione descritta nell'Esercizio 3.7 scorrendo la matrice ed incrementando il valore assegnato alla quantità *test* se è verificata la condizione $\frac{m_{1i}-m_{1j}}{\mathrm{MCD}(m_{3i},m_{3j}} \in \mathbb{Z}$, altrimenti associa alla quantità *male* il valore ∞. Come output restituisce il valore più grande tra *test* e *male*.

```
Clear[testCNS];

testCNS[m_]:=
  Module[{test, male},
    male=0;
    test=1;
    Do[
      For[j=Length[m[[1]]],j>i, j--,
```

```
        If[IntegerQ[(m[[1, i]] - m[[1, j]])/
              GCD[m[[3, i]], m[[3, j]]]],
          test++,
          male=Infinity]],
      {i, 1, Length[m[[1]]]-1}];
     If[male>test,
          Return[male],
          Return[test]]];
```

Diamo due esempi per essere più chiari.

m={{2, 2, 14}, {2, 3, 7}, {4, 5, 21}}
testCNS[m]

{{2, 2, 14}, {2, 3, 7}, {4, 5, 21}}
4

m={{2, 2, 15}, {2, 3, 7}, {3, 5, 21}}
testCNS[m]

{{2, 2, 15}, {2, 3, 7}, {3, 5, 21}}
∞

♦ **3.2.3.4.** La funzione **testModuli[m]** controlla che i moduli del sistema siano relativamente primi a coppie. Il ragionamento su cui si basa è lo stesso usato per la funzione **testCNS[m]** 3.2.3.3 come anche l'output finale.

```
Clear[testModuli];

testModuli[m_]:=
  Module[{test, male},
    male=0;
    test=1;
    Do[
      For[j=Length[m[[1]],j>i, j--,
        If[GCD[m[[3, i]],m[[3, j]]]!= 1,
          male=Infinity,
          test++]],
      {i, 1, Length[m[[1]]]-1}];
  If[male>test,
    Return[male],
    Return[test]]];
```

m={{2, 2, 15}, {2, 3, 5}, {4, 5, 7}}
testModuli[m]

{{2, 2, 15}, {2, 3, 5}, {4, 5, 7}}
4

m={{2, 2, 15}, {2, 3, 5}, {4, 6, 8}}

testModuli[m]

{{2, 2, 15}, {2, 3, 5}, {4, 6, 8}}
∞

♦ **3.2.3.5.** La funzione **sistemaTrasformato[matrice]** trasforma il sistema dato in input, "riducendo" ogni congruenza con una "equivalente minimale".

```
Clear[sistematrasformato];

sistemaTrasformato[matrice_] :=
    Table[m[[i,  j]] = (matrice[[i,  j]]/
          GCD[matrice[[1,  j]], matrice[[3,  j]]]),
      {i, 1, 3},
      {j, 1, Length[matrice[[1]]]}];
```

Per fare questo abbiamo usato un'opzione "nuova" della funzione built-in **Table**. Abbiamo cioè usato due variabili i e j da incrementare nel seguente modo: fissata $j = 1$ si fa variare i tra 1 e 3, quindi si incrementa j e si resetta i in modo da farla variare nuovamente tra 1 e 3, ... fino a che j supera il numero di equazioni del sistema.
Diamo un esempio:

m={{4, 6, 5}, {7, 12, 3}, {5, 6, 9}}

{{4, 6, 5}, {7, 12, 3}, {5, 6, 9}}

sistemaTrasformato[m]

{{4, 1, 5}, {7, 2, 3}, {5, 1, 9}}

♦ **3.2.3.6.** La funzione **controlloModulo[matrice]** verifica che il sistema dato in input sia trattabile con il Teorema Cinese dei Resti.
Nel caso non lo sia, restituisce il valore ∞.
Il ragionamento con cui è stata sviluppata è lo stesso usato per la funzione **testCNS** 3.2.3.3.

```
clear[controlloModulo];

controlloModulo[m_]:=
  Module[{test, male},
    male=0;
    test=1;
    For[j=1, j<=Length[m[[1]]], j++,
      If[IntegerQ[m[[2, j]]],
        test++,
        male=Infinity]];
    If[male>test,
      Return[male],
      Return[test]]];
```

m={{4, 6, 5}, {7, 5, 3}, {5, 41, 9}}
controlloModulo[m]

{{4, 6, 5}, {7, 5, 3}, {5, 41, 9}}
4

m={{4, 6, 5}, {7, 5/3, 3}, {5, 41, 9}}
controlloModulo[m]

{{4, 6, 5}, {7, $\frac{5}{3}$, 3}, {5, 41, 9}}
∞

♦ **3.2.3.7.** La funzione **trasformoSistema[matrice]** trasforma il sistema in un sistema associato ponendo i coefficienti delle X tutti pari a 1 e modificando gli elementi della seconda colonna secondo la regola $m_{1j}^{\varphi(m_{3j})-1} \cdot m_{2j}$ riscalando tutto $\pmod{m_{3j}}$. Gli unici elementi che restano invariati sono quelli della terza colonna.

```
trasformoSistema[matrice_]:=
  Module[{m},m=matrice;
    Table [m[[1, j]]=1, {j, 1, Length[matrice[[1]]]}];
Table [m[[2, j]]=
        Mod[(matrice[[1, j]]^(EulerPhi[matrice[[3, j]]]-1))*
            matrice[[2, j]],
          matrice[[3, j]] ], {j, 1,Length[matrice[[1]]]};
    Table[m[[3, j]]=
        matrice[[3, j]], {j, 1,
        Length[matrice[[1]]]};
Return[m]];
```

Si osservi che nella funzione non si è modificata direttamente la matrice in input (*matrice*), ma si è creata una matrice copia (m) che è stata modificata. Questo perchè per scrivere i "nuovi" elementi della seconda colonna si utilizzano i "vecchi" elementi della prima e se avessimo mantenuto una sola matrice ci saremmo trovati con tutti elementi pari ad 1.
Si poteva però, per usare una sola matrice, modificare prima la seconda riga e poi la prima. Non si è fatta questa scelta perché il programma sarebbe risultato più difficile da capire alla lettura e non si sarebbero tratti vantaggi di tempo.
Diamo un esempio:

m={{4, 6, 5}, {7, 9, 3}, {8, 14, 21}}

{{4, 6, 5}, {7, 9, 3}, {8, 14, 21}}

trasformoSistema[m]

{{1, 1, 1}, {0, 12, 9}, {8, 14, 21}}

♦ **3.2.3.8.** La funzione **moduloFinale[m]** calcola il modulo finale in cui, nella funzione **sistemaCong[m]** 3.2.3.2 vengono espresse le soluzioni del sistema di congruenze associato alla matrice in input.
Il calcolo viene svolto in modo molto semplice: si moltiplicano tra loro tutti gli elementi della terza colonna della matrice m.

```
moduloFinale[matrice_]:=
  Module[{modulo}, modulo=1;
    For[ i=1, i<=Length[matrice[[1]]],
      i++, modulo =
        modulo * matrice[[3, i]]];
    Return[modulo]];
```

Diamo un esempio:

m={{1, 1, 1}, {7, 9, 3}, {8, 3, 7}}

{{1, 1, 1}, {7, 9, 3}, {8, 3, 7}}

moduloFinale[m]

168

♦ **3.2.3.9.** La funzione **divisori[m]** calcola i vari MCD tra gli elementi della prima colonna e i rispettivi elementi della terza colonna (cioè il MCD(m_{1i}, m_{3i})) e quindi fa il prodotto.

```
divisori[matrice_]:=
  Module[{div}, div=1;
    For[ i=1, i<=Length[matrice[[1]]],
      i++, div =
        div * GCD[matrice[[3, i]],
            matrice[[1, i]]]];
    Return[div]];
```

Ad esempio:

m={{7, 8, 4}, {7, 9, 3}, {14, 5, 7}}

{{7, 8, 4}, {7, 9, 3}, {14, 5, 7}}

divisori[m]

7

♦ **3.2.3.10.** La funzione **funzioneListe[lista1, lista2]** restituisce un grafico riportante la differenza tra i vari valori di due liste.

```
funzioneListe[l1_, l2_]:=
  Module[{grafico, funzione},  m=Min[Length[l1], Length[l2]];
    funzione=
```

```
    Table[l1[[i]]-
        l2[[i]], {i, 1,  m}];
  grafico=ListPlot[funzione,
      PlotStyle->{PointSize[0.015], RGBColor[1, 0, 0]}];
  Return[funzione]];
```

Analizziamo ora le funzioni che ci hanno permesso di graficare il Crivello di Eratostene.

♦ **3.2.3.11.** È noto che n è primo se e soltanto se $(n-1)! \equiv -1 \pmod{n}$. La funzione **eseguiCrivelloA[max]** mette insieme varie funzioni. Lo scopo è quello di creare una tabella con i numeri primi segnati in rosso applicando il Crivello di Eratostene.
Per prima cosa tale funzione crea una lista 3.2.3.12 subito visualizzata con la funzione **visualizzaCrivelloA** 3.2.3.14. Quindi, per tutti i primi minori del valore dato in input, **calcolaCrivelloA** 3.2.3.13.

```
Clear[eseguiCrivelloA];

eseguiCrivelloA[u_]:=
  Module[{s=Table[0,{u}],n},
    s[[1]]=
      s[[2]]=1;n=1;
     visualizzaCrivelloA[s];
    While[Prime[n] Prime[n]<u,
     s=calcolaCrivelloA[s,Prime[n]]; n++;
     visualizzaCrivelloA[s]];]
```

♦ **3.2.3.12.** La funzione **iniziaCrivelloA[m]** crea una lista di m elementi tutti pari a 0 tranne i primi due che vengono posti pari ad 1.

```
Clear[iniziacrivelloA];
iniziacrivelloA[n_]:=
  Module[{s=Table[0,{n}]},
    s[[1]]=
      s[[2]]=1;s]
```

iniziaCrivelloA[14]

{1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}

♦ **3.2.3.13.** La funzione **calcolaCrivelloA[s, p]** prendendo la lista s assegna il valore 1 a tutti i termini s_i della lista s che risultano verificare la seguente proprietà: $i-1$ è divisibile per p.

```
Clear[calcolaCrivelloA];
calcolaCrivelloA[s_,p_]:=
  Module[{t=s},
    Do[t[[i+1]]=
        If[Mod[i,p]==0,1,t[[i+1]]],
         {i, 2 p, Length[t]-1}];
      t]
```

s= {1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}
calcolaCrivelloA[s ,2];

{1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1}

♦ **3.2.3.14.** La funzione **visualizzaCrivelloA[s]** crea una tabella sulla base dei valori assunti nella lista s, colorando di Rosso i posti che hanno associato il valore 1.

```
Clear[visualizzaCrivelloA];
newtickf[minimo_,maximo_]:=
   Table[{i+1/2,i},{i,Floor[minimo],Ceiling[maximo]}];

visualizzaCrivelloA[s_] :=
    Module[{u}, u = Ceiling[Length[s]/10];
      ListDensityPlot[Partition[s, 10],
        FrameTicks->{newtickf, Table[{i - 1/2, i - 1}, {i, 1, u}]},
        FrameLabel->{"unita'", " "},
        ColorFunction->(Hue[#1/0.21]&)]; ]
```

s=Table[Random[Integer, 0, 1], i, 1, 100];
visualizzaCrivelloA[s]

Analizziamo ora le funzioni che ci hanno permesso di graficare i numeri che verificano la seguente condizione:

$$2^n - 2 \equiv 0 \pmod{n}$$

Per distinguerlo dal Crivello di Eratostene si è deciso di chiamarlo **CrivelloB**.

♦ **3.2.3.15.** La funzione **inCrivelloB[n]** restituisce un lista di n elementi. I primi due risultano essere pari ad 1 mentre gli altri risultano tutti pari a 0.

```
Clear[inCrivelloB];
inCrivelloB[n_]:=
  Module[{s=Table[0,{i, 2, n}]},
    s[[1]]=
      s[[2]]=1; s]
```

inCrivelloB[10]

{1, 1, 0, 0, 0, 0, 0, 0, 0}

♦ **3.2.3.16.** La funzione **visualizzaCrivelloB[*lista*]** crea una scacchiera colorata 10× (lunghezza *lista*) con in rosso i quadretti corrispondenti al valore 0 e in giallo quelli a valore 1.
Si noti che la lunghezza della lista deve essere un maggiore di 20 per permettere al computer di tracciare una scacchiera.

```
Clear[visualizzaCrivelloB]
visualizzaCrivelloB[s_] :=
    Module[{u}, u = Ceiling[Length[s]/10];
      ListDensityPlot[Partition[s, 10],
        FrameTicks -> {newtickf, Table[{i - 1/2, i - 1},
           {i, 1, u}]},
        FrameLabel -> {"unita'", " "},
        ColorFunction -> (Hue[#1/6]&)]];
```

s=Table[Random[Integer, 0, 1], i, 1, 100];
visualizzaCrivelloB[s]

♦ **3.2.3.17.** La funzione **calcolaCrivelloB[s]** assegna il valore 1 al termine i della lista s se il valore $i-1$ è un "primo" secondo la funzione testPrimi[n].

```
Clear[calcolaCrivelloB];
testPrimi[m_]:=If[Mod[2^m-2, m]==0, 0,1];

calcolaCrivelloB[s_]:=
  Module[{t=s},
    Do[t[[i+1]]=
        If[testPrimi[i]==0,1,t[[i+1]]],{
        i,2,Length[t]-1}];t]
```

calcolaCrivelloB[{1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}]

{1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1}

♦ **3.2.3.18.** La funzione **testPrimi[n]** assegna il valore 0 ai numeri che verificano: $2^n - 2 \equiv 0 \pmod{n}$ (Osservazione 3.4).

```
Clear[testPrimi];
testPrimi[m_]:=If[Mod[2^m-2, m]==0, 0,1]
```

