TN1 - Introduzione alla teoria dei numeri - A.A. 2009/2010
Valutazione "in itinere" - II Prova

MATRICOLA (o, altro identificativo personale): .....
COGNOME: ..... **NOME:** .....

esercizio	**1**		**2**		**3**		**4**						**5**				**6**		
punteggio max	6	4	6	4	6	2	3	2	3	2	4	6	2	3	3	4	6	3	2
punteggio assegnato																			
totale																			

ESERCIZIO 1. (a) Determinare per quali valori del parametro λ, con $0 \leq \lambda \leq 10$, la seguente congruenza è risolubile:

$$5X^2 + \lambda \cdot X + 9 \equiv 0 \pmod{77}.$$

(b) Per almeno uno dei valori di λ, con $0 \leq \lambda \leq 10$, per il quale la congruenza in **(a)** è risolubile determinare tutte le sue soluzioni.

ESERCIZIO 2. **(a)** Determinare per quali valori di a, con $0 \leq a \leq 12$, la seguente congruenza esponenziale (in una indeterminata X)

$$9^X \equiv a \pmod{13}$$

è risolubile.

(b) Per ciascuno dei valori di a, con $0 \leq a \leq 12$, per i quali la congruenza precedente è risolubile determinare tutte le soluzioni $\pmod{12}$.

ESERCIZIO 3. **(a)** Sia p un primo dispari e sia a un intero tale che $p \nmid a$. Dimostrare che il valore del simbolo di Legendre $\left(\frac{a}{p}\right)$ coincide con $(-1)^{\nu(a)}$, dove $\nu(a)$ è il numero degli elementi ka, per $1 \leq k \leq (p-1)/2$, aventi la proprietà che $ka \equiv r_k \pmod{p}$, con $(p+1)/2 \leq r_k \leq p-1$.

(b) Utilizzando il metodo descritto in **(a)**, calcolare

$$\left(\frac{a}{17}\right)$$

per $a = 7, 8$.

ESERCIZIO 4. **(a)** Mostrare che 18 possiede una radice primitiva dell'unità (cioè, mostare che esiste un intero r tale che $r^k \equiv 1 \pmod{18}$ per $k = \varphi(18)$ e $r^h \not\equiv 1 \pmod{18}$, per ogni h, con $1 \leq h \lneq \varphi(18)$).

(b) Determinare tutte le radici primitive dell'unità (mod 18).

(c) Determinare la più piccola radice primitiva dell'unità (mod 18), che denotiamo con r, e poi calcolare $\mathrm{ind}_r(a)$ per ogni a, con $1 \leq a \leq 17$ e $\mathrm{MCD}(a, 18) = 1$.

(d) Determinare per quali valori di a, con $\mathrm{MCD}(a, 18) = 1$ e $1 \leq a \leq 17$, la congruenza

$$X^{15} \equiv a \pmod{18}$$

è risolubile.

(e) Determinare se, eventualmente, ci sono altri valori di a, con $0 \leq a \leq 17$ (e $\mathrm{MCD}(a, 18) \neq 1$), per i quali la $X^{15} \equiv a \pmod{18}$ è risolubile.

(f) Per ogni valore di a per il quale la congruenza in **(c)** è risolubile, determinarne tutte le soluzioni.

ESERCIZIO 5. Per ogni intero $n \geq 1$ sia

$$F(n) := \prod_{d|n} d.$$

(dove al solito per "$d \mid n$" si intende "$d \mid n$ e $1 \leq d \leq n$").

(a) Mostrare che F è una funzione aritmetica invertibile (rispetto al prodotto $*$ di convoluzione), ma che non è una funzione moltiplicativa.

(b) Determinare $F(6)$ e $F^{-1}(6)$.

(c) Sia f la funzione aritmetica tale che $F = \sigma_f (= f * \mathbf{1})$. Determinare $f(6)$.

(d) Sia $n = p^k$ con p primo e $k \in \mathbb{N}$. Dimostrare che $F(n) = n^{\frac{\tau(n)}{2}}$.

ESERCIZIO 6. **(a)** Enunciare la Legge di Reciprocità Quadratica nella forma generale, usando il simbolo di Jacobi.

(b) Calcolare il valore del seguente simbolo di Jacobi (spiegandone le modalità di calcolo):

$$\left(\frac{1121}{1212}\right) .$$

(c) Stabilire se la congruenza quadratica $X^2 - 1121 \equiv 0 \pmod{1212}$ è oppure non è risolubile.

