TN1 - Introduzione alla teoria dei numeri - A.A. 2006/2007
Valutazione "in itinere" - II Prova

MATRICOLA/IDENTIFICATIVO PERSONALE: .....
COGNOME: ..... **NOME:** .....

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

ESERCIZIO 1. (a) Determinare per quali valori del parametro λ, $0 \leq \lambda \leq 12$, la seguente congruenza è risolubile:

$$9X^2 + (4 - 12\lambda)X + \lambda^2 - 8\lambda + 4 \equiv 0 \pmod{13}.$$

(b) Per ogni valore di λ per il quale la congruenza in **(a)** è risolubile determinare tutte le sue soluzioni.

ESERCIZIO 2. Sia p un primo dispari e siano $a, b \in \mathbb{Z}$ due interi non nulli tali che $\mathrm{MCD}(a, p) = \mathrm{MCD}(b, p) = 1$.

(a) Dimostrare che

$$aX^2 \equiv b \pmod{p} \text{ è risolubile} \quad \Leftrightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) .$$

(b) Determinare tutti gli interi $a \pmod 7$ per i quali la conguenza $aX^2 \equiv -2 \pmod 7$ è risolubile.

ESERCIZIO 3. **(a)** Mostrare che le seguenti congruenze:

(i) $X^2 + (X+1)^2 + (X+2)^2 \equiv 0 \pmod{10}$, **(ii)** $(X+1)^2 \equiv 6 \pmod{10}$

sono equivalenti (cioè, un intero $a \in \mathbb{Z}$ è soluzione di **(i)** se e soltanto se a è soluzione di **(ii)**).

[Suggerimento: determinare due interi α e β in modo tale che si possa scrivere $X^2 + (X+1)^2 + (X+2)^2 = \alpha(X+1)^2 + \beta$.]

(b) Utilizzando il punto **(a)**, determinare tutti gli interi naturali multipli di 10 che si possono scrivere come somma di tre quadrati di interi consecutivi.

[Suggerimento: utilizzare le soluzioni di **(ii)** *(notare che, ad esempio, $50 = 3^2 + 4^2 + 5^2$ e $110 = 5^2 + 6^2 + 7^2$ dove 3 e 5 sono tra le soluzioni di* **(ii)***)].*

ESERCIZIO 4. **(a)** Enunciare la Legge di Reciprocità Quadratica nella forma generale, usando il simbolo di Jacobi.

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

$$\left(\frac{401}{444}\right) .$$

(c) Stabilire se la congruenza quadratica $X^2 - 401 \equiv 0 \pmod{444}$ è oppure non è risolubile.

ESERCIZIO 5. (a) Determinare la più piccola radice primitiva positiva $r \pmod{23}$ con $1 \leq r \leq 22$.

(b) Determinare la tabella degli indici rispetto alla radice primitiva positiva minima r modulo 23.

(c) Determinare per quali valori del parametro μ, $0 \leq \mu \leq 22$, la seguente equazione diofantea è risolubile:

$$6X^4 - 23Y - \mu = 0\,.$$

(d) Per il più piccolo valore di μ *positivo* ($\mu \neq 0$) per il quale l'equazione diofantea data in **(c)** è risolubile determinare tutte le infinite coppie $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ che sono soluzioni di tale equazione diofantea.
In particolare, per il più piccolo intero positivo $\bar{x}$ tale che $(\bar{x}, \bar{y})$ è soluzione, determinare esplicitamente $\bar{y}$.

ESERCIZIO 6. **(a)** Scrivere 14985 come somma di due quadrati.

(b) Determinare due terne pitagoriche diverse (x_1, y_1, z) e (x_2, y_2, z) con $z = 14985$.

Soluzioni

1. La congruenza data si riconduce alla risoluzione di una congruenza del tipo $Y^2 \equiv \Delta_\lambda \pmod{13}$, dove $\Delta_\lambda := 108\lambda^2 + 192\lambda - 128 \equiv 4\lambda^2 + 10\lambda + 2 \pmod{13}$. Questa congruenza nella indeterminata Y è risolubile per $\lambda = 1, 2, 3, 5, 8, 9, 12$ ed ha come soluzioni rispettivamente $\{4, 9\}$; $\{5, 8\}$; $\{4, 9\}$; $\{3, 10\}$; $\{0\}$; $\{0\}$; $\{3, 10\}$.

Avendo posto $Y := 18X + (4 - 12\lambda)$, si ricava che la congruenza data (nella indeterminata X) è risolubile per i valori di $\lambda = 1, 2, 3, 5, 8, 9, 12$ (determinati sopra) ed ha come soluzioni rispettivamente $\{5, 6\}$; $\{3, 5\}$; $\{2, 3\}$; $\{4, 8\}$; $\{8\}$; $\{0\}$; $\{0, 4\}$.