♦ **3.2.3.19.** Le funzioni **listaPrimi[n]** e **listaPrimi1[n]** restituiscono l'elenco dei numeri minori di n che verificano **PrimeQ** (funzione built-in che determina se un intero è "veramente primo") e **testPrimi** (funzione sopra definita) rispettivamente.

```
Clear[listaPrimi, listaPrimi1];

listaPrimi[m_]:=
  Module[{risultato, appoggio},
        risultato={2};
        appoggio=Range[m];
For[i=3, i<=m, i++,
          If[PrimeQ[appoggio[[i]]],
           risultato= Append[risultato,
            appoggio[[i]]]]];
        Return[risultato]];

listaPrimi1[m_]:=
  Module[{risultato, appoggio},
     risultato={2};
     appoggio=Range[m];
     For[i=3, i<=m, i++,
      If[testPrimi[appoggio[[i]]]==0,
        risultato=
          Append[risultato,
            appoggio[[i]]]]];
    Return[risultato]];
```

♦ **3.2.3.20.** Le funzioni **testWilson[n]** restituisce il valore della congruenza $(n-1)!\pmod{n}$.

```
Clear[testWilson]
testWilson[a_]:=
If[Mod[Factorial[a-1], a]==Mod[-1, a], -1, Mod[Factorial[a-1], a]]
```

♦ **3.2.3.21.** La funzione **visualizzaPrimi[min, max]** crea una tabella nella quale visualizza tutti i primi (in rosso) tra Min e Max.

```
Clear[visualizzaPrimi]
visualizzaPrimi[min_,max_]:=
     Module[{t,u,n,sum,array,t1,t2},
       t1=Floor[min/10];
       t2=Ceiling[max/10]+1;
       array=Table[0,{t,t1,t2-1},{u,1,10}];
       For[t=t1+1,t<=t2,t++,
          For[u=1,u<=10,u++, n=10 (t-1)+(u-1);
           array[[t-t1,u]]=
            If[PrimeQ[n],0,1]]];
```

```
      ListDensityPlot[array,
              FrameTicks->{newtickf,Table[{i-t1+1/2,i},
                     {i,t1,t2-1}]},
FrameLabel->{"unita'",""},
               ColorFunction->(Hue[#1 (5)/9]&)]]
```

♦ **3.2.3.22.** La funzione **differenzaListe[lista1, lista2]** sottrae dalla lista più lunga i primi n elementi dove n è la lunghezza della lista più breve. Tale funzione è stata creata a partire dal presupposto che la lista1 sia un'estensione della lista2. Cioè, se si suppone che la lista2 abbia n elementi, la lista1 ne avrà $m > n$ e soprattutti i primi n coincidono con quelli della lista2.

```
Clear[differenzaListe];
differenzaListe[lista1_, lista2_]:=
  Module[{ risultato},
     m=Length[lista1];
     n=Length[lista2];
     If[m<n,
       differenzaListe[lista2, lista1]];
       risultato=
         Table[lista1[[i]], {i, n+1, m}];
     Return[risultato]];
```

s1=Table[i, i, 1, 20]

{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20}

s1=Table[i, i, 1, 10]

{1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

differenzaListe[s1, s2]

{11, 12, 13, 14, 15, 16, 17, 18, 19, 20}

4 Generalità sulle congruenze polinomiali, Teorema di Lagrange e Teorema di Chevalley

Nel corso del Paragrafo 4 della prima parte (cfr. pag. 38) abbiamo considerato congruenze particolari (Esempio 4.9, Lemma 4.11). Approfondiamo ora lo studio di congruenze polinomiali del tipo:

$$f_p = X^p - X \equiv 0 \pmod{p} \qquad (\mathfrak{F})$$

con p primo.

4.1 Il polinomio $X^p - X$

Sappiamo che la congruenza $(\mathfrak{F})$ ha al massimo p soluzioni (Teorema 4.18). Applicando il "Piccolo" Teorema di Fermat (Teorema 3.1) si può concludere, più precisamente, che la congruenza $(\mathfrak{F})$ ha **esattamente** p soluzioni.
L'esistenza del polinomio $f_p(X) = X^p - X$ con tale caratteristica ci permette, nel caso di una congruenza polinomiale modulo p-primo, di limitare lo studio a polinomi di grado al massimo p.

Suppiamo che $f(X)$ sia un polinomio tale che $\deg(f) \geqslant p$. Dividendo il polinomio $f(X)$ per $f_p(X)$ si ottiene:

$$f(X) = f_p(X)g(X) + r(X)$$

con $g(X)$ e $r(X) \in \mathbb{Z}[X]$ e $0 \leqslant \deg(r(X)) < p$.
Tale divisione non restituisce alcun polinomio a coefficienti razionali perché il polinomio $f_p(X)$ ha coefficiente direttore pari a 1.
La congruenza $f(X) = (X^p - X)g(X) + r(X) \equiv 0 \pmod{p}$ risulta avere quindi come insieme di soluzioni lo stesso della congruenza $r(X) \equiv 0 \pmod{p}$ e solo nel caso in cui $r(X) \equiv_X 0 \pmod{p}$ la congruenza $f(X) \equiv 0 \pmod{p}$ ha il massimo delle soluzioni, e cioè p soluzioni.

Proposizione 21. *La congruenza polinomiale $f(X) \equiv 0 \pmod{p}$, con p primo e $n = deg(f(x))$ e in più con il coefficiente direttore di $f(X)$ pari a 1, ha esattamente n soluzioni se, e solo se, esistono $q(X), r'(X) \in \mathbb{Z}[X]$ tali che:*

$$X^p - X = f(X)q(X) + pr'(X)$$

e $0 \leqslant deg(r'(X)) < p$.

Dimostrazione. Se la congruenza risulta avere n soluzioni allora, necessariamente, $n \leqslant p$.
Applicando la divisione tra polinomi ad $f_p(X)$ e $f(X)$ otteniamo:

$$f_p(X) = f(X)q(X) + r(X)$$

dove $0 \leqslant \deg(r(X)) < p$.
Come dicevamo prima, questa uguaglianza ci garantisce che le soluzioni per

$f(X)$ coincidono con quelle per $r(X) \equiv 0 \pmod{p}$.
Nel caso in cui $\deg(r(X)) > 0$, visto che per ipotesi la congruenza ha n soluzioni, deve essere $\deg(r(X)) = n$. Perché questa condizione sia verificata $r(X) = pr'(X)$ dove $r'(X)$ verifica la tesi dell'enunciato.

Assumiamo dunque che la scomposizione sia $X^p - X = f(X)q(X) + pr'(X)$ verificante le ipotesi descritte nell'enunciato. Risulta così che $f(X)q(X) \equiv 0 \pmod{p}$ ha p soluzioni.
Per il Teorema di Lagrange (Teorema 4.18) e per le ipotesi del testo, abbiamo che le congruenze $f(X) \equiv 0 \pmod{p}$ e $q(X) \equiv 0 \pmod{p}$ hanno, rispettivamente, al massimo n e $(p-n)$ soluzioni.
In più il fatto che $f(X)q(X) \equiv 0 \pmod{p}$ determina, in particolare, che $f(X) \equiv 0 \pmod{p}$ deve avere esattamente n soluzioni. □

Applicando tale ragionamento possiamo ridimostrare il Teorema di Wilson (cfr. pag. 29).
Per il Teorema di Lagrange (Teorema 4.18) sappiamo che la congruenza $X^p - 1 \equiv 0 \pmod{p}$ ha non più di $p-1$ soluzioni ma il "Piccolo" Teorema di Fermat (Teorema 3.1) ci garantisce che ha **esattamente** $p-1$ soluzioni e cioè: $\{1, 2, 3, \ldots, p-1\}$.
Applicando la Proposizione 21 otteniamo:

$$X^p - X = (X^{p-1} - 1)q(X) + pr'(X)$$

con $q(X)$ e $r'(X) \in \mathbb{Z}[X]$, precisamente $q(X) = X$ e $r'(X)$ polinomio nullo. In più, conoscendo esplicitamente le soluzioni di $X^p - 1 \equiv 0 \pmod{p}$ possiamo scrivere:

$$X^p - 1 \equiv (X-1) \cdot (X-2) \cdot \cdots \cdot (X-(p-1)) \pmod{p} \qquad (\blacktriangle)$$

da cui:

$$X^p - 1 - [(X-1) \cdot (X-2) \cdot \cdots \cdot (X-(p-1))] \equiv 0 \pmod{p}.$$

Il termine noto di tale polinomio

$$-1 - ((-1) \cdot (-2) \cdot (-3) \cdot \cdots \cdot (-(p-1))) = (-1) - (p-1)!$$

perché la congruenza sia verificata, deve essere divisibile per p e cioé:

$$(p-1)! \equiv -1 \pmod{p} \qquad \textbf{Teorema di Wilson}.$$

4.2 Il Teorema di Wolstenholme

Utilizzando quanto dimostrato poco sopra, dimostriamo i seguenti risultati:

Proposizione 22. *Sia p un primo dispari e per ogni l intero tra 1 e $p-1$ definiamo S_l come la somma di tutti i prodotti di l elementi tra $\{1, 2, \ldots, p-1\}$. Allora:*

$$S_l \equiv 0 \pmod{p}.$$

Dimostrazione. Scriviamo:

$$(X-1)\cdot(X-2)\cdot\cdots\cdot(X-(p-1)) = X^{p-1} - S_1X^{p-2} + \cdots + S_{p-1} \quad (*)$$

Abbiamo appena visto che $S_{p-1} = (p-1)!$.
Per la (▲) otteniamo che $p \mid S_k$ con $1 \leqslant k \leqslant p-2$. □

Teorema 23. (Teorema di Wolstenholme) *Sia p un primo maggiore di 3. Allora*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2}$$

dove con $\frac{1}{i}$ si intende l'inverso aritmetico di i $\pmod{p^2}$.

Dimostrazione. Calcoliamo la $(*)$ per X uguale a p ed otteniamo in questo modo

$$(p-1)! = p^{p-1} - S_1p^{p-2} + \cdots - S_{p-2}p + S_{p-1}$$

cioè:

$$p^{p-2} - S_1p^{p-3} + \cdots - S_{p-2} = 0$$

Per la Proposizione 22 si ottiene che $S_{p-2} \equiv 0 \pmod{p^2}$. Infatti, risulta che $S_{p-2} = \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}\right)$ dove con $\frac{1}{i}$ si intende l'inverso aritmetico di i $\pmod{p^2}$. Manualmente infatti si osserva che

$$i\left(\frac{1}{i} + \frac{1}{p-i}\right) = i\cdot\frac{1}{i} - \frac{i}{(p-i)} \equiv 1 - 1 = 0 \pmod{p^2}$$

e quindi $S_{p-2} \equiv 0 \pmod{p^2}$. □

4.3 Il software *Mathematica* e le congruenze polinomiali

4.3.1 Il polinomio derivato

Nel corso del paragrafo della prima parte a cui facciamo riferimento abbiamo parlato del polinomio derivato (Definizione 4.3). Per calcolarlo basta definire la seguente funzione:

```
derivato[f_]:= D[f, Variables[f][[1]]];
```

ottenendo così:

```
f:=x^4 + 4 x + 3;
derivato[f]
```

$4 + 4\,x^3$

La definizione di tale polinomio ci occorre per la risoluzione delle **Congruenze polinomiali**.

4.3.2 Le congruenze polinomiali

Nel software è già inserita una funzione che ci restituisce in casi "ragionevoli" le soluzioni di congruenze del tipo

$$f(X) \equiv 0 \pmod{n}$$

Solve[xˆ3+3 xˆ4 ==0 && Modulus==20, x]

{{Modulus→ 20, x→ 0}, {Modulus→ 20, x→ 5}, {Modulus→ 20, x→ 8}, {Modulus→ 20, x→ 10}, {Modulus→ 20, x→ 13}, { Modulus→ 20, x→ 18}}

Tale funzione non utilizza, peró, l'algoritmo "p-adico" descritto nella prima parte del testo.

Descriviamo quindi una funzione che utilizzi il metodo descritto nella prima parte. Si tratta di una funzione ricorsiva visto che la soluzione per $f(X) \equiv 0 \pmod{p^e}$ è calcolata a partire dalla soluzione di $f(X) \equiv 0 \pmod{p^{e-1}}$.
Come tutte le funzioni ricorsive, ha bisogno quindi di un passo base. Abbiamo così definito la funzione **congruPoli[f(x), p]** 4.3.4.3 che restituisce (per tentativi) le soluzioni dell'equazione $f(X) \equiv 0 \pmod{p}$.

congruPoli[xˆ3 - 2, 5]

{3}

congruPoli[xˆ2 + x + 7, 5]

La congruenza non ha soluzioni

A questo punto non ci resta che parlare della funzione **congruenzaPolinomiale[f(X), p, e]** 4.3.4.1. Abbiamo detto che è stata definita in modo ricorsivo (cioè le soluzioni per $e > 1$ sono calcolate a partire dalle soluzioni per $e - 1$).

congruenzaPolinomiale[xˆ2 + x + 7, 3, 2]

Il polinomio che stiamo studiando è: $x^2 + x + 7$
Le soluzioni sono:
{1, 4, 7}

Verifichiamo che nel caso $e = 1$ la funzione sia ben definita.

congruenzaPolinomiale[1+ 3x+ 2xˆ2+ 4xˆ4+ 2xˆ6+ xˆ7, 5, 1]

Il polinomio che stiamo studiando è: $1+ 3x+ 2x^2+ 4x^4+ 2x^6+ x^7$
Le soluzioni sono:
{2, 4}

Abbiamo già detto che *Mathematica* ha già una funzione built-in per la

risoluzione di tali congruenze. Paragoniamo il tempo che le due funzioni impiegano per risolvere i seguenti problemi:

Solve[xˆ10- 1==0 && Modulus==25, x]//Timing

{0. Second, {{Modulus→25, x→1}, {Modulus→25, x→4},
{Modulus→25, x→64}, {Modulus→25, x→9}, {Modulus→25, x→11},
{Modulus→25, x→14}, {Modulus→25, x→16}, {Modulus→25, x→19},
{Modulus→25, x→21}, {Modulus→25, x→24}}}

congruenzaPolinomiale[xˆ10- 1, 5,2]//Timing

Il polinomio che stiamo studiando è: -1 $+x^{10}$
Le soluzioni sono:
{0.12 Second, {1, 4, 6, 9, 11, 14, 16, 19, 21, 24}}

La differenza di tempo è dovuta al fatto che mentre la prima è una funzione built-in e quindi lavora con le funzioni base, la nostra è definita a partire da altre funzioni built-in e si basa anche sulla funzione **congruPoli[f(X), p]** che calcola le soluzioni in modo non efficiente effettuando molti *passaggi elementari*.