Soluzioni

ESERCIZIO 1

(1, a&b) La risoluzione della congruenza data si riconduce

• alla risoluzione di una congruenza del tipo $Y^2 \equiv \Delta_\lambda \pmod{77}$, dove $\Delta_\lambda := \lambda^2 - 180 \equiv \lambda^2 - 26 \pmod{77}$ e, poi,

◦ alla risoluzione della congruenza $y \equiv 10X + \lambda \pmod{77}$, per ogni y soluzione della congruenza $Y^2 \equiv \Delta_\lambda \pmod{77}$.

• La congruenza $Y^2 \equiv \Delta_\lambda \equiv \lambda^2 - 26 \equiv \lambda^2 - 5 \pmod{7}$ è risolubile se e soltanto se

$$\left(\frac{\lambda^2 - 5}{7}\right) = 1 \text{ od anche } = 0$$

al variare di λ, con $0 \leq \lambda \leq 10$, cioè se e soltanto se $\lambda = 0, 3, 4$ e, quindi, anche per $\lambda = 7, 10$.

Precisamente, questa congruenza nella indeterminata Y è risolubile ed ha come soluzioni rispettivamente:
$\lambda = 0, 7 \rightsquigarrow \{3, 4\}$;
$\lambda = 3, 10 \rightsquigarrow \{2, 5\}$;
$\lambda = 4 \rightsquigarrow \{2, 5\}$.

• La congruenza $Y^2 \equiv \Delta_\lambda \equiv \lambda^2 - 26 \equiv \lambda^2 - 4 \pmod{11}$ è risolubile se e soltanto se

$$\left(\frac{\lambda^2 - 4}{11}\right) = 1 \text{ od anche } = 0$$

al variare di λ, con $0 \leq \lambda \leq 10$. A calcoli fatti, ciò accade se (e soltanto se) $\lambda = 2, 3, 4, 7, 8, 9$ (dove precisamente per $\lambda = 2, 9$ il simbolo di Legendre vale 0).

Questa congruenza nella indeterminata Y è risolubile ed ha come soluzioni rispettivamente:
$\lambda = 2, 9 \rightsquigarrow \{0\}$;
$\lambda = 3, 8 \rightsquigarrow \{4, 7\}$;
$\lambda = 4, 7 \rightsquigarrow \{1, 10\}$.

Pertanto,

•• la congruenza $Y^2 \equiv \lambda^2 - 26 \pmod{77}$ è risolubile per $\lambda = 3, 4, 7$ ed ha come soluzioni:
$\lambda = 3 \rightsquigarrow \{26, 37, 40, 51\}$;
$\lambda = 4 \rightsquigarrow \{12, 23, 54, 65\}$;
$\lambda = 7 \rightsquigarrow \{10, 32, 45, 67\}$.

◦ Per i valori sopra trovati, la congruenza $10X \equiv y - \lambda \pmod{77}$ è risolubile ed ha le seguenti soluzioni (che sono soluzioni della congruenza quadratica assegnata) e che sono rappresentate implicitamente da $X \equiv 54(y - \lambda) \pmod{77}$ (essendo 54 l'inverso aritmetico di 10 (mod 77)):
$\lambda = 3 \rightsquigarrow \{10, 51, 65, 73\}$;
$\lambda = 4 \rightsquigarrow \{5, 25, 47, 60\}$;
$\lambda = 7 \rightsquigarrow \{6, 8, 41, 50\}$.

ESERCIZIO 2

(2, a) $r = 2$ è una radice primitiva dell'unità (mod 13). La congruenza è risolubile se e soltanto se è risolubile la congruenza

$$8 \cdot X \equiv \mathrm{ind}_2(a) \pmod{12}$$

dove $8 = \text{ind}_2(9)$. Quindi, la congruenza data è risolubile se e soltanto se $4 \mid \text{ind}_2(a)$ e cioè se e soltanto se $a = 1, 3, 9$.

(2, b) Le soluzioni per $a = 1$ sono date da $0, 3, 6, 9 \pmod{12}$;
le soluzioni per $a = 3$ sono date da $2, 5, 8, 11 \pmod{12}$;
le soluzioni per $a = 9$ sono date da $1, 4, 7, 10 \pmod{12}$.

ESERCIZIO 3

(3, b) Modulo 17, si ha $\nu(7) = 3$ e $\nu(8) = 4$.

ESERCIZIO 4

(4, a) Si noti che $\varphi(18) = 6$. Si vede che nell'insieme degli interi relativamente primi con 18, $\{1, 5, 7, 11, 13, 17\}$, gli elementi 5 e 11 hanno ordine 6. Si vede anche che 7 ha ordine 3, 13 ha odine 3, 17 ha ordine 2 e, ovviamente, 1 ha ordine 1.