2. (a) Se a^* è l'inverso aritmetico di $a \pmod{p}$, allora $X^2 \equiv a^*b \pmod{p}$ è risolubile se esoltanto se $\left(\frac{a^*b}{p}\right) = 1$ se e soltanto se $\left(\left(\frac{a^*}{p}\right) =\right) \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(b) E' risolubile per $a = 3, 5, 6$ ed ha come soluzioni (mod 7) rispettivamente $\{2, 5\}$; $\{1, 6\}$; $\{3, 4\}$.

3. (a) Si noti che $X^2 + (X+1)^2 + (X+2)^2 = 3(X+1)^2 + 2$ e che $3(X+1)^2 + 2 \equiv 0 \pmod{10}$ è equivalente a $(X+1)^2 - 6 \equiv 0 \pmod{10}$.

$(X+1)^2 \equiv 6 \pmod{2}$ ha come soluzione 1 (mod 2);

$(X+1)^2 \equiv 6 \pmod{5}$ ha come soluzioni 0, 3 (mod 5); $(X+1)^2 \equiv 6 \pmod{10}$ ha come soluzioni 3, 5 (mod 10).

(b) Da (a) deduciamo che, per $x'_k := 3 + k \cdot 10$ e $x''_h := 5 + h \cdot 10$, al variare comunque di $k, h \in \mathbb{Z}$, si ha:

$(x'_k)^2 + (x'_k + 1)^2 + (x'_k + 2)^2 = t_k \cdot 10$, per qualche intero t_k,

$(x''_h)^2 + (x''_h + 1)^2 + (x''_h + 2)^2 = s_h \cdot 10$, per qualche intero s_h.

4. (b) $\left(\frac{401}{444}\right) = \left(\frac{401}{4\cdot 111}\right) = \left(\frac{401}{111}\right) = \left(\frac{68}{111}\right) = \left(\frac{4\cdot 17}{111}\right) = \left(\frac{17}{111}\right) = \left(\frac{17}{3\cdot 37}\right) = \left(\frac{17}{3}\right)\left(\frac{17}{37}\right) = \left(\frac{2}{3}\right)\left(\frac{37}{17}\right) = \left(\frac{2}{3}\right)\left(\frac{3}{17}\right) = \left(\frac{2}{3}\right)\left(\frac{17}{3}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{3}\right) = (-1)\cdot(-1) = 1$.

(c) Non è risolubile, perché non è risolubile $X^2 - 401 \equiv 0 \pmod{3}$ ovvero $X^2 - 2 \equiv 0 \pmod{3}$.

5. (a) $r = 5$. le altre radici primitive sono date da r^k, con $\mathrm{MCD}(k, 22) = 1$, e cioè sono date rispettivamente da: 10, 20, 17, 11, 21, 19, 15, 7, 14.

(b) $(a, \mathrm{ind}_5(a)) = (1, 22)$, $(5, 1)$, $(2, 2)$, $(10, 3)$, $(4, 4)$, $(20, 5)$, $(8, 6)$, $(17, 7)$, $(16, 8)$, $(11, 9)$, $(9, 10)$, $(22, 11)$, $(18, 12)$, $(21, 13)$, $(13, 14)$, $(19, 15)$, $(3, 16)$, $(15, 17)$, $(6, 18)$, $(7, 19)$, $(12, 20)$, $(14, 21)$.

(c) La congruenza $6X^4 \equiv \mu \pmod{23}$ ovvero $X^4 \equiv 4\mu \pmod{23}$ è risolubile se e soltanto se $\mathrm{MCD}(4, 22) = 2$ divide $\mathrm{ind}_5(4\mu)$.

La conguenza data è risolubile per $\mu = 0, \mathbf{1}, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18$ ed ha per soluzioni, rispettivamente, 0; $\mathbf{\{5, 18\}}$; $\{6, 17\}$; $\{3, 20\}$; $\{2, 21\}$; $\{1, 22\}$; $\{7, 16\}$; $\{11, 12\}$; $\{8, 15\}$; $\{9, 14\}$; $\{10, 13\}$; $\{4, 19\}$.

(d) Le soluzioni sono $x_k = 5 + k \cdot 23$, $y_k = \frac{6(5+k\cdot 23)^4 - 1}{23}$ e $x'_h = 18 + h \cdot 23$, $y'_h = \frac{6(18+h\cdot 23)^4 - 1}{23}$; al variare di $k, h \in \mathbb{Z}$.

Per $k = 0$, $\bar{x} = x_0$ è minimo tra gli interi positivi che sono soluzioni, e $(\bar{x}, \bar{y}) = (x_0, y_0) = (5, 163)$ è la soluzione richiesta.

