TN1 - Introduzione alla teoria dei numeri - A.A. 2006/2007

Esame: Appello C - Gennaio 2008

MATRICOLA/IDENTIFICATIVO PERSONALE: .....

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

esercizio	1	2		3		4			5	6	7	
punteggio max	10	3	4	4	2	5	5	8	5	5	4	4
punteggio assegnato												
totale												

ESERCIZIO 1. Enunciare e dimostrare il teorema fondamentale sulle terne pitagoriche primitive (teorema che descrive esplicitamente tutte le terne pitagoriche primitive).

ESERCIZIO 2. **(a)** Trovare la radice primitiva minima positiva per $p = 13$.

(b) Ricordando che $X^6 - 1 = (X - 1)(1 + X + X^2 + X^3 + X^4 + X^5)$, trovare, se esistono, le soluzioni della congruenza:

$$1 + X + X^2 + X^3 + X^4 + X^5 \equiv 0 \pmod{13}.$$

ESERCIZIO 3. Si consideri il seguente sistema di congruenze lineari in due indeterminate:

$$\begin{cases} 3X + 7\lambda Y \equiv 3 \pmod{19} \\ -2X + 14Y \equiv 9 \pmod{19}\,. \end{cases}$$

(a) Determinare, al variare di λ, con $0 \leq \lambda \leq 18$, quando e quali tra i seguenti casi si verificano (mod 19): il sistema è risolubile ed ammette un'unica soluzione; il sistema è risolubile ed ammette più di una soluzione; il sistema non è risolubile.
(b) Determinare esplicitamente le eventuali soluzioni del sistema per $\lambda = 1$.

ESERCIZIO 4. Sia p un primo dispari e sia a un intero coprimo con p. Dimostrare le seguenti affermazioni:

(a) $a^d \not\equiv 1 \pmod{p}$ per ogni divisore proprio d di $p-1$ se e soltanto se $a^{\frac{p-1}{d}} \not\equiv 1 \pmod{p}$ per ogni divisore proprio d di $p-1$;

(b) Se m è un divisore di $p-1$ e q è un primo tale che $q \mid m$, allora $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$ implica anche che $a^{\frac{p-1}{m}} \not\equiv 1 \pmod{p}$;

(c) a è una radice primitiva di p se e soltanto se $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$, per ogni divisore primo di $p-1$.

ESERCIZIO 5. Determinare tutte le (eventuali) soluzioni della congruenza polinomiale:

$$f(X) := X^5 + 10X^4 - 4X^3 + 5X^2 - 23X + 36 \equiv 0 \pmod{45 \quad (= 3^2 \cdot 5)}\,.$$

ESERCIZIO 6. Trovare tutte le eventuali soluzioni della congruenza

$$25X^2 - 10\lambda X + \lambda^2 - \lambda \equiv 0 \pmod{13},$$

al variare di λ, $0 \leq \lambda \leq 12$.

ESERCIZIO 7. **(a)** Determinare per quali interi a, $1 \leq a \leq 20$, relativamente primi con 21 il seguente simbolo di Jacobi vale 1:

$$\left(\frac{a}{21}\right).$$

(b) Determinare per quali interi a, $1 \leq a \leq 20$, relativamente primi con 21 la congruenza quadratica $X^2 - a \equiv 0 \pmod{21}$ è risolubile.

ESERCIZIO 2. Soluzione.

(a) 2 è una radice primitiva di 13. Precisamente,
Per $a = 1, 2, 3, \ldots, 12$ si ha, rispettivamente, che
$\mathrm{ind}_2(a) = 12, 1, 4, 2, 9, 5, 11, 3, 8, 10, 7, 6$.

(b) Osserviamo che $X^6 - 1 = (X-1)(1 + X + X^2 + X^3 + X^4 + X^5)$. Dunque le soluzioni della congruenza data sono tutte le soluzioni, diverse da 1, della congruenza $X^6 - 1 \equiv 0 \pmod{13}$, le quali si ottengono risolvendo la congruenza (nell'incognita $Y := \mathrm{ind}_2(X)$):

$$6Y \equiv 0 \pmod{12} \text{ ovvero } Y \equiv 0 \pmod{2}.$$

Le soluzioni non banali sono $y \equiv 2, 4, 6, 8, 10 \pmod{12}$ e, quindi, le soluzioni della congruenza data sono $x \equiv 4, 3, 12, 9, 10 \pmod{13}$.

ESERCIZIO 3: Soluzione.

(a) Abbiamo che $\Delta \equiv 14\lambda + 3 \cdot 14 \pmod{19}$. Il sistema ammette un'unica soluzione per $\Delta \not\equiv 0 \pmod{19}$ ovvero per $\lambda \not\equiv 16 \pmod{19}$. Mentre per $\lambda \equiv 16 \pmod{19}$ il sistema non è risolubile.

(b) Per $\lambda = 1$, $\Delta \equiv 1 \pmod{19}$, pertanto l'unica soluzione del sistema è data da $(2, 5) \pmod{19}$.

ESERCIZIO 4: Soluzione.

(a) basta osservare che se d è un divisore proprio di $p-1$, allora anche $\frac{p-1}{d}$ è un divisore proprio di $p-1$ e viceversa.

(b) Sia $q \mid m$. Poiché $\frac{p-1}{m} \mid \frac{p-1}{q}$, si ha che se $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$, allora anche $a^{\frac{p-1}{m}} \not\equiv 1 \pmod{p}$.