(4, b) Quindi, le radici primitive dell'unit (mod 18) –che sono in numero di $\varphi(\varphi(18)) = \varphi(6) = 2$– sono 5 ed 11.

(4, c) $r = 5$. Si calcola facilmente che:

$\text{ind}_5(1) = 6$;
$\text{ind}_5(5) = 1$;
$\text{ind}_5(7) = 2$;
$\text{ind}_5(11) = 5$;
$\text{ind}_5(13) = 4$;
$\text{ind}_5(17) = 3$.

(4, d) La congruenza data per $a \in \{1, 5, 7, 11, 13, 17\}$ è risolubile se e soltanto se è risolubile la congruenza $15Y \equiv \text{ind}_5(a) \pmod{6}$, cioè, se e soltanto se $3 \mid \text{ind}_5(a)$ ovvero per $a = 1, 17$.

(4, e) Si noti che per il teorema di Euler-Fermat risolvere la congruenza $X^{15} \equiv a \pmod{18}$ è equivalente a risolvere la congruenza $X^3 \equiv a \pmod{18}$. Questa congruenza è risolubile se e soltanto se sono risolubili, contemporaneamente, $X^3 \equiv a \pmod{2}$ e $X^3 \equiv a \pmod{9}$. La prima di queste è sempre risolubile, mentre $X^3 \equiv a \pmod{9}$ è risolubile se e soltanto se $a \equiv 0, 1, 8 \pmod{9}$. Pertanto, la congruenza $X^3 \equiv a \pmod{18}$ è risolubile se e soltanto se $a \in \{0, 1, 8, 9, 10, 17\}$, quando $0 \leq a \leq 18$.

(4, f)

Per $a = 1$, le soluzioni (mod 18) sono date da $x = 1, 7, 13$;
per $a = 17$, le soluzioni (mod 18) sono date da $x = 5, 11, 17$.

Inoltre,
per $a = 0$, le soluzioni (mod 18) sono date da $x = 0, 6, 12$;
per $a = 8$, le soluzioni (mod 18) sono date da $x = 2, 8, 14$;
per $a = 9$, le soluzioni (mod 18) sono date da $x = 3, 9, 15$;
per $a = 10$, le soluzioni (mod 18) sono date da $x = 4, 10, 16$.

ESERCIZIO 5

(5, a) $F(2) = 2, F(3) = 3$, ma $F(6) = 36$.

(5, b) $F(1) = 1 \neq 0$, dunque F è invertibile. Già abbiamo visto che $F(6) = 36$. Per calcolare $F^{-1}(6)$, notiamo che $0 = F * F^{-1}(6) = F(1)F^{-1}(6) + F(2)F^{-1}(3) + F(3)F^{-1}(2) + F(6)F^{-1}(1)$. Dato che $F(1) = 1$, si ha $F^{-1}(1) = 1/F(1) = 1$. Inoltre, $F(p) = p$ e $F^{-1}(p) = -p$ per un primo p , quindi $0 = F * F^{-1}(6) = F^{-1}(6) - 6 - 6 + 36$ e quindi $F^{-1}(6) = -24$.

(5, c) Dal fatto che $f = F * \mu$ si ricava che $f(6) = 1 \cdot 1 + 2 \cdot (-1) + 3 \cdot (-1) + 36 \cdot 1 = 32$.

(5, d) $F(p^k) = p \cdot p^2 \dots p^k = p^{1+2+\dots+k} = p^{\frac{k\cdot(k+1)}{2}} = (p^k)^{\frac{k+1}{2}} = n^{\frac{\tau(n)}{2}}$ (utilizzando il fatto che $\tau(p^k) = k+1$)).

ESERCIZIO 6

(6, b) $1212 = 4 \cdot 3 \cdot 101$. Quindi

$$\left(\frac{1121}{1212}\right) = \left(\frac{1121}{4}\right)\left(\frac{1121}{3}\right)\left(\frac{1121}{101}\right) = 1 \cdot \left(\frac{2}{3}\right)\left(\frac{10}{101}\right).$$

Dove

$$\left(\frac{2}{3}\right) = -1\,, \quad \left(\frac{10}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{5}{101}\right) = -1 \cdot 1 = -1\,.$$

Pertanto,

$$\left(\frac{1121}{1212}\right) = 1\,.$$

(6, c) La congruenza quadratica $X^2 - 1121 \equiv 0 \pmod{1212}$ non è risolubile, perché non è risolubile $X^2 - 1121 \equiv 0 \pmod 3$ (ed anche $X^2 - 1121 \equiv 0 \pmod{101}$ non è risolubile).