4.3.3 Il Teorema di Lagrange

Nella prima parte abbiamo enunciato il Teorema di Lagrange (Teorema 4.18).
Per poterne parlare in modo più approfondito dobbiamo sfruttare una funzione definita nel libro di Al Hibbard e Ken Levasseur *Exploring Abstract Algebra with Mathematica* (EAAM) edito da Springer Verlag, a cui è allegato un pacchetto di funzioni. Per richiamarla basta digitare:

```
Needs["AbstractAlgebra‘Master‘"]
SwitchStructureTo[Ring]
```

così che il computer riconosca la funzione **Poly[R, opzioni]** che ci viene spiegata digitando semplicemente:

```
?Poly
```

"Poly[R, expr, opts] creates the polynomial over the Ringoid R given by expr and using the options given by opts. A polynomial such as 2 + 3x + xˆ3 (over some ring R) can be constructed by Poly[R, 2 + 3x + xˆ3], which, by default, would return 2 + 3x + xˆ3. The form xˆ3 + 3x + 2 could be returned by entering Poly[R, 2 + 3x + xˆ3, PowersIncrease → RightToLeft], or by changing this option globally. One can also specify a polynomial by just using the coefficients. Thus, Poly[R, 1, 0, 3, 2] returns 1 + 3xˆ2 + 2xˆ3, while Poly[R, 2, 3, 0, 1, PowersIncrease → RightToLeft] returns 2xˆ3 + 3xˆ2 + 1. When entering just the coefficients, the default indeterminate is 'x', but this can

be changed by using the option Indeterminate → var, where var is any (valueless) symbol. FlexibleEntering, an option taking either True or False (defaulting to True), can be used if one wishes to enter polynomials allowing subtraction of terms or allowing entering the negation of an element by using -r. It also allows all coefficients of the polynomial to be reduced mod n if the base ring is Z[n]. If RP is a ring of polynomials, Poly[RP, expr, opts] works in a similar fashion."

Noi la useremo nel seguente modo: **Poly[R, coef, coef, ... , coef]** così da creare una serie casuale di polinomi di grado 7 utilizzando la funzione **Random[Integer, {0, 4}]** che restituisce in modo del tutto casuale un valore intero (Integer) tra 0 e 4. Visto che si vogliono tutti polinomi di pari grado, la funzione del settimo coefficiente sceglie un intero tra 1 e 4.

```
l=Table[Poly[Z[5], Random[Integer, {0, 4}],
Random[Integer, {0, 4}], Random[Integer, {0, 4}],
Random[Integer, {0, 4}], Random[Integer, {0, 4}],
Random[Integer, {0, 4}], Random[Integer, {0, 4}],
Random[Integer, {1, 4}]], {i, 1, 11}]
```

$\{1 + 3x + 2x^2 + 4x^4 + 2x^6 + x^7,$
$5 + 2x + 3x^2 + x^3 + 2x^5 + 4x^6 + 2x^7,$
$x^2 + 2x^4 + 3x^6 + 4x^7,$
$4 + 3x + 3x^3 + 2x^6 + 4x^7,$
$5x + 2x^2 + x^3 + 3x^4 + 5x^5 + x^6 + 4x^7,$
$3 + 3x^3 + 3x^4 + 2x^5 + 3x^6 + 3x^7,$
$5x + x^2 + 2x^3 + x^4 + 5x^5 + 4x^6 + 2x^7,$
$1 + 5x + x^2 + 4x^3 + x^4 + 3x^6 + 2x^7,$
$3x + x^2 + x^4 + 5x^6 + 4x^7,$
$5 + 2x + 2x^2 + 2x^3 + 2x^4 + 5x^5 + 2x^6 + 2x^7,$
$1 + 5\,x + 2x^3 + x^4 + 2x^5 + 4x^7\}$[16]

Calcoliamo ora il numero di soluzioni che tali polinomi risultano nelle congruenze (mod 5).

```
s=Table[Length[congruPoli[l[[i]], 5], {i, 11}]
```

{2, 3, 3, 1, 3, 1, 2, 2, 2, 2, 2}

Visualizziamo con un grafico la validità del Teorema di Lagrange tracciando con una linea blu il grado dei polinomi che studiamo mentre in rosso il numero delle soluzioni.

```
P1=Plot[7, {x, 0, 10},
PlotStyle→RGBColor[0, 0, 0.996109]];
```

[16] I risultati che abbiamo riportato si riferiscono ad una delle prove effettuate. Qualora infatti si calcolasse il file, è quasi impossibile che si ottengano gli stessi risultati.

```
P2=ListPlot[s, PlotStyle→ {PointSize[0.02],
RGBColor[0.95314, 0.156252, 0.0429694]}];
Show[P1, P2];
```

Infine, sempre con un grafico, verifichiamo come questo non valga nel caso in cui il modulo non sia primo rifacendoci ad un esempio che abbiamo anche descritto nella prima parte.
Per fare ciò utilizziamo sempre la funzione **Random[Integer, {min, max}]** creando 11 polinomi di secondo grado con coefficienti variabili tra 0 e 7.

```
s=Table[Length[ congPoli[Random[Integer, {0, 7}] +
Random[Integer, {1, 7}] x^2 , 2, 3]], {i, 11}]
```

```
{4, 0, 0, 8, 0, 4, 0, 8, 4, 0, 8}
```

Graficamente:

```
P1=Plot[2, {x, 0, 11},
PlotStyle→RGBColor[0.95314, 0.156252, 0.0429694]];
P2=ListPlot[s, PlotStyle→ {PointSize[0.02],
RGBColor[0, 0, 0.996109]}];
Show[P1, P2];
```

4.3.4 Funzioni utilizzate

♦ **4.3.4.1.** La funzione **congruenzaPolinomiale[f(x), p, e]** calcola le soluzioni della congruenza $f(x) \equiv 0 \pmod{p^e}$ riscrivendo come informazione il polinomio $f(X)$ e calcolando la soluzione tramite la funzione **congPoli[f, p, e]** 4.3.4.2.

```
Clear[congruenzaPolinomiale];

congruenzaPolinomiale[f_, p_, e_]:=
  Module[{solu},
    solu={};
    Print["Il polinomio che stiamo studiando e': ", f];
    Print["Le soluzioni sono:"];
    Return[congPoli[f, p, e]]];
```

♦ **4.3.4.2.** La funzione **congPoli[f, p, e]** a seconda del valore di e determina la funzione da utilizzare:
e = 1 → utilizza la funzione **congruPoli[f, p]** 4.3.4.3;
e > 1 → utilizza la funzione **poliCongru[f, p, e]** 4.3.4.4.
Non restituisce output.

```
congPoli[f_, p_, e_]:=
     If[e==1,
        congruPoli[f, p],
        poliCongru[f, p, e]];
```

♦ **4.3.4.3.** La funzione **congruPoli[f, p]** calcola il valore della congruenza polinomiale $f(x) \equiv 0 \pmod{p}$. Qualora non esistessero soluzioni restituisce la scritta **La congruenza non ha soluzioni**.

```
congruPoli[f_, p_]:=
  Module[{solu}, solu={};
    l=Table[Mod[calcolo[f, i], p], {i, 1, p}];
    appoggio={};
    For[j=0, j<p, j++;
      If[l[[j]]==0, AppendTo[solu, j],
        AppendTo[appoggio, j]]];
    If[solu=={},
      Return["La congruenza non ha soluzioni"],
      Return[solu]]];
```

♦ **4.3.4.4.** La funzione **poliCongru[f, p, e]** calcola la soluzione per $f(x) \equiv 0 \pmod{p^e}$ con $e > 1$ partendo dalle soluzioni di $f(x) \equiv 0 \pmod{p^{e-1}}$ come descritto nell'algoritmo nella parte precedente. Per fare questo utilizza la funzioni **calcolo[f, a]** 4.3.4.5 per calcolare il valore del polinomio derivato e del polinomio f nelle soluzioni per $e - 1$. A questo punto, a seconda delle varie possibilità: calcola direttamente la soluzione, utilizza la funzione **casoDue** 4.3.4.6 oppure scrive **Non ci sono soluzioni**.

```
poliCongru[f_, p_, e_]:=
    Module[{solu},
```

```
solu={};
g:=D[f, Variables[f][[1]]];
b=congPoli[f, p, e-1];
a=Mod[calcolo[g, b], p];
c=Mod[calcolo[f, b], p^e];
k=1;
While[k<Length[b]+1,
   If[a[[k]]==0,
      If[c[[k]]==0,
         solu=casoDue[f, p, e],
        {solu=solu,
         Print["Non ci sono soluzioni"]}],
      {s=Mod[congPoli[f, p, e-1][[k]] -
            calcolo[f, b][[k]] *
                calcolo[g, b][[k]]^(p-2), p^e],
   solu=Union[solu, s]};
   k++];
 Return[solu]];
```

♦ **4.3.4.5.** La funzione **calcolo[f(x), a]** calcola il valore del polinomio $f(x)$ per $x = a$. È stata definita per permettere di inserire nella funzione **congruenzaPolinomiale[f(x), p, e]** 4.3.4.1 un polinomio definito in qualsiasi modo.

```
Clear[calcolo];

calcolo[m_, v_]:=
  Module[{valore}, valore=0;
    coef=CoefficientList[m,
        Variables[m][[1]]];
    l=Length[coef];
    s=Table[valore=valore +coef[[i]]*v^(i-1),
         {i, 1, l}];
    Return[s[[l]]]];
```

calcolo[x^3+4, 5]

129

Qualora si inserisse un polinomio con più variabili, la funzione considererebbe solo la prima secondo il seguente ordine: {x, y, z, ... }

calcolo[z^2+ 4 x y - 1, 6]
calcolo[z^2+ 4 y - 1, 6]

-1 + 24 y + z^2
23 + z^2

♦ **4.3.4.6.** La funzione **casoDue[f(x), p, e]** calcola le soluzioni della congruenza $f(x) \equiv 0 \pmod{p^e}$ utilizzando la formula descritta nell'algoritmo

nel caso in cui $f'(y) \equiv 0 \pmod{p}$ e $f(y) \equiv 0 \pmod{p^e}$. Viene utilizzata dalla funzione **poliCongru[f, p, e]** 4.3.4.4 e utilizza il risultato che si ottiene con **poliCongru[f, p, e-1]** .

```
Clear[casoDue];

casoDue[f_, p_, e_]:=
  Module[{soluzioni},
    soluzioni={};
    s=Table[Mod[congPoli[f, p, e-1]+ t*(p^(e-1)), p^e],
      {t, 1, p}];
    i=1;
    While[i<Length[s]+1,
        {sol=s[[i]],
        soluzioni=Union[ soluzioni,sol]};
        i++];
  Return[soluzioni]];
```

5 Radici primitive dell'unità e congruenze del tipo $\mathbf{X}^m \equiv \mathbf{a} \pmod{n}$

5.1 Dimostrazione del Teorema di Gauss sull'esistenza delle radici primitive

Per prima cosa enunciamo un Lemma che ci servirà nella dimostrazione.

Lemma 24. *Per ogni* $n \in \mathbb{N}$

$$\sum_{d|n} \varphi(d) = n.$$

Dimostrazione. Supponiamo che $n = \prod_{p \text{ primo}} p^e$. Se $d \mid n$ allora si avrà che $d = \prod_{p \text{ primo}} p^{e'}$ con $0 \leqslant e' \leqslant e \quad \forall p$. Scriviamo:

$$\varphi(n) = \sum_{d|n} \varphi(d) = \sum_{p,\, e'} \prod \varphi(p^e) = \prod_p \{1 + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^e)\}.$$

Applicando le proprietà di φ scriviamo

$$\begin{aligned} \varphi(n) &= \prod_p \{1 + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^e)\} \\ &= \prod_p \{1 + p - 1 + p(p-1) + \cdots + p^{e-1}(p-1)\} \\ &= \prod_p p^e = n. \qquad \square \end{aligned}$$

Riprendiamo il teorema:

Teorema 25. (Gauss, 1801). *Sia n un intero positivo. Esiste una radice primitiva* $\pmod{n}$ *se, e soltanto se, n è uno dei seguenti interi:*

$$2, 4, p^k, 2p^k$$

con $k \geqslant 1$ e p primo dispari.

Dimostrazione. Mostriamo innanzitutto che gli interi elencati ammettono radice primitiva.
Per $2, 4$ si verifica con un semplice calcolo.
Consideriamo dapprima il caso $m = p$ con p primo dispari fissato. Vogliamo verificare che esista almeno un intero g tale che $\mathrm{ord}_p(g) = \varphi(p) = p - 1$. Possiamo limitarci a cercare tale elemento nell'insieme $\{1, 2, \ldots, p-1\}$.
Sia dunque $b \in \{1, 2, \ldots, p-1\}$ con $\mathrm{ord}_p(b) = d$ dove necessariamente $d \mid p-1$ (cfr. Proposizione 5.4(2)). Verifichiamo che $b = p - 1$ per almeno una scelta di b.