(c) Un intero a coprimo con p è una radice primitiva di p se e soltanto se $a^d \not\equiv 1 \pmod{p}$, per ogni divisore proprio d di $p-1$.
Per il punto **(a)** questo è equivalente a chiedere che $a^{\frac{p-1}{d}} \not\equiv 1 \pmod{p}$, per ogni divisore proprio d di $p-1$.
Fissiamo un divisore proprio d di $p-1$. Se q è un primo che divide d, allora $q \mid p-1$. Assumiamo, per ipotesi, che $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$. Dal punto **(b)** segue che $a^{\frac{p-1}{d}} \not\equiv 1 \pmod{p}$. Quindi a è una radice primitiva di p. Il viceversa è banale.

ESERCIZIO 5: Soluzione.

$f(X) \equiv 0 \pmod{3} \longrightarrow x \equiv 0 \pmod{3}$;
$f(X) \equiv 0 \pmod{9} \longrightarrow x \equiv 0 \pmod{9}$;
$f(X) \equiv 0 \pmod{5} \longrightarrow x \equiv 1, 2 \pmod{5}$;
$f(X) \equiv 0 \pmod{45} \longrightarrow x \equiv 27, 36 \pmod{45}$.

ESERCIZIO 6: Soluzione. Basta risolvere la congruenza $Y^2 \equiv \lambda \pmod{13}$, dove $Y := 5X - \lambda$. Questa congruenza è risolubile per $\lambda = 0, 1, 3, 4, 9, 10, 12$ e le soluzioni rispettive per questi valori di λ sono $y_1 = 0, 1, 4, 2, 3, 6, 5$ e $y_2 = 0, 12, 9, 11, 10, 7, 8$. Dunque, le soluzioni della congruenza data sono le seguenti:

Per $\lambda = 0 \rightarrow x = 0, 0$;
Per $\lambda = 1 \rightarrow x = 0, 3$;
Per $\lambda = 3 \rightarrow x = 4, 5$;
Per $\lambda = 4 \rightarrow x = 3, 9$;
Per $\lambda = 9 \rightarrow x = 5, 9$;
Per $\lambda = 10 \rightarrow x = 6, 11$;

Per $\lambda = 12 \;\rightarrow\; x = 4, 6$.

ESERCIZIO 7: Soluzione.

(a) Si calcola agevolmente che
$\left(\frac{1}{3}\right) = 1 \;, \left(\frac{1}{7}\right) = 1 \;, \left(\frac{1}{21}\right) = 1 \;\blacktriangleleft$.
$\left(\frac{2}{3}\right) = -1 \;, \left(\frac{2}{7}\right) = 1 \;, \left(\frac{2}{21}\right) = -1$.
$\left(\frac{4}{3}\right) = 1 \;, \left(\frac{4}{7}\right) = 1 \;, \left(\frac{4}{21}\right) = 1 \;\blacktriangleleft$.
$\left(\frac{5}{3}\right) = -1 \;, \left(\frac{5}{7}\right) = -1 \;, \left(\frac{5}{21}\right) = 1 \;\bullet$.
$\left(\frac{8}{3}\right) = -1 \;, \left(\frac{8}{7}\right) = 1 \;, \left(\frac{8}{21}\right) = -1$.
$\left(\frac{10}{3}\right) = 1 \;, \left(\frac{10}{7}\right) = \left(\frac{3}{7}\right) = -1 \;, \left(\frac{10}{21}\right) = -1$.
$\left(\frac{11}{3}\right) = -1 \;, \left(\frac{11}{7}\right) = 1 \;, \left(\frac{11}{21}\right) = -1$.
$\left(\frac{13}{3}\right) = 1 \;, \left(\frac{13}{7}\right) = -1 \;, \left(\frac{13}{21}\right) = -1$.
$\left(\frac{16}{3}\right) = 1 \;, \left(\frac{16}{7}\right) = 1 \;, \left(\frac{16}{21}\right) = 1 \;\blacktriangleleft$.
$\left(\frac{17}{3}\right) = -1 \;, \left(\frac{17}{7}\right) = -1 \;, \left(\frac{17}{21}\right) = 1 \;\bullet$.
$\left(\frac{19}{3}\right) = 1 \;, \left(\frac{19}{7}\right) = -1 \;, \left(\frac{19}{21}\right) = -1$.
$\left(\frac{20}{3}\right) = -1 \;, \left(\frac{20}{7}\right) = -1 \;, \left(\frac{20}{21}\right) = 1 \;\bullet$.

(b) Se $1 \leq a \leq 20$ e $\mathrm{MCD}(a, 21) = 1$, da quanto sopra si ricava che $X^2 - a \equiv 0 \pmod{20}$ è risolubile se e soltanto se $a \equiv 1, 4, 16 \pmod{21}$.

Per $a = 1$, l'insieme delle soluzioni (mod 21) è dato da $\{1, 8, 13, 20\}$.

Per $a = 4$, l'insieme delle soluzioni (mod 21) è dato da $\{2, 5, 16, 19\}$.

Per $a = 16$, l'insieme delle soluzioni (mod 21) è dato da $\{4, 10, 11, 17\}$.

Si noti anche che la congruenza $X^2 - a \equiv 0 \pmod{21}$ è anche risolubile per altri valori di a non relativamente primi con 21 e cioè $a \equiv 0, 7, 9, 15, 18 \pmod{21}$.

Per $a = 0$, l'insieme delle soluzioni (mod 21) è dato da $\{0\}$.

Per $a = 7$, l'insieme delle soluzioni (mod 21) è dato da $\{7, 14\}$.

Per $a = 9$, l'insieme delle soluzioni (mod 21) è dato da $\{3, 18\}$.

Per $a = 15$, l'insieme delle soluzioni (mod 21) è dato da $\{6, 15\}$.

Per $a = 18$, l'insieme delle soluzioni (mod 21) è dato da $\{9, 12\}$.