6. (a) $14985 = 3^4 \cdot 37 \cdot 5$ è somma di due quadrati perché $5 \equiv 37 \equiv 1$ modulo 4. Non è difficile mostrare che $14985 = 99^2 + 72^2 = 117^2 + 36^2$.

(b) $(14256, 4617, 14985)$ e $(8424, 12393, 14985)$ sono due terne pitagoriche che si ottengono da (a) e dalle espressioni parametriche delle terne pitagoriche.

TN1 - Introduzione alla teoria dei numeri - A.A. 2006/2007
Valutazione "in itinere" - II Prova

MATRICOLA/IDENTIFICATIVO PERSONALE: .....
COGNOME: ..... **NOME:** .....

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

ESERCIZIO 1. **(a)** Determinare per quali valori del parametro μ, $0 \leq \mu \leq 12$, la seguente congruenza è risolubile:

$$9X^2 + (3 - 12\mu)X + \mu^2 - 10\mu \equiv 0 \pmod{13}.$$

(b) Per ogni valore di μ per il quale la congruenza in **(a)** è risolubile determinare tutte le sue soluzioni.

ESERCIZIO 2. **(a)** Mostrare che le seguenti congruenze:

(i) $X^2 + (X+1)^2 + (X+2)^2 \equiv 0 \pmod{10}$, **(ii)** $(X+1)^2 \equiv 6 \pmod{10}$

sono equivalenti (cioè, un intero $a \in \mathbb{Z}$ è soluzione di **(i)** se e soltanto se a è soluzione di **(ii)**).
[Suggerimento: determinare due interi α e β in modo tale che si possa scrivere $X^2 + (X+1)^2 + (X+2)^2 = \alpha(X+1)^2 + \beta$.]

(b) Utilizzando il punto **(a)**, determinare tutti gli interi naturali multipli di 10 che si possono scrivere come somma di tre quadrati di interi consecutivi.
[Suggerimento: utilizzare le soluzioni di **(ii)** *(notare che, ad esempio, $50 = 3^2 + 4^2 + 5^2$ e $110 = 5^2 + 6^2 + 7^2$ dove 3 e 5 sono tra le soluzioni di* **(ii)***)].*

ESERCIZIO 3. Sia p un primo dispari e siano $a, b \in \mathbb{Z}$ due interi non nulli tali che $\mathrm{MCD}(a, p) = \mathrm{MCD}(b, p) = 1$.

(a) Dimostrare che

$$aX^2 \equiv b \pmod{p} \text{ è risolubile} \quad \Leftrightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) .$$

(b) Determinare tutti gli interi $a \pmod 7$ per i quali la conguenza $aX^2 \equiv -2 \pmod 7$ è risolubile.

ESERCIZIO 4. **(a)** Enunciare la Legge di Reciprocità Quadratica nella forma generale, usando il simbolo di Jacobi.

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

$$\left(\frac{512}{111}\right) .$$

(c) Stabilire se la congruenza quadratica $X^2 - 512 \equiv 0 \pmod{111}$ è oppure non è risolubile.

ESERCIZIO 5. (a) Determinare la più piccola radice primitiva positiva $r \pmod{23}$ con $1 \leq r \leq 22$.

(b) Determinare la tabella degli indici rispetto alla radice primitiva positiva minima r modulo 23.

(c) Determinare per quali valori del parametro λ, $0 \leq \lambda \leq 22$, la seguente equazione diofantea è risolubile:

$$4X^4 - 23Y - \lambda = 0\,.$$

(d) Per il più piccolo valore di λ *positivo* ($\lambda \neq 0$) per il quale l'equazione diofantea data in **(c)** è risolubile determinare tutte le infinite coppie $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ che sono soluzioni di tale equazione diofantea.
In particolare, per il più piccolo intero positivo $\bar{x}$ tale che $(\bar{x}, \bar{y})$ è soluzione, determinare esplicitamente $\bar{y}$.

ESERCIZIO 6. **(a)** Scrivere 16605 come somma di due quadrati.

(b) Determinare due terne pitagoriche diverse (x_1, y_1, z) e (x_2, y_2, z) con $z = 16605$.

Soluzioni

1. Per maggiori dettagli teorici su questo esercizio si consiglia di vedere la soluzione dell'Esercizio 1 dell'altra versione della prova.

La congruenza data è risolubile per $\mu = 0, 2, 3, 4, 6, 9, 10$ ed ha come soluzioni rispettivamente $\{0, 4\}$; $\{5, 6\}$; $\{3, 5\}$; $\{2, 3\}$; $\{4, 8\}$; $\{8\}$; $\{0\}$.

2. (a) Si noti che $X^2+(X+1)^2+(X+2)^2 = 3(X+1)^2+2$ e che $3(X+1)^2+2 \equiv 0 \pmod{10}$ è equivalente a $(X+1)^2 - 6 \equiv 0 \pmod{10}$.