Per ogni d fissato tale che $d \mid p-1$ indichiamo con $\eta(d)$ il numero degli elementi $b \in \{1, 2, \ldots, p-1\}$ con $\mathrm{ord}_p(b) = d$. Visto che $b^d \equiv 1 \pmod{p}$ abbiamo che:

$$(b^2)^d \equiv 1 \pmod{p},\ \ldots,\ (b^{d-1})^d \equiv 1 \pmod{p},\ (b^d)^d \equiv 1 \pmod{p}.$$

Quindi il polinomio $X^d \equiv 1 \pmod{p}$ di grado d ha precisamente d soluzioni: $\{1, b, b^2, \ldots, b^{d-1}\}$.
Possiamo quindi concludere (Proposizione 5.4(3)) che $\eta(d) = \varphi(d)$.
Riassumendo:
(i) preso comunque d tale che $d \mid \varphi(p) = p-1$, allora $\eta(d) = 0$ oppure $\eta(d) = \varphi(d)$;
(ii) $\sum_{d|p-1} \varphi(d) \geqslant \sum_{d|p-1} \eta(d) = \varphi(p)$.
Per il Lemma 24 otteniamo che $\eta(d) = \varphi(d)$ con $d \mid \varphi(p) = p-1$.
Nel nostro caso abbiamo che $d = p-1$ e quindi $\eta(p-1) = \varphi(p-1) > 0$, cioè c'è almeno un elemento g tale che $1 \leqslant g \leqslant p-1$ e con $\mathrm{ord}_p(g) = p-1$.

Ora che abbiamo dimostrato che per ogni p primo dispari c'è almeno una radice primitiva, possiamo dimostrare che anche p^k ha almeno una radice primitiva per ogni $k \geqslant 1$.
Precisamente dimostreremo che se g è una radice primitiva di p allora esiste x tale che $g' = g + px$ risulta essere radice primitiva di p^k.
Dato che $g^{p-1} \equiv 1 \pmod{p}$, possiamo scrivere $g^{p-1} = 1 + py$ per qualche y.
Quindi:

$$\begin{aligned}(g')^{p-1} &= (g+px)^{p-1} \\ &= g^{p-1} + \binom{p-1}{1} g^{p-2} px + p^2 \sum_{j=2}^{p-1} \binom{p-1}{j} g^{p-j-1} p^{j-2} x^j \\ &= 1 + py + p(p-1) g^{p-2} x + p^2 \sum_{j=2}^{p-1} \binom{p-1}{j} g^{p-j-1} p^{j-2} x^j\end{aligned}$$

così da poter definire $z \in \mathbb{Z}$ tale che $(g')^{p-1} = 1 + pz$ e che verifichi la condizione $z \equiv y + (p-1) g^{p-2} x \pmod{p}$.
La congruenza lineare in x $(p-1) g^{p-2} x \equiv z - y \pmod{p}$ è risolubile comunque preso z. Se prendiamo dunque z relativamente primo con p abbiamo che g' è una radice primitiva per $p^k, k \geqslant 1$.
Ma z si può prendere in questo modo visto che:

$$\varphi(p) = p-1 = \mathrm{ord}_p(g') \mid \mathrm{ord}_{p^k}(g') \mid p^{k-1}(p-1)$$

(visto che g' è una radice primitiva per p). Se scriviamo $\mathrm{ord}_{p^k}(g') = p^e(p-1)$, con $e \leqslant k-1$, allora $(g')^{\mathrm{ord}_{p^k}(g')} = ((g')^{p-1})^p = (1+pz)^p = 1 + p^{e+1} z_e$, esiste z_e relativamente primo con p. Visto che $p^{e+1} \mid ((g')^{\mathrm{ord}_{p^k}(g')} - 1)$ mentre $p^k \mid ((g')^{\mathrm{ord}_{p^k}(g')} - 1)$ così che $k \leqslant e+1$ e quindi $e = k-1$ come volevamo

dimostrare.

Avendo quindi dimostrato che per ogni intero k e ogni primo p dispari esiste una radice primitiva g' di p^k, è semplice dimostrare l'esistenza di una radice primitiva per interi del tipo $2p^k$.

Per concludere dimostriamo che nessun numero del tipo 2^e oppure p_1p_2 con $e \geqslant 3$ e $\text{MCD}(p_1, p_2) = 1$ ammette radici primitive.
Prendendo b dispari, si verifica, per induzione su $e > 2$, che $b^{2^{e-2}} \equiv 1 \pmod{2^e}$. (Per la base dell'induzione, $e = 3$ si veda la soluzione dell'Esercizio 1.3 a pag. 113).
Quindi 2^e non ammette radici primitive. Per $n = p_1p_2$, consideriamo $b^{\frac{\varphi(n)}{2}} = (b^{\varphi(p_1)})^{\frac{\varphi(p_2)}{2}} \equiv 1 \pmod{p_1}$ e anche $b^{\frac{\varphi(n)}{2}} = (b^{\varphi(p_2)})^{\frac{\varphi(p_1)}{2}} \equiv 1 \pmod{p_2}$ cioè $b^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{n}$. □

5.2 Il software *Mathematica* , radici primitive, ordine ed indice

5.2.1 L'ordine di un elemento

La funzione per calcolare l'ordine di un elemento $a \pmod{n}$ **ordine[a, n]** 5.2.5.1 è stata da noi definita in modo tale che se $\text{MCD}(a, n) \neq 1$ restituisca il valore 0.

ordine[2, 7]

3

ordine[3, 6]

0

Verifichiamo ora il risultato descritto nella Proposizione 5.3 tramite la funzione **test1[n]** 5.2.5.7. (La possibilità che appaia la stringa **Errore** è nulla visto che abbiamo dimostrato la validità della proposizione.)
Si osservi che, anche una volta assegnato il valore ad n, l'output può variare visto che a è scelto in modo casuale.

test1[21]

Abbiamo n = 21
Prendiamo a = 25
Prendiamo b = 4
ord_n a = 3
ord_n b = 3
Il risultato è quindi verificato

Per rendere più generale il test, si potrebbe calcolare il seguente input:
test1[Random[Integer, 2, 1000]]

ma vista la casualità con cui vengono scelti i valori si rischia di impegnare il computer per tempi lunghi. Per dare un'idea del risultato abbiamo ristretto il numero delle possibilità ottenendo:

test1[Random[Integer, 2, 50]][17]

Abbiamo n = 45
Prendiamo a = 52
Prendiamo b = 7
ord_n a = 12
ord_n b = 12
Il risultato è quindi verificato

5.2.2 La radice primitiva

Abbiamo definito una funzione **radicePrimitiva[n]** 5.2.5.2 che restituisce gli elementi del Sistema Completo di Residui che risultano essere radici primitive. Per il particolare criterio che abbiamo usato (vedere descrizione della funzione) l'output ci riporta le radici primitive in ordine crescente.

radicePrimitiva[7]

{3, 5}

Come dimostrato da Gauss (Teorema 5.17) abbiamo che:

radicePrimitiva[8]

Non sono state trovate radici primitive
{ }

Abbiamo enunciato il Teorema 5.10, testiamolo, verifichiamo cioè la relazione che intercorre tra il numero di radici primitive modulo p e il valore $\varphi(p-1)$.
Per fare ciò si è creata la funzione **verificateorema1[n]** 5.2.5.3.

verificateorema1[30]

I valori per cui si è verifcato il teorema sono: {3, 5, 7, 11, 13, 17, 19, 23, 29}
Le rispettive radici primitive risultano: {{2}, {2, 3}, {3, 5}, {2, 6, 7, 8}, {2, 6, 7, 11}, {3, 5, 6, 7, 10, 11, 12, 14}, {2, 3, 10, 13, 14, 15}, {5, 7, 10, 11, 14, 15, 17, 19, 20, 21}, {2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27}}
per un numero di: {1, 2, 2, 4, 4, 8, 6, 10, 12}
mentre $\varphi(n-1)$ ha valori: {1, 2, 2, 4, 4, 8, 6, 10, 12}

[17] Si fa presente che data la casualità della scelta, inserendo lo stesso input, si possono ottenere risultati diversi.

A questo punto, utilizzando l'algoritmo descritto da Gauss calcoliamo la radice primitiva **primitivaGauss[n]** 5.2.5.4 ma come abbiamo già osservato, tale algoritmo non ci permette in generale di determinare la radice minima. Confrontiamo il risultato ottenuto con tale funzione con quello che ci restituisce l'elenco delle radici primitive 5.2.5.2.

primitivaGauss[43]//Timing

{0.07 Second, 30}

radicePrimitiva[43]//Timing

{0.13 Second, {3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34}}

primitivaGauss[97]//Timing

{0.02 Second, 38}

radicePrimitiva[97]//Timing

{0.511 Second, {5, 7, 10, 13, 14, 15, 17, 21, 23, 26, 29, 37, 38, 39, 40, 41, 56, 57, 58, 59, 60, 68, 71, 74, 76, 80, 82, 83, 84, 87, 90, 92}}

primitivaGauss[51]//Timing

{0. Second, primitivaGauss[51]}[18]

radicePrimitiva[51]//Timing

Non sono state trovate radici primitive
{ 0.055 Second, { }}

5.2.3 L'indice di un elemento

Per calcolare l'indice di un elemento (cfr. 5.2.5.8) ci occorre dare in input l'elemento, una radice primitiva e il modulo secondo il quale si vuole calcolare l'indice.

indice[4, 2, 13]

2

indice[1, 3, 13]

Input sbagliato, il secondo elemento non è una radice primitiva.
Riprovare scegliendo tra i seguenti elementi: {2, 6, 7, 11}
∞

[18] Si ricordi che l'algoritmo è definito solo per interi primi.

Verifichiamo alcune proprietà che abbiamo dimostrato nella Proposizione 5.22.

$$\mathrm{ind}_r(r) = 1$$

indice[5, 5, 9]

1

Esaminiamo la relazione

$$\mathrm{ind}_r(1) = \varphi(n)$$

Calcoliamo da p prima le radici primitive per $n = 169 = 13^2$

radicePrimitiva[169]

{2, 6, 7, 11, 15, 20, 24, 28, 32, 33, 37, 41, 45, 46, 50, 54, 58, 59, 63, 67, 71, 72, 76, 84, 85, 93, 97, 98, 102, 106, 110, 111, 115, 119, 123, 124, 128, 132, 136, 137, 141, 145, 149, 154, 158, 162, 163, 167}

A questo punto scegliamo una radice primitiva (ad esempio 102) e calcoliamo

indice[1, 102, 169]
EulerPhi[169]

156
156

Verifichiamo ora la proprietà dell'inverso.
Per calcolare l'inverso di $a \pmod p$ utilizziamo la funzione **Inverse[{{a}}, Modulus→p][[1, 1]]**. Visto che la funzione di base è definita per matrici, bisogna inserire l'opzione [[1, 1]] per non ottenere come output una matrice 1×1 ma un numero.
Oltre alla differenza concettuale appena descritta, c'è anche una differenza di output grafica:

Inverse[{{17}}, Modulus→23]

{{19}}

Inverse[{{17}}, Modulus→23][[1, 1]]

19

In più, senza questo accorgimento, nel calcolo generale si otterebbe un errore

indice[Inverse[{{17}}, Modulus→23], 7, 23]

∞

Verifichiamo che:

$$\text{ind}_r(a^*) \equiv -\text{ind}_r(a) \pmod{\varphi(n)}$$

indice[Inverse[{{17}}, Modulus→23][[1, 1]], 7, 23]

17

indice[17, 7, 23]

5

Mod[-5, 22]

17

5.2.4 Soluzione di $\mathbf{X^m \equiv a} \pmod{\mathbf{n}}$

Per finire studiamo la soluzione di congruenze del tipo: $X^m \equiv a \pmod{n}$. Per fare ciò utilizziamo la funzione built-in **Solve[f(X) == 0 && Modulus == n, X]** che abbiamo descritto nel paragrafo precedente.
Si è fatta questa scelta per motivi di praticità, visto la velocità già testata della funzione.

Scriviamo ora un comando che ci restituisca per i vari valori di a, le varie soluzioni di $X^4 \equiv a \pmod{13}$ limitandoci a studiare i casi $1 \leqslant a \leqslant 12$

```
Table[{Print["Per a= ", a],
Print["Le soluzioni sono: ",
Solve[xˆ4-a ==0 && Modulus==13, x]]},
{a, 1, 12}];
```

Per a = 1
Le soluzioni sono: {{Modulus→13, x→1}, { Modulus→13, x→5},
{Modulus→13, x→8}, { Modulus→13, x→12}}
Per a = 2
Le soluzioni sono: { }
Per a = 3
Le soluzioni sono: {{Modulus→13, x→2}, { Modulus→13, x→3},
{Modulus→13, x→10}, { Modulus→13, x→11}}
Per a = 4
Le soluzioni sono: { }
Per a = 5
Le soluzioni sono: { }
Per a = 6
Le soluzioni sono: { }
Per a = 7
Le soluzioni sono: { }

Per a = 8
Le soluzioni sono: { }
Per a = 9
Le soluzioni sono: {{Modulus→13, x→4}, { Modulus→13, x→6},
{Modulus→13, x→7}, { Modulus→13, x→9}}
Per a = 10
Le soluzioni sono: { }
Per a = 11
Le soluzioni sono: { }
Per a = 12
Le soluzioni sono: { }

Studiamo le varie soluzioni di $8X^5 \equiv a \pmod 7$ limitandoci, ovviamente, a studiare i casi $1 \leqslant a \leqslant 6$

Table[{Print["Per a= ", a],
Print["Le soluzioni sono: ",
Solve[8 xˆ5-a ==0 && Modulus==7, x]]},
{a, 1, 6}];

Per a = 1
Le soluzioni sono: {{Modulus→7, x→1}}
Per a = 2
Le soluzioni sono: {{Modulus→7, x→4}}
Per a = 3
Le soluzioni sono: {{Modulus→7, x→5}}
Per a = 4
Le soluzioni sono: {{Modulus→7, x→2}}
Per a = 5
Le soluzioni sono: {{Modulus→7, x→3}}
Per a = 6
Le soluzioni sono: {{Modulus→7, x→0}}

Per concludere utilizziamo la funzione **soluzioni[coefficiente, esponente, modulo]** 5.2.5.9 che ci restituisce solamente i valori di a per cui ci siano soluzioni per la congruenza

$$\text{coefficiente} \cdot X^{\text{esponente}} \equiv \text{a} \pmod{\text{modulo}}.$$

Consideriamo ad esempio:

$$8X^5 \equiv a \pmod{17}$$

soluzioni[8, 5, 17]

La congruenza ha soluzione per i seguenti valori di a:
{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16}

$$2X^7 \equiv a \pmod 9$$

soluzioni[2, 7, 9]

La congruenza ha soluzione per i seguenti valori di a:
{1, 2, 4, 5, 7, 8}

5.2.5 Funzioni utilizzate

♦ **5.2.5.1.** La funzione **ordine[a, n]** calcola l'ordine dell'elemento a restituendo 0 qualora l'ordine non fosse definito, cioè se $\text{MCD}(a, n) \neq 1$.

```
Clear[ordine];

ordine[a_, n_]:=
  Module[{ordine},
   ordine=0;
   If[GCD[a, n]!=1,
      Return[0]];
   k=1;
   While[Mod[a^k, n]!= 1, a; k++];
   ordine=k;
   Return[ordine]];
```

♦ **5.2.5.2.** La funzione **radicePrimitiva[n]** restituisce l'elenco di tutti gli elementi appartenenti al Sistema Completo di Residui che risultano essere radici primitive prendendoli in considerazione a partire dal più piccolo e scorrendoli tutti calcolandone l'ordine. Qualora nessuno soddisfacesse la condizione richiesta, avremmo come output la stringa **Non sono sono state trovate radici primitive** ed il valore { }.

```
Clear[radicePrimitiva];

radicePrimitiva[n_]:=
  Module[{radice},
    radice={};
    b=EulerPhi[n];
    For[i=1, i<n, i++;
     If[ordine[i, n]==b,
        radice=Append[radice, i], i]];
    If[radice == {},
     Print["Non sono sono state
        trovate radici primitive"]];
    Return[radice]];
```

♦ **5.2.5.3.** La funzione **verificateorema1[n]** restituisce i seguenti output:
- i valori minori di n che hanno radici primitive;
- le rispettive radici primitive;
- il numero delle varie radici primitive;
- il valore della funzione $\varphi(n-1)$ per i valori di n descritti all'inizio.

