3 Il "piccolo" Teorema di Fermat

Pierre de Fermat, francese, giudice presso il tribunale di Tolosa, è considerato 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:

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

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. Innanzitutto, mostriamo che: 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 questione:

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

Per maggiori dettagli storici su tale problematica rinviamo a [R, pag. 85]. Tale questione ha una risposta positiva per $n \leqslant 340$, ma l'esempio precedente (che è dovuto a Sarrus e risale al 1819) mostra che, in generale, la risposta è negativa. 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, la cui esistenza dimostra che il "Piccolo" Teorema di Fermat non si inverte.

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 ad esempio che $3^{340} \equiv 56 \pmod{341}$). 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 $\mathrm{MCD}(a, n) = 1$, 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:

$$a^{\varphi(n)} \cdot k_1 \cdot k_2 \cdot \ldots \cdot k_{\varphi(n)} = ak_1 \cdot ak_2 \cdot \ldots \cdot ak_{\varphi(n)} \equiv k_1 \cdot k_2 \cdot \ldots \cdot k_{\varphi(n)} \pmod{n}.$$

Poiché $\mathrm{MCD}(k_1 \cdot k_2 \cdot \ldots \cdot k_{\varphi(n)}, n) = 1$, 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 $a^{\varphi(n)+1} \not\equiv a \pmod{n}$.
(c) Si noti che, se $\mathrm{MCD}(a, n) = 1$, allora $a^{\varphi(n)-1}$ è un inverso aritmetico (mod n) di a.

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 $\mathrm{MCD}(a, n) =: d \mid b$, sono date da:

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

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

Il seguente celebre risultato verrà utilizzato tra poco per fornire una ulteriore applicazione del "Piccolo" Teorema di Fermat, e precisamente nella risoluzione delle congruenze quadratiche del tipo $X^2 \equiv -1 \pmod{p}$, dove p è un numero primo dispari.

Teorema 3.9. *(**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:

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

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

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

Osservazione 3.10. (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 $d = 1$.
(c) Si osservi che, se $p \geq 5$ è un primo, allora $(p-3)!$ è un inverso aritmetico di $p-2 \pmod{p}$, essendo $1 \equiv (p-2)! = (p-2)(p-3)! \pmod{p}$. Più generalmente, si può osservare che, per ogni k, $1 \leq k \leq p-2$, l'intero $((p-2)!)/k$ è un inverso aritmetico di $k \pmod{p}$.

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.).

II APPLICAZIONE: Il Teorema Cinese dei Resti.
Siano $n_1, n_2, \ldots, n_r$ *interi positivi tali che* $\mathrm{MCD}(n_i, n_j) = 1$ *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 $\bmod n_1 \cdot n_2 \cdot \ldots \cdot n_r$.

Dimostrazione. Sia $n := n_1 \cdot n_2 \cdot \ldots \cdot n_r$ 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 $\mathrm{MCD}(N_i, n_i) = 1$, allora $N_i^{\varphi(n_i)} \equiv 1 \pmod{n_i}$ (Teorema di Euler-Fermat). 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). □

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.

III 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 $\mathrm{MCD}(m_i, m_j) = 1$, *se* $i \neq j$. *Si ponga* $d_i := \mathrm{MCD}(a_i, m_i)$, $a_i' := \dfrac{a_i}{d_i}$, $b_i' := \dfrac{b_i}{d_i}$ *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. In tal caso, le soluzioni di* (2) *si trovano considerando il seguente 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 $\mathrm{MCD}(n_i, n_j) = 1$, *se* $i \neq j$.
Precisamente, se $m := m_1 m_2 \cdot \ldots \cdot m_r, d := d_1 d_2 \cdot \ldots \cdot d_r, n := n_1 n_2 \cdot \ldots \cdot n_r$ *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)*:*