$(X+1)^2 \equiv 6 \pmod 2$ ha come soluzione $1 \pmod 2$;

$(X+1)^2 \equiv 6 \pmod 5$ ha come soluzioni $0, 3 \pmod 5$; $(X+1)^2 \equiv 6 \pmod{10}$ ha come soluzioni $3, 5 \pmod{10}$.

(b) Da (a) deduciamo che, per $x'_k := 3 + k \cdot 10$ e $x''_h := 5 + h \cdot 10$, al variare comunque di $k, h \in \mathbb{Z}$, si ha:

$(x'_k)^2 + (x'_k + 1)^2 + (x'_k + 2)^2 = t_k \cdot 10$, per qualche intero t_k,

$(x''_h)^2 + (x''_h + 1)^2 + (x''_h + 2)^2 = s_h \cdot 10$, per qualche intero s_h.

3. (a) Se a^* è l'inverso aritmetico di $a \pmod p$, allora $X^2 \equiv a^*b \pmod p$ è risolubile se esoltanto se $\left(\frac{a^*b}{p}\right) = 1$ se e soltanto se $\left(\left(\frac{a^*}{p}\right) =\right) \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(b) E' risolubile per $a = 3, 5, 6$ ed ha come soluzioni (mod 7) rispettivamente $\{2, 5\}$; $\{1, 6\}$; $\{3, 4\}$.

4. (b) $\left(\frac{512}{111}\right) = \left(\frac{68}{111}\right) = \left(\frac{4\cdot 17}{111}\right) = \left(\frac{17}{111}\right) = \left(\frac{17}{3\cdot 37}\right) = \left(\frac{17}{3}\right)\left(\frac{17}{37}\right) = \left(\frac{2}{3}\right)\left(\frac{37}{17}\right) = \left(\frac{2}{3}\right)\left(\frac{3}{17}\right) = \left(\frac{2}{3}\right)\left(\frac{17}{3}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{3}\right) = (-1)\cdot(-1) = 1$.

(c) Non è risolubile, perché non è risolubile $X^2 - 512 \equiv 0 \pmod 3$ (notare che $3 \mid 512$) ovvero $X^2 - 2 \equiv 0 \pmod 3$.

5. (a) $r = 5$. le altre radici primitive sono date da r^k, con $\mathrm{MCD}(k, 22) = 1$, e cioè sono date rispettivamente da: 10, 20, 17, 11, 21, 19, 15, 7, 14.

(b) $(a, \mathrm{ind}_5(a))$ = (1, 22), (5, 1), (2, 2), (10, 3), (4, 4), (20, 5), (8, 6), (17, 7), (16, 8), (11, 9), (9, 10), (22, 11), (18, 12), (21, 13), (13, 14), (19, 15), (3, 16), (15, 17), (6, 18), (7, 19), (12, 20), (14, 21).

(c) La congruenza $4X^4 \equiv \lambda \pmod{23}$ ovvero $X^4 \equiv 6\lambda \pmod{23}$ è risolubile se e soltanto se $\mathrm{MCD}(4, 22) = 2$ divide $\mathrm{ind}_5(6\lambda)$.

La conguenza data è risolubile per $\lambda = 0, \mathbf{1}, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18$ ed ha per soluzioni, rispettivamente, 0; $\mathbf{\{9, 14\}}$; $\{3, 20\}$; $\{10, 13\}$; $\{1, 22\}$; $\{11, 12\}$; $\{8, 15\}$; $\{6, 17\}$; $\{4, 19\}$; $\{7, 16\}$; $\{5, 18\}$; $\{2, 21\}$.

(d) Le soluzioni sono $x_k = 9 + k \cdot 23$, $y_k = \frac{4(9+k\cdot 23)^4-1}{23}$ e $x'_h = 14 + h \cdot 23$, $y'_h = \frac{4(14+h\cdot 23)^4-1}{23}$; al variare di $k, h \in \mathbb{Z}$.

Per $k = 0$, $\bar{x} = x_0$ è minimo tra gli interi positivi che sono soluzioni, e $(\bar{x}, \bar{y}) = (x_0, y_0) = (9, 1141)$ è la soluzione richiesta.

6. (a) $16605 = 3^4 \cdot 41 \cdot 5$ è somma di due quadrati perché $5 \equiv 41 \equiv 1$ modulo 4. Non è difficile mostrare che $16605 = 54^2 + 117^2 = 126^2 + 27^2$.

(b) $(12636, 10773, 16605)$ e $(6804, 15147, 16605)$ sono due terne pitagoriche che si ottengono da (a) e dalle espressioni parametriche delle terne pitagoriche.