La funzione fa uso di altre due funzioni quali: **radicePrimitiva1[n]** che come unica differenza dalla precedente **radicePrimitiva[n]** ha che non appare la scritta *Non sono state trovate radici primitive* qualora queste non esistessero. Questo perché tale caratteristica avrebbe creato un output confuso con il ripetersi più volte della stringa.
Altra funzione che utilizza è **lunghezza[p]** che restituisce il numero di radici primitive modulo p.

```
Clear[radicePrimitiva1, verificateorema1, lunghezza];

radicePrimitiva1[n_]:=
  Module[{radice},
    radice={};
    b=EulerPhi[n];
    For[i=1, i<n, i++;
     If[ordine[i, n]==b,
        radice=Append[radice, i], i]];
    Return[radice]];

lunghezza[p_]:=Length[radicePrimitiva1[p]];

verificateorema1[p_]:=
  Module[{n, radice, cardinalita,eulero},
    n={3};
    s=3;
    radice={radicePrimitiva1[n[[1]]]};
    cardinalita={lunghezza[n[[1]]]};
    eulero=EulerPhi[n-1];
    finale={};
    For[j=4, j<p,
       {s=s+1 ,
       If[PrimeQ[s],
            {AppendTo[radice, radicePrimitiva1[s]],
            AppendTo[n, s],
            AppendTo[cardinalita, lunghezza[s]],
            AppendTo[eulero, EulerPhi[s-1]]}];
       j++];
    Print["I valori per cui si  verificato
         il teorema sono: ", n];
    Print["Le rispettive radici primitive
         risultano: ", radice];
    Print["per un numero di: ", cardinalita];
    Print["Mentre Eulero(n-1)
            ha valori: ", eulero]];
```

♦ **5.2.5.4.** La funzione **primitivaGauss[p]** calcola, applicando l'algoritmo di Gauss, una radici primitiva modulo p solo se p è primo. Questa selezione viene effettuata immediatamente al momento di leggere l'input.
Per lavorare la funzione utilizza altre due funzioni **passo3[d, t]** 5.2.5.5 e **scelta[lista, a, p]** 5.2.5.6.

È stato necessario l'utilizzo della funzione built-in **Break[n]** che interrompe qualsiasi ciclo restituendo il valore di n. In più si è fatto un controllo sui valori dati dalla funzione **passo3** in modo da assegnarvi lo stesso simbolo utilizzato nella descrizione dell'algoritmo.
Descriviamo alcuni accorgimenti presi:

- il valore di a è stato scelto nel seguente modo: data una *lista* degli elementi tra 2 e $p-1$ si è scelto a caso un numero i tra 1 e $p-2$ (che è appunto la lunghezza della *lista*) e si è assegnato ad a il valore che si trova al posto i;

- ogni volta che viene scelto dalla *lista* un valore, questo viene cancellato per evitare di riperere la stessa scelta più volte;

- per la scelta di b si è ricorso alla funzione **scelta[*lista*, a, p]**;

- per la scelta di t' e d', rispettivamente $t1$ e $d1$ nel programma, si è usata la funzione **passo3[d, t]**. Per assegnarne il valore corretto, si verifica che $\frac{d}{d'}$ sia intero altrimenti si invertono i valori.

```
Clear[primitivaGauss];

primitivaGauss[p_Integer?PrimeQ]:=
  Module[{a},
    lista=Delete[Range[p-1], 1];
    s=Length[lista];
    i=Random[Integer, {1, s}];
    a=lista[[i]];
    lista=Delete[lista, i];
    d=ordine[a, p];
    If[d==p-1,
       Return[a]];
    While[lista!={},
       {b=scelta[lista, a, p],
        t=ordine[b, p],
        If[t==p-1,
           Break[b],
           {d1=passo3[d,t][[1]],
           If[IntegerQ[d/d1],
              t1=passo3[d,t][[2]],
                {t1=passo3[d,t][[1]],
                d1=passo3[d,t][[2]]}],
              alpha=Mod[a^(d/d1), p],
              beta=Mod[b^(t/t1), p],
              a=Mod[alpha * beta, p],
              d=ordine[a, p],
              If[d1==p-1,
                 Break[a]]}]};
        lista=Delete[lista, Position[lista, b]]
     ]];
```

♦ **5.2.5.5.** La funzione **passo3[d, t]** come dice il nome, ci permette di effettuare i calcoli descritti nel Passo 3 dell'algoritmo di Gauss per la radice primitiva (cfr. pag. 65).
La funzione ha come scopo quello di calcolare d' e t' tali che $d' \cdot t' = \text{mcm}(d, t)$. Per effettuare ciò svolge il seguente ragionamento:
considera una *lista* dei divisori di $d_1 = \text{mcm}(d, t)$ togliendo il temine 1. Quindi, partendo selezionando il primo elemento (*elem*) scorre la lista cercando un elemento (*elem2*) che sia primo con *elem*. Se in più la coppia così creata soddisfa la condizione $elem \cdot elem2 = d_1$ finisce il calcolo restituendo tale coppia, altrimenti riconsidera la *lista* togliendo il primo elemento e ricomincia da capo.

```
Clear[passo3];

passo3[d_, t_]:=
  Module[{elem},
    elem2=1;
    d1=LCM[d, t];
    lista=Delete[Divisors[d1], 1];
    elem=lista[[1]];
    s=Length[lista];
    For[i=1, i<s, i++;
      If[GCD[elem, lista[[i]]]==1,
        elem2=lista[[i]]]];
    If[(elem * elem2) == d1,
       Return[{elem2, elem}]];
    lista=Delete[lista, 1];
    While[lista!={},
       {elem=lista[[1]],
       s=Length[lista],
       For[i=1, i<s, i++;
         If[GCD[elem, lista[[i]]]==1,
           elem2=lista[[i]]]],
         If[(elem * elem2) == d1,
           Break[{elem2, elem}]]};
       lista=Delete[lista, 1]];
    Return[{elem2, elem}]];
```

♦ **5.2.5.6.** La funzione **scelta[lista, a, p]** ci permette di scegliere b con $2 \leqslant b \leqslant p-1, b \not\equiv a^i$ per ogni $i, 1 \leqslant i \leqslant d$ nel seguente modo: prendiamo a caso un numero i compreso tra 1 e la lunghezza della *lista* data in input, consideriamo il valore al posto i e quindi controlliamo che tale valore non si trovi nella lista creata dai valori di a^i per ogni $i, 1 \leqslant i \leqslant d$. Se ciò non si verificasse allora si cancella il calore scelto dalla *lista* e si ricomincia.

```
Clear[scelta];

scelta[lista_, a_, p_]:=
  Module[{b},
    While[lista!={},
       {i=Random[Integer, {1, Length[lista]}];
```

```
      b=lista[[i]];
      d=ordine[a, p];
      test=Mod[Table[a^j, {j, 1, d}], p];
      prova=Position[test, b];
      If[prova=={},
         Break[b]]};
      lista=lista=Delete[lista, Position[lista, b]]];
```

♦ **5.2.5.7.** La funzione **test1[n]** sceglie a in modo casuale tra i valori $n+1$ ed $2n-1$, poi prende b tale che sia verificato $a \equiv b \pmod{n}$ e quindi calcola $\mathrm{ord}_n(a)$ e $\mathrm{ord}_n(b)$ restituendo la stringa **Il risultato è quindi verificato** se i due valori coincidono, altrimenti restituisce la stringa **Errore**.
La casualità con cui è scelto a e la richiesta che tale valore risulti primo con n possono determinare un tempo vario per il calcolo della funzione, soprattutto se n non è primo.
La funzione, per accellerare i tempi, è stata definita in modo tale che ad un primo passaggio scelga a tra i valori $n+1$ ed $2n-1$, ma se $\mathrm{MCD}(a,n) \neq 1$ allora si ripete la scelta di a ma questa volta tra i valori $n+1$ e $a-1$.

```
Clear[test1];

test1[n_] :=
   Module[{test},
      test = 0;
      Print["Abbiamo n = ",  n];
      a=Random[Integer, {n+1, 2n-1}];
      mcd=GCD[a, n];
      While[mcd != 1,
         a=Random[Integer, {n+1, a-1}]];
      Print["Prendiamo a = ", a];
      b = Mod[a, n];
      Print["Prendiamo b = ", b];
      t1 = ordine[a, n];
      t2 = ordine[b, n];
      Print["ord_(n)a = ", t1];
      Print["ord_(n)b = ", t2];
      If[t1 == t2,
        Print["Il risultato e' quindi verificato"],
        Print["Errore"]]];
```

♦ **5.2.5.8.** La funzione **indice[a, r, n]** calcola il valore di $\mathrm{ind}_r(a) \pmod{n}$. Qualora fosse verificato che $\mathrm{MCD}(a,n) \neq 1$ restituisce come output il valore ∞ e la stringa *Non si può calcolare l'indice perché a e n non sono primi tra loro.* Prima però di arrivare a questo controllo verifica che r sia una radice primitiva di n utilizzando la funzione **radicePrimitiva[n]** 5.2.5.2 nel seguente modo: crea la lista *radice* e verifica tramite la funzione **Position[*lista*, *elemento*]** che r sia compresa in tale lista. Qualora tale condizione non fosse verificata l'output risulterebbe essere il valore ∞ e la stringa *Input sbagliato, il secondo elemento non e' una radice primitiva. Riprovare scegliendo tra i seguenti elementi:* seguita dalla lista delle radici primitive.

```
Clear[indice];

indice[a_, r_,  n_]:=
  Module[{ind},
    ind=Infinity;
    radice=radicePrimitiva[n];
    s=Position[radice, r];
    If[s=={},
      {Print["Input sbagliato,
        il secondo elemento non e' una radice primitiva.\n
        Riprovare scegliendo tra i seguenti
        elementi: \t  ", radice] ,
       Return[ind]},
       {If[GCD[a, n]!=1,
           {Print["Non si puo' calcolare l'indice perche'
                  a e n non sono primi tra loro "],
            Return[ind]},
           {sist=Mod[Table[r^j, {j, 1, EulerPhi[n]}], n],
           h=Position[sist, a][[1, 1]],
           ind= h}]}];
     Return[ind]];
```

♦ **5.2.5.9.** La funzione **soluzioni[b, m, n]** restituisce la lista dei valori di a per cui esistano soluzioni alla congruenza $bX^m \equiv a \pmod{n}$.
Per fare ciò utilizza la funzione **Solve** come già detto.

```
Clear[soluzioni];

soluzioni[coef_, exp_, mod_]:=
  Module[{solu},
    solu={};
    non={};
    j=1;
    While[j<mod,
     If[Solve[(coef)x^(exp) - j == 0 && Modulus==mod, x]!={},
       solu=Append[solu, j],
       AppendTo[non, j]];
     j++];
    Print["La congruenza ha soluzione per i
         seguenti valori di a: "];
    Return[solu]];
```

6 Congruenze quadratiche e legge di reciprocità

6.1 Radice quadrata modulo un primo p

Analizziamo ora un'applicazione particolare dei Simboli di Legendre e Jacobi: il calcolo della radice quadrata modulo p primo.
Supponiamo che p sia un primo dispari. Supponiamo anche di aver determinato a tale che $\left(\frac{a}{p}\right) = 1$. Abbiamo quindi che esiste x tale che $x^2 \equiv a \pmod{p}$. Cerchiamo di determinare esplicitamente x.
Un calcolo brutale (che richiederebbe un tempo pari a $\mathcal{O}(p)$, cioè pari a circa p operazioni) è dato dal determinare tale x analizzando singolarmente tutti gli elementi dell'insieme $\{1, \ldots, p-1\}$ (cfr. pag. 219).
Riassumiamo qui di seguito i risultati che ci permetteranno di definire un algoritmo pratico e veloce.

