TN01 - Introduzione alla teoria dei numeri - A.A. 2002/2003
Valutazione "in itinere" - II Prova

MATRICOLA: ....
COGNOME: .... **NOME:** ....

ESERCIZIO 1.
(1) (**3pt**) Si determinino tutte le radici primitive $(\mathrm{mod}\ 13)$.
(2) (**3pt**) Se r è la radice primitiva minima positiva $(\mathrm{mod}\ 13)$, si determini $\mathrm{ind}_r(a)$ per ogni $1 \leq a \leq 12$.
(3) (**4pt**) Trovare per quali valori di a, con $1 \leq a \leq 12$, la congruenza:

$$3X^8 \equiv 2a \pmod{13},$$

è risolubile e
(4) (**2pt**) per il minimo di questi valori di a risolvere la congruenza data.

ESERCIZIO 2. (**3pt**) Determinare tutte le eventuali soluzioni dell'equazione diofantea:

$$9X^8 + 39Y = 3.$$

ESERCIZIO 3. (**7pt**) Determinare $(\mathrm{mod}\ 52)$ tutte le soluzioni della congruenza:

$$5^X \equiv X^7 \pmod{13}.$$

ESERCIZIO 4.
(1) (**3pt**) Calcolare il simbolo di Jacobi:

$$\left(\frac{42+\beta}{3731}\right)$$

per ogni β, con $0 \leq \beta \leq 2$;
(2) (**4pt**) Determinare le eventuali soluzioni della congruenza:

$$X^2 \equiv 43 \pmod{91}.$$

ESERCIZIO 5. Sia $*$ il prodotto di Dirichlet di funzioni aritmetiche e si ponga $F := \tau * \sigma^2$.
(1) (**3pt**) Enunciare la formula di inversione di Möbius.
(2) (**2pt**) Calcolare $F(28)$.
(3) (**3pt**) Sia f la funzione aritmetica determinata dalla formula di inversione di Möbius. Calcolare $f(28)$.

ESERCIZIO 6. (**3pt**) Se n è un intero positivo tale che $n \equiv 3 \pmod 4$, cosa possiamo dire sulla sua rappresentazione come somma di due quadrati?
(Il punteggio sarà assegnato solo se la risposta sarà adeguatamente motivata.)

SOLUZIONI

Soluzione Esercizio 1.

(1) Le radici primitive modulo 13 sono $2, 6, 7, 11$.

(2) Per $a = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$, abbiamo che
$$\operatorname{ind}_2(a) = 12, 1, 4, 2, 9, 5, 11, 3, 8, 10, 7, 6.$$

(3) La congruenza è risolubile per i valori di a tali che $\operatorname{ind}_2(a) - 3 \equiv 0 \pmod 4$, cioè per $a = 7, 8, 11$.

(4) Per $a = 7$, la congruenza diventa $3X^8 \equiv 1 \pmod{13}$. Le soluzioni della congruenza sono $X \equiv 2, 3, 10, 11 \pmod{13}$.

Soluzione Esercizio 2. L'equazione diofantea data è equivalente all'equazione diofantea $3X^8 + 13Y = 3$. Basta, quindi, trovare le soluzioni di quest'ultima. Osserviamo che se (x, y) è una soluzione dell'equazione diofantea data, allora x deve soddisfare la congruenza: $3X^8 \equiv 1 \pmod{13}$, che è proprio la congruenza studiata nell'esercizio precedente. Quindi $x = 2 + 13k$ oppure $x = 3 + 13h$, oppure $x = 10 + 13s$, oppure $x = 11 + 13t$, con $k, h, s, t \in \mathbb{Z}$. Il corrispondente valore della y si ricava dall'equazione stessa. Quindi tutte le soluzioni dell'equazione sono date dai seguenti insiemi: $\{(2+13k, \frac{1-3(2+13k)^8}{13}), k \in \mathbb{Z}\}$, $\{(3+13h, \frac{1-3(3+13h)^8}{13}), h \in \mathbb{Z}\}$, $\{(10 + 13s, \frac{1-3(10+13s)^8}{13}), s \in \mathbb{Z}\}$, $\{(11 + 13t, \frac{1-3(11+13t)^8}{13}), t \in \mathbb{Z}\}$.

Soluzione Esercizio 3.

Scegliamo $r = 2$ come radice primitiva $\pmod{13}$. Le soluzioni della congruenza sono le soluzioni del sistema:

$$\begin{cases} X \equiv a \pmod{17} \\ X \operatorname{ind}_2(5) \equiv 7 \operatorname{ind}_2(a) \pmod{16}. \end{cases}$$

La seconda equazione del sistema è risolubile se e soltanto se $\operatorname{ind}_2(a) \equiv 0 \pmod 3$. Questo avviene se e soltanto se $a \equiv 1, 5, 8, 12 \pmod{13}$. In corrispondenza di questi valori di a, le soluzioni della congruenza sono $x \equiv 21, 31, 38, 40 \pmod{52}$.

Soluzione Esercizio 4. Si ha che $3731 = 7 \cdots 13 \cdot 41$.

(1) per $\beta = 0$, si ha $(\frac{42}{3731}) = 0$, per $\beta = 1$, si ha $(\frac{43}{3731}) = 0$ ed infine per $\beta = 2$, si ha $(\frac{43}{3731}) = 1$.

(2) Poiché $91 = 7 \cdot 13$, la congruenza data è risolubile se e soltanto se $(\frac{43}{7}) = 1$ e $(\frac{43}{13}) = 1$. Questo avviene, quindi la congruenza è risolubile ed ammette 4 soluzioni distinte: $x \equiv 15, 41, 50, 76 \pmod{91}$.

Soluzione Esercizio 5.

(2) $F(28) = \tau(28)+\tau(14)\sigma^2(2)+\tau(7)\sigma^2(4)+\tau(4)\sigma^2(7)+\tau(2)\sigma^2(14)+\sigma^2(28) = 6 + 4 \cdot 5 + 2 \cdot 21 + 3 \cdot 50 + 2 \cdot 196 + 1050 = 1768$.

(3) $f(28) = \mu(28) + F(2)\mu(14) + F(4)\mu(7) + F(7)\mu(4) + F(14)\mu(2) + F(28) = 0 + 7 - 34 + 0 - 364 + 1768 = 1377$.

Soluzione Esercizio 6.

Si verifica che se $n \equiv 3 \pmod 4$ allora n possiede un fattore primo, non quadratico, che è congruente a 3 modulo 4. Per il Teorema di rappresentazione degli interi come somma di due quadrati, n non è somma di due quadrati interi.