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

[Nota: *"Sollevando" in* $\mathbb{Z}$ *le soluzioni dei sistemi di congruenze* (2) *e* $(2^{\#})$, *abbiamo che l'insieme delle "soluzioni in* $\mathbb{Z}$*" del sistema* $(2^{\#})$ *è dato da* $\{\mathring{x} + tn : t \in \mathbb{Z}\}$ *e coincide con l'insieme delle "soluzioni in* $\mathbb{Z}$*" di* (2)*, che è 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, $x \equiv \mathring{x} \pmod{n}$. Da ciò si conclude facilmente. □

Esempio 3.11. Si consideri il seguente sistema:

$$\begin{cases} 2X \equiv 2 \pmod{4} \\ 2X \equiv 3 \pmod{5} \\ 14X \equiv 7 \pmod{21} \end{cases} \tag{3.11.1}$$

Tenendo presente che l'inverso aritmetico di 2 (mod 5) è 3 e l'inverso aritmetico di 2 (mod 3) è 2, al sistema (3.11.1) è associato il seguente sistema:

$$\begin{cases} X & \equiv 1 \pmod 2 \\ X & \equiv 4 \pmod 5 \\ X & \equiv 2 \pmod 3 \end{cases} \tag{3.11.2}$$

Il sistema (3.11.2) ha un'unica soluzione $\mathring{x} = 1 \cdot 15 + 4 \cdot 6^4 + 2 \cdot 10^2 \equiv -1 \pmod{30}$. Questa determina 14 soluzioni di (3.11.1) (modulo 420) date da:

$$x_k = -1 + k \cdot 30, \quad 0 \leqslant k \leqslant 13.$$

IV 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:

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

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. □

V APPLICAZIONE: *Sia n un intero tale che* $\mathrm{MCD}(n, 10) = 1$. *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 $3 \mid 111$.

VI APPLICAZIONE: *Siano $n, a \in \mathbb{Z},\ n > 0$ tali che* $\mathrm{MCD}(a, n) = \mathrm{MCD}(a - 1, n) = 1$. *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 (oltre alla condizione $\mathrm{MCD}(a, n) = 1$) 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 $3^{10} \pmod{11}$, senza usare il "Piccolo" Teorema di Fermat, 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 ricorsivo 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, $0 \leqslant h \leqslant k$:

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

Si noti anche che $r_{h+1} \equiv (r_h)^2 \pmod{n}$, per $0 \leqslant h \leqslant k-1$.

Conclusione.

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

Esempio 3.12. Per calcolare il più piccolo intero positivo congruo a $2^{138} \pmod{23}$, scriviamo:

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

Poiché:

$$\begin{aligned} 2^{2^0} &\equiv 2 \pmod{23} & 2^{2^1} &\equiv 4 \pmod{23} \\ 2^{2^2} &\equiv 16 \equiv -7 \pmod{23} & 2^{2^3} &\equiv 49 \equiv 3 \pmod{23} \\ 2^{2^4} &\equiv 9 \pmod{23} & 2^{2^5} &\equiv 81 \equiv 12 \pmod{23} \\ 2^{2^6} &\equiv 144 \equiv 6 \pmod{23} & 2^{2^7} &\equiv 36 \equiv 13 \pmod{23}, \end{aligned}$$

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, il suo 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 proprietà sono equivalenti:
(i) l'enunciato del "Piccolo" Teorema di Fermat assieme all'enunciato del 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 già 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:

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

definita da $\rho(a + n\mathbb{Z}) := (a + n_1\mathbb{Z}, \ldots, a + n_r\mathbb{Z})$, è un isomorfismo di anelli.
[Suggerimento: se $a + n\mathbb{Z} \in \mathrm{Ker}(\rho)$, allora $a \in \cap n_i\mathbb{Z} = n\mathbb{Z}$, dove $n = \mathrm{mcm}(n_i \mid 1 \leqslant i \leqslant r)$. La suriettività di ρ 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 della congruenza $a^{\varphi(n)} \equiv 1 \pmod{n}$ 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 $2^{N-1} \equiv 1 \pmod N$.]