Per la "metà" dei primi p, cioè per p tale che $p \equiv 3 \pmod{4}$, abbiamo che la soluzione è data da:

$$x = a^{\frac{p+1}{4}} \pmod{p},$$

visto che se a è un residuo quadratico allora $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ e quindi

$$x^2 \equiv a^{\frac{p+1}{2}} \equiv a \cdot a^{\frac{p-1}{2}} \equiv a \pmod{p}.$$

Per gli altri primi, il calcolo risulta più difficile.
Per i primi tali che $p \equiv 5 \pmod{8}$ dato che $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ si ha che

$$a^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}.$$

Nel caso di segno positivo

$$x = a^{\frac{p+3}{8}} \pmod{p}$$

sarà soluzione. Altrimenti, utilizzando il fatto che $p \equiv 5 \pmod{8}$ ed il Corollario 6.14 si ottiene che $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ con soluzione

$$x = 2a \cdot (4a)^{\frac{p-5}{8}} \pmod{p}.$$

Rimane quindi il caso $p \equiv 1 \pmod{8}$ che risulta essere il più complicato.

Prima di analizzare un'algoritmo che ci permetta di calcolare x comunque preso p diamo dei cenni su teorie che applicheremo.

6.1.1 Alcuni cenni sui sottogruppi di Sylow

Richiamiamo qui le definizioni di gruppo e sottogruppo di Sylow.

Definizione 26. Sia G un insieme con un'operazione binaria $\psi : G \times G \to G$ tale che valgano le seguenti proprietà:

1. presi comunque $a, b, c \in G$ allora

$$\psi(\psi(a,b),c) = \psi(a,\psi(b,c));$$

2. esiste un elemento, che indicheremo con $1 \in G$ tale che

$$\psi(1,a) = \psi(a,1) = a;$$

3. per ogni $a \in G$ esiste un elemento $\bar{a} \in G$ tale che

$$\psi(a,\bar{a}) = \psi(\bar{a},a) = 1.$$

La coppia (G,ψ) è detta *Gruppo.*

Definizione 27. Diremo *ordine* di un gruppo (G,ψ) la cardinalità dell'insieme G.

Definizione 28. Un insieme $I \subset G$ si dirà *sottogruppo* di G se:

A. presi comunque $a, b \in I$ allora $\psi(a,b) \in I$;

B. $1 \in I$;

C. per ogni $a \in I$ allora $\bar{a} \in I$.

Definizione 29. Sia G un gruppo finito con ordine $p^n m$ dove p è primo e $p \nmid m$. Diremo che P, sottogruppo di G, è un *p-sottogruppo di Sylow* se ha ordine p^n.

Enunciamo ora un teorema noto com Teorema di Sylow.

Teorema 30. *Dato G gruppo con ordine $p^n m$ dove p è primo e $p \nmid m$, esiste sempre un p-sottogruppo di Sylow.*

Per la dimostrazione [Ga].
Per concludere questi richiami diamo la seguente:

Definizione 31. Un gruppo (G,ψ) si dirà *ciclico* se esiste un elemento $g \in G$ tale che $G = \{g^i \ : \ i \in \mathbb{Z}\}$.
Si noti che, se G è ciclico con ordine finito uguale ad n, allora $G = \{g^i \ : \ 0 \leqslant i \leqslant n-1\}$.
L'elemento g viene detto quindi *generatore* del gruppo.

6.1.2 Algoritmo di Tonelli & Shanks

Per risolvere il problema si può far uso delle funzioni definite nel Paragrafo 4 (cfr. pag. 187).
Andando però al caso particolare Tonelli (1891) descrisse un algoritmo che successivamente fu reso più efficiente da Shanks (1972).
Si tratta di una generalizzazione dei casi precedentemente analizzati. Descriviamolo, per dettagli tecnici riguardandi la programmazione cfr. funzione 6.2.4.4.

Possiamo sempre scrivere $p-1 = 2^n \cdot q$ con n massimo e quindi q dispari (non necessariamente primo).
Per il Teorema 30 sappiamo che esiste I_n 2-sottogruppo di Sylow ciclico di ordine 2^n e con z indichiamo l'elemento generatore di I_n non residuo quadratico.
Sia a un residuo quadratico $\pmod p$, abbiamo:

$$a^{\frac{p-1}{2}} = (a^q)^{2^{n-1}} \equiv 1 \pmod p,$$

e ponendo $b = a^q \pmod p$ determiniamo una radice quadrata di a in I_n. Questo perché visto che I_n è ciclico, gli elementi che risultano essere radici di a devono avere ordine 2^{n-1}. Abbiamo quindi che esiste un intero pari k, $0 \leqslant k < 2^{n-1}$, tale che $bz^k = 1$ in I_n. Poniamo dunque

$$x = a^{\frac{q+1}{2}} z^{\frac{k}{2}},$$

ottenendo che $x^2 \equiv a \pmod p$.

L'algoritmo deve risolvere due problemi:
- trovare z generatore di I_n;
- calcolare l'esponente k.

La difficoltà si trova tutta nel primo problema anche se poi nella pratica è il più facile.

Il modo migliore per determinare il generatore z del sottogruppo I_n è quello di prendere a caso un intero m e di porre $z \equiv m^q \pmod p$.
Chiaramente risulta che z così definito è un generatore del sottogruppo I_n se, e soltanto se, m è un non residuo quadratico $\pmod p$.
La possibilità di scegliere m correttamente è di $\frac{p-1}{2p}$, in pratica molto alta.
Un esempio: la possibilità di scegliere un m sbagliato in venti prove è inferiore a 10^{-6}.

Per la determinazione dell'esponente k si procede per tentativi secondo il seguente criterio: Si procede nella ricerca fino a che

$$b^{2^m} = (a(a^{\frac{q-1}{2}})^2)^{2^m} \equiv 1 \pmod p$$

con $1 \leqslant m$.

6.2 Il software *Mathematica* , simbolo Jacobi e la LRQ

6.2.1 I residui quadratici e simbolo di Jacobi

Dato p primo, si crea l'insieme $\mathbb{Z}_p$ composto dagli elementi $\{0, 1, \ldots, p-1\}$ alcuni dei quali risultano quadrati modulo p, altri no.
Abbiamo visto che, se $p \geqslant 3$ esattamente metà degli interi non nulli di $\mathbb{Z}_p$ sono quadrati.
La ragione è evidente se si analizza la struttura della lista seguente che mostra che ogni quadrato ha esattamente due radici (quadrate): r e $p - r$.

PowerMod[Range[1, 18], 2, 19]

{1, 4, 9, 16, 6, 17, 11, 7, 5, 5, 7, 11, 17, 6, 16, 9, 4, 1}

Abbiamo qui usato le seguenti funzioni built-in:

Range[min, max] che genera la lista di interi {min, ..., max}. Visto che nel nostro input abbiamo min = 1, potevamo usare anche l'opzione **Range[max]** che restituisce la lista {1, ..., max}.

PowerMod[a, b, n] Che restituisce il valore $a^b \pmod n$.

Utilizzando il simbolo di Legendre sappiamo che se $(\frac{a}{p}) = 1$ allora a è un residuo quadratico. Ci sono due metodi per determinare se a è un residuo quadratico. Il criterio di Eulero afferma che se p è un primo dispari, e a è un intero positivo non multiplo di p, allora vale

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p.$$

Il criterio di Eulero si può programmare (**eulero[a, p]** cfr. 6.2.4.1) in modo efficiente perché **PowerMod** è veloce.

eulero[5, 17]

5 non è un residuo quadratico
-1

eulero[15, 16]

eulero[15, 16]

Esiste però un algoritmo ancora più veloce basato sulla legge della reciprocità quadratica, incorporato in *Mathematica* con il nome **JacobiSymbol[a, p]**.

eulero[5726, 13457]//Timing

5726 non è un residuo quadratico

{0.051 Second, -1}

JacobiSymbol[5726, 13457]//Timing

{0. Second, -1}

Analiziamo ora il seguente output:

JacobiSymbol[Range[18], 19]

{1, -1, -1, 1, 1, 1, 1, -1, 1, -1, 1, -1, -1, -1, -1, 1, 1, -1}

dove i valori positivi corrispondono ai quadrati, come si verifica confrontando la lista dei quadrati generata da **PowerMod** con quella seguente.

Flatten[Position[%, 1]]

{1, 4, 5, 6, 7, 9, 11, 16, 17}

Un caso particolare è quando $a = -1$; talvolta è un residuo quadratico (per esempio per $p = 5$), talvolta no (per esempio, se $p = 3$). Il seguente comando calcola l'insieme dei 30 primi dispari iniziali e mostra quelli rispetto ai quali -1 è un residuo quadratico. Teniamo presente che la funzione **Prime[n]** restituisce l'ennesimo primo.

Select[Prime[Range[2, 30]], JacobiSymbol[-1, #] == 1&]

{5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113}

Come si potrebbe vedere calcolando anche:

Select[Prime[Range[2, 30]], Mod[#, 4] == 1&]

{5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113}

i primi per cui -1 è un quadrato sono quelli che sono congrui a 1 (mod 4). Quando esiste non è difficile trovare una radice di -1.
Se si prende infatti $c = 4k + 1$ non residuo quadratico (mod p), per il Criterio di Euler si ha che $c^{2k} \equiv -1 \pmod{p}$ e quindi c^k è una radice di -1. Per trovare la radice di -1, quindi, basta determinare un non residuo modulo p.
A tale scopo è stata definita la funzione **noResiduo[p]** 6.2.4.2 che avrà come risultato:

noResiduo[Prime[Range[100, 130]]]

{2, 2, 2, 2, 3, 2, 5, 2, 3, 7, 7, 3, 2, 3, 2, 3, 3, 2, 5, 2, 2, 2, 5, 2, 2, 2, 2, 2, 11, 3, 2}

Si vede che la ricerca si ferma spesso a 2 o 3 e una volta arriva fino a 11.

6.2.2 Radice quadrata modulo un intero

Per prima cosa cerchiamo di risolvere il problema di determinare la radice di -1 modulo p per quei primi per cui esiste.
Per fare questo abbiamo definito la funzione **radice1[p]** 6.2.4.3:

radice1[53]

30

Si può comunque controllare la definizione per i primi 140 numeri primi nel seguente modo:

⋆ elenchiamo i primi 140 numeri primi che sono congrui ad 1 $\pmod 4$ con la funzione

primi = Select[Prime[Range[140]], Mod[#, 4] == 1&]

{5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193, 197, 229, 233, 241, 257, 269, 277, 281, 293, 313, 317, 337, 349, 353, 373, 389, 397, 401, 409, 421, 433, 449, 457, 461, 509, 521, 541, 557, 569, 577, 593, 601, 613, 617, 641, 653, 661, 673, 677, 701, 709, 733, 757, 761, 769, 773, 797, 809}

⋆ calcoliamo il valore di $r^2 \pmod p$ dove r è la radice di $-1 \pmod p$ calcolata con la funzione **radice1[p]** mentre p è un elemento dell'insieme *primi* prima definito.
Sottraendo a questo punto i vari p si dovrebbe ottenere una lista di -1. Per fare ciò usiamo la funzione **PowerMod[a, b, p]**

PowerMod[radice1/@ primi, 2, primi] - primi

{-1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1}

Passiamo ora al problema riguardante la risoluzione di:

$$X^2 \equiv a \pmod n$$

con n qualsiasi.
Procediamo per passi studiando per primo il caso $n = p$ primo. Sappiamo che:

Teorema 32. *Se $p > 2$ è primo, allora, per ogni a residuo quadratico $\pmod p$ ci sono al più 2 radici $\pmod p$.*

Dimostrazione. Supponiamo che x, y siano due radici di $a \pmod{p}$. Avremmo allora, che $p \mid (x^2 - y^2) = (x - y) \cdot (x + y)$ cioè $p \mid (x - y)$ oppure $p \mid (x + y)$ e quindi si ha che $y \equiv \pm x \pmod{p}$. □

Definiamo quindi la funzione **radiceModuloP[a, p]** 6.2.4.4.

radiceModuloP[25, 4073]

5

Si prendano ora in considerazione quaranta primi a partire dal centesimo:

testprimi=Prime[Range[100, 140]]

{541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809}

Verifichiamo che 49 è un residuo quadratico per tutti:

radiceModuloP[49, testprimi]

{7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7}

Questo perché 49 è un quadrato in $\mathbb{Z}$. Se invece studiamo la lista per 48.

radiceModuloP[48, testPrimi]

{46, { }, { }, 79, { }, { }, 219, 168, { }, 153, 95, { }, 50, { }, { }, { }, { }, { }, 159, { }, 45, 252, 82, { }, 148, { }, { }, 307, 178, { }, 261, { }, 187, { }, 220, { }, 260, { }, { }, { }, { }}

A questo punto passiamo allo studio del caso $n = p^r$.
Il procedimento che applicheremo sarà quello di ridurre, passo dopo passo, gli esponenti.
Il problema si differenzia a seconda che p sia pari o $p \geqslant 3$. Dipende anche se a sia o meno divisibile per p.
L'algoritmo **radiceModPotP[a, p, r]** 6.2.4.5 rispetta le seguenti regole:

$p > 2$ **e** $\mathbf{MCD}(a, p) = 1$**.** Si ha soluzione se, e solo se, ha soluzione $x^2 \equiv a \pmod{p}$.
Le soluzioni $\pmod{p^r}$ si ottengono per induzione secondo la seguente formula:

$$x = \bar{y} - (2\bar{y})^{-1}(\bar{y}^2 - a)$$

dove $\bar{y}$ è soluzione di $y^2 \equiv a \pmod{p^{r-1}}$ e $(2\bar{y})^{-1}$ è l'inverso aritmetico di $2\bar{y} \pmod{p}$.

radiceModPotP[5, 7, 4]

{ }

radiceModPotP[16, 7, 3]

{4, 339}

$p = 2$**, MCD**$(a, 2) = 1$ **e** $r = 2$**.** Si hanno soluzioni se, e solo se, $a \equiv 1 \pmod 4$ visto che a deve essere dispari e le soluzioni saranno precisamente $\{1, 3\}$.

radiceModPotP[9, 2, 2]

{1, 3}

radiceModPotP[3, 2, 2]

{ }

$p = 2$**, MCD**$(a, 2) = 1$ **e** $r \geqslant 3$**.** In questo caso si hanno soluzioni se, e solo se, è risolubile la congruenza $x^2 \equiv a \pmod 8$, cioè se e solo se $a \equiv 1 \pmod 8$.
Se, in più, esistono soluzioni queste sono esattamente 3 e cioè:

$$x,\ x + 2^{r-1},\ -x + 2^{r-1}.$$

Anche in questo caso le soluzioni si calcolano per induzione. Se, infatti, $\bar{y}$ è soluzione di $y^2 \equiv a \pmod{2^{r-1}}$, le soluzioni per $x^2 \equiv a \pmod{2^r}$ saranno date da:

$$x = \frac{\bar{y}^3 + (2 - a)\bar{y}}{2}$$

partendo da $\bar{y} = 1$ soluzione per $r = 3$.

radiceModPotP[9, 2, 7]

{3, 61, 67, 125}

radiceModPotP[5, 2, 9]

{ }

MCD$(a, p) \neq 1$**.** In questo caso si prende in considerazione s tale che $p^s \mid a$ e $p^{s+1} \nmid a$.
Se risulta $s = r$ le soluzioni saranno date da:

$$\{0, p^{\left[\frac{p}{2}\right]}, 2p^{\left[\frac{p}{2}\right]}, \ldots, p^r - p^{\left[\frac{p}{2}\right]}\}.$$

Se, invece, $s \neq r$ e s risulta **dispari**, non ci sono soluzioni; se risulta **pari** le soluzioni ci saranno se, e solo se,

$$x^2 \equiv \frac{a}{p^s} \pmod{p^{r-s}}$$

ha soluzione $\bar{y}$ determinando così come soluzioni dell'equazione di partenza

$$\{p^{\frac{r}{2}}(y + jp^{r-s}) \text{ con } j \in \{0, 1, \ldots, p^{\frac{r}{2}-1}\}\}.$$

radiceModPotP[14, 7, 9]

{ }

radiceModPotP[121, 11, 3]

{11, 110, 132, 231, 253, 352, 374, 473, 495, 594, 616, 715, 737, 836, 858, 957, 979, 1078, 1100, 1199, 1221, 1320}

Osserviamo che questa funzione è più veloce di un eventuale calcolo effettuato per tentativi definito dal comando:

```
radiceViaTentativi[a_, n_]:=
Select[Range[0, n-1], Mod[#^2, n] == Mod[a, n]&];
Attributes[radiceViaTentativi]=Listable;
```

Confrontiamo i tempi:

radiceViaTentativi[Range[32], 2^5]//Timing

{0.07 Second, {{1, 15, 17, 31}, { }, { }, {2, 6, 10, 14, 18, 22, 26, 30}, { }, { }, { }, { }, {3, 13, 19, 29}, { }, { }, { }, { }, { }, { }, {4, 12, 20, 28}, {7, 9, 23, 25,}, { }, { }, { }, { }, { }, { }, { }, {5, 11, 21, 27}, { }, { }, { }, { }, { }, { }, {0, 8, 16, 24}}}

radiceModPotP[Range[32], 2^5]//Timing

{0.021 Second, {{1, 15, 17, 31}, { }, { }, {2, 6, 10, 14, 18, 22, 26, 30}, { }, { }, { }, { }, {3, 13, 19, 29}, { }, { }, { }, { }, { }, { }, {4, 12, 20, 28}, {7, 9, 23, 25,}, { }, { }, { }, { }, { }, { }, { }, {5, 11, 21, 27}, { }, { }, { }, { }, { }, { }, {0, 8, 16, 24}}}

Siamo così arrivati al calcolo della radice modulo un intero n qualunque. Sappiamo che a ammette radice modulo $n = \prod_i p_i^{e_i}$ se, e solo se, a ammette radici per ogni $p_i^{e_i}$ della fattorizzazione di n. Per come è stata definita, la "velocità" della funzione **radiceN[a, n]** 6.2.4.8 è condizionata alla grandezza di n. Per interi molto grandi, infatti, si è soggetti alla velocità della funzione **FactorInteger[n]**. Quindi, per interi con molti fattori il tempo di risoluzione cresce in modo esponenziale.

radiceN[12, 32]

{ }

radiceN[16, 32]

{4, 12, 20, 28}

6.2.3 Di nuovo sulle congruenze polinomiali

Nel Paragrafo 4 di questa parte, abbiamo descritto delle funzioni per risolvere le congruenze polinomiali. Tutte partivano da una funzione **congruPoli[f(x), p]** 4.3.4.3 che risolveva la congruenza $f(X) \equiv 0 \pmod{p}$ effettuando prove con tutti gli elementi del sistema completo di Residui modulo p.
Come abbiamo già osservato nel Paragrafo 4, tale funzione è "lenta". Ora, tramite la funzione **radiceModuloP[a, p]** 6.2.4.4, possiamo ridefinirla in modo più pratico.

Descriviamo qui di seguito l'algoritmo che abbiamo implementato dando in input il polinomio $f(X)$ e il valore del modulo p.

Passo 1. Calcoliamo il valore del polinomio $g(X)$ che risulta essere il $\text{MCD}(f(X), X^p - X)$.
Quindi, se il polinomio $g(X)$ non ha termine noto abbiamo che una radice di $f(X)$ è 0 e quindi semplifichiamo ponendo $g(X) = \frac{g(X)}{X}$.

Passo 2. Calcoliamo il grado del polinomio $g(X)$ e, se risulta essere pari a 0 terminiamo i calcoli.
Se $g(X)$ risulta a grado 1 abbiamo la soluzione pari a $-\frac{a_0}{a_1}$ supponendo di scrivere $g(X) = a_1X + a_0$.
Se, invece, risulta di grado 2 e quindi $g(X) = a_2X^2 + a_1X + a_0$, le soluzioni (due) vengono calcolate determinando prima $d = a_1^2 - 4a_0a_2$, quindi calcolando $e = \sqrt{d}$ e restituendo come output $\{\frac{-a_1+e}{2a_2}, \frac{-a_1+e}{2a_2}\}$.
Per come è definito d abbiamo che e (cioè la radice) esiste sempre.

Passo 3. A questo punto prendiamo y a caso nel Sistema Completo di Residui modulo p e calcoliamo $h(X) = \text{MCD}(g(X), (X + y)^{\frac{p-1}{2}})$.
Se dunque il grado di $h(X)$ è uguale al grado di $g(X)$ oppure è 0, cambiamo la scelta di y.

Passo 4. Le soluzioni della funzione vengono calcolate in modo ricorsivo calcolando il presente algoritmo per i polinomi $h(X)$ e $\frac{g(X)}{h(X)}$.

Prima di dare degli esempi, facciamo delle osservazioni sull'algoritmo.
Al **Passo 1** si è preso $g(X)$ così che corrisponde al prodotto dei fattori $X - a$ dove a è radice del polinomio $f(X)$.
Al **Passo 3** si cerca y in modo tale che $(a + y)$ sia un residuo quadratico. La possibilità di sbagliare, nella scelta casuale di y, è pari a $\frac{1}{2^{\deg(g(X))-1}}$. Questo ci dice che se p è molto piccolo rispetto al grado del polinomio $g(X)$, conviene risolvere la congruenza testando semplicemente gli elementi del Sistema Completo di Residui.

La funzione che deriva da questo algoritmo risulta essere **congPolinomiale[f, p]** 6.2.4.9 che qui di seguito confrontiamo con la precedentemente

descritta **congruPoli[f, p]** 4.3.4.3.

congPolinomiale[x^4 - 3, 73]//Timing

{0.01 Second, { }}

congruPoli[x^4 - 3, 73]//Timing

{0.05 Second, La congruenza non ha soluzione}

Questo avendo posto $p >> \deg(f(X))$. Altrimenti:

congPolinomiale[2 x^14 + x^17 - 4 x^22, 11]//Timing

{0.05 Second, 0}

congruPoli[2 x^14 + x^17 - 4 x^22, 11]//Timing

{0.02 Second, {11}}

6.2.4 Funzioni utilizzate

♦ **6.2.4.1.** La funzione **eulero[a, p]** calcola il valore dell'espressione $a^{\frac{p-1}{2}} \pmod p$ tramite la funzione **PowerMod[a, b, p]** e quindi, se tale valore risulta essere pari ad 1 stampa la stringa *è un residuo quadratico*, altrimenti stampa *non è un residuo quadratico*. Come output restituisce il valore della congruenza valutato -1 se la funzione PowerMod restituisce lo stesso valore della funzione Mod[-1, p].

```
Clear[eulero];

eulero[a_, p_Integer?PrimeQ]:=
  Module[{valore},
   valore = PowerMod[a, (p-1)/2, p];
   If[valore==1,
     Print[StringForm["`` e' un residuo quadratico", a]],
     Print[StringForm["`` non e' un residuo quadratico", a]]];
   If[Mod[-1, p]==valore,
     valore=-1];
   Return[valore]]
```

♦ **6.2.4.2.** La funzione **noResiduo[p]** calcola un non residuo per poter, successivamete calcolare la radice. La funzione lavora esclusivamente su valori dispari di p ed utilizza la funzione built-in **Block** (che permette di inserire una serie di comandi, separati da un punto e virgola, da effettuare nell'ordine) con la stessa funzione della già usata **Module** ma che in questo caso permette una definizione più chiara della funzione.
Il lavoro che svolge la funzione è quello di calcolare, per i primi determinati al variare di un contatore n (**Prime[n]**) il valore del simbolo di Jacobi restituendo in output il primo di tali elementi che risultano avere tale valore pari ad 1.

```
Clear[noResiduo];

noResiduo[p_Integer?PrimeQ]:=
     Block[{n},
        n=0;
       While[JacobiSymbol[Prime[++n], p]==1];
       Prime[n]];

Attributes[noResiduo]=Listable;
```

Al termine abbiamo assegnato alla funzione la proprietà di essere *Listable* cioè di poter lavorare su liste.

La tecnica per la ricerca dei non resudui è molto pratica, ma in teoria può creare seri problemi.
Potrebbe capitare che per primi molto grandi il "primo" non residuo risultasse molto grande. Ci è comunque garantito da Riemann che è possibile trovere un non residuo modulo p minore di $2(\lg p)^2$.
Con varie prove si può arrivare a determinare che per i primi $p \leqslant 36.000.000$ il primo non residuo è sempre minore di 60. Come da grafico:

```
ListPlot[Table[noResiduo[Prime[i]], {i, 2, 1009}],
PlotRange → {0, 10}, PlotStyle→ {PointSize[0.01],
RGBColor[0.128908, 0.859388, 0.0468757]}];
```

ListPlot[Table[noResiduo[Prime[i]], {i, 1010, 2000}], PlotRange → {0, 10}, PlotStyle→ {PointSize[0.015], RGBColor[0.128908, 0.859388, 0.0468757]}];

Vediamo che in entrambi i grafici (il primo per i primi 1009 primi, il secondo per i successivi 990) i valori sono tutti addensati tra i valori 2 e 3 e giungono al massimo a 7, cioè sono tutti < 60.

♦ **6.2.4.3.** La funzione **radice1[p]** restituisce un valore della $x \pmod p$ (nel caso $p \equiv 1 \pmod 4$) tale che $x^2 \equiv -1 \pmod p$. Per fare ciò abbiamo utilizzato una scrittura diversa per la funzione built-in **If**, in questo caso più pratica. La funzione **radice1** è stata definita con l'ausilio delle funzioni **PowerMod[a, b, p]** e **noResiduo[p]** 6.2.4.2 applicando il criterio di Euler. Le operazioni, per la presenza della stringa **/;**, vengono effettuate solo se è verificata la condizione *Mod[p, 4]==1*.
È stata scelta questa scrittura e non la funzione **If** perché ci è sembrato più semplice e chiaro anche a livello visivo, ma soprattutto perchè non è stato necessario definire un'operazione alternativa.

```
Clear[radice1];

radice1[p_]:=PowerMod[noResiduo[p], (p-1)/4, p] /; Mod[p, 4]==1

radice1[2]:=1
```

♦ **6.2.4.4.** La funzione **radiceModuloP[a, p]** restituisce un valore di x tale che $x^2 \equiv a \pmod p$.
Si è definita la funzione suddividendola in varie possibilità. Non si sono usate le funzioni **Module** ed **If** per problemi pratici: avremmo dovuto scrivere una serie di If e Return concatenati l'uno dentro l'altro, che avrebbero reso illeggibile il listato e determinando maggior possibilità di errore nella scrittura del programma stesso.

Si sono suddivisi quindi i casi come da descrizione dell'algoritmo al Paragrafo 6.1.

```
Clear[radiceModuloP];
```

```
radiceModuloP[a_, 2]:=Mod[a, 2];

radiceModuloP[a_, p_]:= {} /; JacobiSymbol[a, p] == -1;

radiceModuloP[a_, p_]:= 0 /; Mod[a, p]== 0;

radiceModuloP[a_, p_]:=
  Min[ PowerMod[a, (p+1)/4, p]*{-1, 1} + {p, 0}] /; Mod[p, 4] == 3;

radiceModuloP[a_, p_]:=
      (l = (p-1)/4;
       s=0;
       h=noResiduo[p];
       While[EvenQ[l], l/=2; s++];
       k = p-1;
       Scan[(k/=2;
         If[Mod[#*PowerMod[h, k, p], p]!=1,
           k+=(p-1)/2])&,
           Reverse[NestList[Mod[# #, p]&, PowerMod[a, l, p], s]]];
       Min[Mod[PowerMod[a, (l+1)/2, p]*PowerMod[h, k/2, p], p]
             * {-1, 1} + {p, 0}])
       /; Mod[p, 4] ==1;

Attributes[radiceModuloP] = Listable;
```

La definizione della seconda regola (*JacobiSymbol[a, p] == -1*) è stata inserita per definire la funzione in tutti i casi restituendo { } qualora a fosse un non residuo.
Nel caso $p \equiv 3 \pmod 4$ si è utilizzata la funzione **Min[lista]** per selezionare la radice più piccola.
Per il caso $p \equiv 1 \pmod 4$ si è implementato l'algoritmo descritto da Tonelli - Shanks riportando, per motivi di efficacia, delle modifiche.
Si è partiti con il calcolo di k tramite un ciclo **While**. Con la funzione **NestList[f, espr, n]** per formare una lista di tutte le potenze di $k \pmod p$. Infine, tramite le funzioni **Scan[espr, lista]** e **Reverse[lista]** si sono svolti i calcoli descritti dall'algoritmo di Tonelli - Shanks.
Sempre in questo caso, è interessante come si è calcolato k.
In un primo tempo si è posto $k = p - 1$. Ad ogni passo k viene diviso per 2 (con il comando *k/=2*). Se il nuovo valore è tale che $a^l h^k \equiv 1 \pmod p$ si interrompono i calcoli, altrimenti si rivaluta k aggiungendo $\frac{p-1}{2}$ (con il comando *k+=(p-1)/2*) e si ricominciano le verifiche.

♦ **6.2.4.5.** La funzione **radiceModPotP[a, p, r]** restituisce tutte le radici di $a \pmod{p^r}$ in ordine crescente facendo uso della funzione **Shanks[a, p]** 6.2.4.6 perchè risulta più veloce della funzione **radiceModuloP[a, p]** 6.2.4.4.

Qui si è descritta la funzione nel caso di esponente 1.
Successivamente si considera sempre $r > 1$.

```
Clear[radiceModPotP];

radiceModPotP[a_, p_, 1]:= Block[{radice=Shanks[a, p]},
      If[!NumberQ[radice],
         {},
         Union[Mod[{p, 0} + {-1, 1} radice, p]]]];
```

Caso in cui $\text{MCD}(a, p) \neq 1$. Tramite la funzione stessa, richiamata, ci si riduce al caso $\text{MCD}(a, p) = 1$.

```
radiceModPotP[a_, p_, r_]:= Block[{s=1, j},
       If[Mod[a, p^r]==0,
          Return[Range[0, p^r-1, p^Ceiling[r/2]]]];
       While[Mod[a, p^s]==0,
           s++];
       s--;
       If[OddQ[s],
           {},
            Flatten@Table[(radiceModPotP[a/p^s, p, r-s] +
                   (j - 1) p^(r-s)) p^(s/2),
                       {j, p^(s/2)}]]]
  /; Mod[a, p] == 0 && r > 1
```

Caso in cui p sia dispari e $\text{MCD}(a, p) = 1$.

```
radiceModPotP[a_, p_, r_]:=Block[{j,
        radice=Shanks[a, p]},
        If[!NumberQ[radice],
           Return[{}],
           Do[ radice = Mod[radice -
                    PowerMod[2 radice, -1, p] *
                    (radice^2 - a),
               {i, 2, r}];
           Return[Sort[{-1, 1} * radice +
                       {p^r, 0}]]]]]
     /; p != 2 && Mod[a, p] != 0 && r > 1
```

Caso in cui $p = 2$ ed:
- $r = 2$ e $a \equiv 3 \pmod 4$;
- $r > 2$ e a è dispari con $a \not\equiv 1 \pmod 8$.

Non restituisce soluzioni.
Il comando || sta ad indicare **OR**.

```
radiceModPotP[a_, 2, r_]:= {}
     /; (r ==2 && Mod[a, 4] == 3) ||
        (r >= 3 && Mod[a, 8] != 1 && OddQ[a])
```

Caso in cui $a \equiv 1 \pmod 4$, $r = 2$ e $\text{MCD}(a, 2) = 1$.

```
radiceModPotP[a_, 2, 2]:={1, 3}
        /; Mod[a, 4] == 1
```

Caso in cui $p = 2$ ma $r \geqslant 3$.

```
radiceModPotP[a_, 2, r_]:=
    Block[{radice=Nest[Mod[(#^3 + (2 - a) #) / 2, 2^r]&,
                       1, r-3]},
          Union[{radice, 2^r - radice},
                Mod[{radice,  2^r - radice} + 2^(r-1),
                     2^r]]]]
   /; OddQ[a] && r >= 3
```

Permettiamo alla funzione di agire su liste.

```
Attributes[radiceModPotP] = Listable
```

♦ **6.2.4.6.** La funzione **Shanks[a, p]** applica l'algoritmo di Tonelli - Shanks (in una forma più pratica della funzione **radiceModuloP[a, p]** 6.2.4.4) restituendo la più piccola radice di $a \pmod p$ se p è primo.
Facciamo uso della funzione **noResiduo[p]** 6.2.4.2. In più anche alla funzione **PowerMod[a, b, n]** diamo la proprietà di essere *Listable* tramite il comando *SetAttributes[PowerMod, Listable]*.
La definizione delle proprietà, in questo caso, va inserita prima della definizione della funzione in quanto in essa si fa uso di tali caratteristiche.

```
Clear[Shanks];

Attribites[Shanks] = Listable

SetAttributes[PowerMod, Listable]

Shanks[a_, 2] := Mod[a, 2]

Shanks[a_, p_] := {}
    /; JacobiSymbol[a, p] == -1

Shanks[a_, p_] :=
      Min[PowerMod[a, (p+1)/4, p]*{-1, 1} + {p, 0}]
   /; Mod[p, 4] == 3

Shanks[a_, p_] := Block[{k = (p-1)/2,
       i, l, n, r, c, b,
       s = 1},
       While[EvenQ[k],
             k /= 2;
             s++];
       {c, r, n} = PowerMod[{noResiduo[p], a, a},
                            {k, (k+1)/2, k},
                            p];
       While[n != 1,
             l = s;
             b = n;
             Do[If[b == 1,
```

```
                b = c;
                s = i - 1,
                b = Mod[b b, p],
                {i, l}];
              {c, r, n} = Mod[b, {b, r, b n}, p]];
          Min[r, p - r]]
    /; Mod[p, 4] == 1
```

♦ **6.2.4.7.** La funzione **teoCinRes[lista, lista]** restituisce la soluzione del sistema di congruenze:

$$\begin{cases} X \equiv a_i \pmod{m_i} \\ 1 \leqslant i \leqslant r \end{cases}$$

con $a_i \in \mathbb{Z}$ e $\text{MCD}(m_i, m_j) = 1$ se $i \neq j$. Applicando il Teorema Cinese dei Resti.
In realtà tale funzione è già definita **ChineseRemainderTheorem[lista, lista]** ma qui la ridefiniamo applicando la funzione **PowerMod[a, -1, p]** per calcolare l'inverso di $a \pmod{p}$.

```
Clear[teoCinRes];

teoCinRes[lista1_, lista2_] :=
      Block[{m = Times@@lista2,
             m2},
             m2 = m /lista2;
             Mod[Apply[Plus,
                       lista1 * m2 *
                       PowerMod[m2, -1, lista2]], m]]
```

♦ **6.2.4.8.** La funzione **radiceN[a, n]** restituisce tutte le radici di a modulo n in ordine crescente. Fa uso delle funzioni **teoCinRes[lista, lista]** 6.2.4.7, **radiceModPotP[a, p, r]** 6.2.4.5, **Shanks[a, p]** 6.2.4.6 e **noResiduo[n]** 6.2.4.2. Anche a questa funzione permettiamo di agire su liste.

```
Clear[radiceN];

radiceN[a_, n_]:=
    Block[{fattori= Transpose@FactorInteger[n]},
           radici=radiceModPotP[a, fattori[[1]], fattori[[2]]];
           If[MemberQ[radici, {}],
              Return[{}]];
           PrependTo[radici,
                 teoCinRes[List[##], fattori[[1]]^fattori[[2]]&];
           Union@Flatten[Outer@@radici,
                 Length[radici] - 2]

Attributes[radiceN] = Listable
```

Il programma per prima cosa raggruppa tutte le radici di a modulo i fattori di n, creando la lista *radici*. Con il comando **Outer** crea tutte le

possibili combinazioni di tali elementi e, ad ognuna, applica la funzione **teoCinRes[lista, lista]**[19]

♦ **6.2.4.9.** La funzione **congPolinomiale[f(x), p]** calcola le soluzioni della congruenza $f(X) \equiv 0 \pmod{p}$ utilizzando la funzione **radiceModuloP[a, p]** 6.2.4.4 secondo l'algoritmo descritto a pag. 220.

```
Clear[congPolinomiale];

<<Algebra`PolynomialPowerMod`

congPolinomiale[f_, p_]:=
  Module[{g=PolynomialGCD[f, x^p - x, Modulus -> p]},
          deg=Exponent[g, x];
          solu={};
          If[deg==0,
             Return[{}]];
          coef=CoefficientList[g, Variables[g][[1]]];
          If[coef[[1]]==0,
             {g=Simplify[g/x],
              solu={0}}];
          If[deg== 1,
             Return[Mod[-coef[[1]]/coef[[2]], p]]];
          d=coef[[2]]^2 - (4 coef[[1]] coef[[3]]);
          e=radiceModuloP[d, p];
          If[deg == 2,
             Return[Mod[{(-coef[[2]]+e)/(2coef[[3]]),
                (-coef[[2]]-e)/(2coef[[3]]) }, p]]];
          insieme= Range[p];
          i=Random[Integer, {1, Length[insieme]}];
          a=insieme[[i]];
          insieme=Delete[insieme, i];
          h=PolynomialGCD[g, (x-a)^((p-1)/2)-1,
                      Modulus->p];
          grado = Exponent[h, x];
          While[(grado == 0 || grado == deg),
             {i=Random[Integer, {1, Length[insieme]}],
              a=insieme[[i]],
              insieme = Delete[insieme, i],
              h=PolynomialGCD[g, (x-a)^((p-1)/2)-1,
                          Modulus->p]};
              grado = Exponent[h, x]];
          g =Simplify[g/h];
          solu=Union[Union[congPolinomiale[h, p],
                           congPolinomiale[g, p]],
                     solu];
          Return[solu]];
```

[19] Il comando **teoCinRes[List[# #], modulo] &** permette di applicare la funzione ad un numero qualsiasi di argomenti. Viene chiamata funzione pura.

Riferimenti bibliografici

[AR] R. B. J. T. Allenby e E. J. Redfern, *Introduction to Number Theory with computing*, Edward Arnold, 1989.

[A] G. E. Andrews, *Number Theory*, New York: Dover, 1994.

[Ba] Bachmann, *Nieder Zahlentheorie*, Teubner, 1902;
ristampato da Chelsea Publ. Co., New York, (1968).

[BN] R. Balasubramanian e S. V. Nagaraj, *Density of Carmichael numbers with three prime factora*, Math. of Computation **66** n. 220 (1997), pag. 1705-1708.

[B] I. G. Bashmakova, *Diophantus and Diophantine Equations*,
Washington, DC: Math. Assoc. Amer., 1997.

[BS] Z. I. Borevich e I. R. Shafarevich, *Number theory*, Academic Press, New York, 1966.

[Bu] D. M. Burton, *Elementary Number Theory*, 4th ed. Boston, MA: Allyn and Bacon, 1989.

[C1] R. D. Carmichael, *Note on a new number theory function*, Bull. Amer. Math. Soc. **16** (1910), pag. 232 - 238.

[C2] R. D. Carmichael, *On composite numbers P which satisfy the Fermat congruence* $a^{P-1} \equiv 1 \pmod{P}$, Amer. Math. Monthly **19** (1912), pag. 22 - 27.

[Ch] J. Chernick, *On Fermat's simple theorem*, Bull. Amer. Math. Soc. **45** (1939), pag. 269-274.

[C] H. Cohen, *A course in computational algebraic number theory*, Springer, 1996.

[Co] H. Cohn, *A second course in Number theory*, John Wiley, New York, 1962.

[CG] J. H. Conway e R. K. Guy, *The book of Numbers*, New York: Springer-Verlag, 1996.

[D] H. Dubner, *A new method for producing large Carmichael numbers*, Math. Comp. **53** (1989), pag. 411-414.

[E] P. Erdös, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen **4** (1956), pag. 201-206.

[F] M. Fontana e S. Gabelli, *Insiemi, Numeri e Polinomi*, CISU, Roma, 1989.

[Ga] J. A. Gallian, *Contemporary Abstract Algebra*, 3th ed. Lexington, Mass: D. C. Health, 1994.

[G] K. F. Gauss, *Disquisitiones Aritmeticae*, New Haven, Yale Univ. Press, 1966.

[GKP] R. L. Graham e D. E. Knuth e O. Patashnik, *concrete mathematics*, Addison-Wesley, Reading, MA, 1989.

[Guy] R. K. Guy, *Unsolved Problems in Number Theory*, 2nd ed. New York: Springer-Verlag, 1994.

[IR] K. Ireland e M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed. New York: Springer-Verlag, 1990.

[JM] J. P. Jones e Yu V. Matiyasevich, "Exponential Diophantine Representation of Recursively Enumerable Sets." *Proceedings of the Herbrans Symposium, Marseilles, 1981*, Amsterdam, Netherlands: North-Holland, 1982.

[Knu] D. E. Knuth, *The Art of Computer Programming*, vol. 2, Addison-Wesley, Reading, Mass. 1971

[K] N. Koblitz, *A course in number theory and Cryptography*, Springer, New York. 1994

[Kr] L. Kronecker, *Zur Geschichte des Reziprozitäs gestezes*, 1875.

[LN] G. Löh e W. Niebuhr, *A new algorithm for constructing large Carmichael numbers*, Math. of Computation **65** n. 214 (1996), pag. 823-836.

[LK] H. Loo-Keng, *Intoduction to Number Theory* (translated by Peter Shiu), Berlin Heidelberg New York: Springer-Verlag, 1982.

[M] L. J. Mordell, *Diophantine Equations*, New York: Academic Press, 1969.

[NZ] I. Niven e H. S. Zuckerman , *An introduction to the theory of numbers*, John Wiley, New York, 1980.

[O] C. D. Olds, *Frazioni Continue*, Zanichelli, 1972.

[S] D. Shanks, *Solved and unsolved Problems in Number Theory*, 4th ed. New York: Chelsea.

[SH] M. Stark, *An introduction to Number Theory*, The MIT Press, 1987.