TN1 - Introduzione alla teoria dei numeri - A.A. 2009/2010

Esame: Appello C (ultima sessione) - Gennaio 2011

MATRICOLA/IDENTIFICATIVO PERSONALE: .....

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

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

ESERCIZIO 1. 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 $d > 0$ 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 $m > 0$ 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 2. Determinare tutte le (eventuali) soluzioni della congruenza polinomiale:

$$f(X) := X^5 + 4X^3 + 5X^2 - 23X + 55 \equiv 0 \pmod{63 \ \ (= 3^2 \cdot 7)}\,.$$

ESERCIZIO 3. **(a)** Enunciare il teorema fondamentale sulle terne pitagoriche primitive (teorema che descrive esplicitamente, in forma parametrica, tutte le terne pitagoriche primitive).

(b) Dimostrare il teorema fondamentale sulle terne pitagoriche primitive.

ESERCIZIO 4. **(a)** Determinare per quali valori di λ, $0 \leq \lambda \leq 16$, la congruenza

$$9X^2 - 6\lambda X + \lambda^2 - \lambda \equiv 0 \pmod{17}$$

è risolubile.

(b) Per ogni valore di λ per il quale la congruenza in (a) è risolubile (od almeno per almeno quattro di tali valori di $\lambda \neq 0$), determinarne tutte le soluzioni (mod 17).

ESERCIZIO 5. **(a)** Enunciare la formula di inversione di Möbius.
(b) Dimostrare la formula di inversione di Möbius.

ESERCIZIO 6. **(a)** Determinare per quali interi a, $1 \leq a \leq 32$, relativamente primi con 33 il seguente simbolo di Jacobi vale 1:

$$\left(\frac{a}{33}\right).$$

(b) Determinare per quali interi a, $1 \leq a \leq 32$, relativamente primi con 33 la congruenza quadratica $X^2 - a \equiv 0 \pmod{33}$ è risolubile.

ESERCIZIO 7. **(a)** Definire la funzione φ di Euler.
(b) Dimostrare che la funzione φ di Euler è moltiplicativa.
(c) Enunciare il Teorema di Euler-Fermat.
(d) Dimostrare il Teorema di Euler-Fermat

ESERCIZIO 1: 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 2: Soluzione.

$f(X) \equiv 0 \pmod 3 \longrightarrow x \equiv 1,\ 2 \pmod 3$;
$f(X) \equiv 0 \pmod 9 \longrightarrow x \equiv 4,\ 5 \pmod 9$;
$f(X) \equiv 0 \pmod 7 \longrightarrow x \equiv 1,\ 4 \pmod 7$;
$f(X) \equiv 0 \pmod{63} \longrightarrow x \equiv 4,\ 22,\ 32,\ 50 \pmod{63}$.

ESERCIZI 3, 5, 7: Soluzioni. Vedere gli appunti delle lezioni.

ESERCIZIO 4: Soluzione. Basta risolvere la congruenza $Y^2 \equiv \lambda \pmod{17}$, dove $Y := 3X - \lambda$. Questa congruenza è risolubile per $\lambda = 0, 1, 2, 4, 8, 9, 13, 15, 16$.

Le soluzioni (mod 17) della congruenza data sono le seguenti:

Per $\lambda = 0 \ \rightarrow \ y = 0 \ \rightarrow \ x = 0$;
Per $\lambda = 1 \ \rightarrow \ y = 1, 16 \ \rightarrow \ x = 0, 12$;
Per $\lambda = 2 \ \rightarrow \ y = 6, 11 \ \rightarrow \ x = 10, 14$;
Per $\lambda = 4 \ \rightarrow \ y = 2, 15 \ \rightarrow \ x = 2, 12$;
Per $\lambda = 8 \ \rightarrow \ y = 5, 12 \ \rightarrow \ x = 1, 10$;
Per $\lambda = 9 \ \rightarrow \ y = 3, 14 \ \rightarrow \ x = 2, 4$;
Per $\lambda = 13 \ \rightarrow \ y = 8, 9 \ \rightarrow \ x = 7, 13$;
Per $\lambda = 15 \ \rightarrow \ y = 7, 10 \ \rightarrow \ x = 13, 14$;
Per $\lambda = 16 \ \rightarrow \ y = 4, 13 \ \rightarrow \ x = 1, 4$.

ESERCIZIO 6: Soluzione. Si calcola agevolmente che

$\left(\frac{1}{3}\right) = 1$, $\left(\frac{1}{11}\right) = 1$, $\left(\frac{1}{33}\right) = 1$ ◀
$\left(\frac{2}{3}\right) = -1$, $\left(\frac{2}{11}\right) = -1$, $\left(\frac{2}{33}\right) = 1$.
$\left(\frac{4}{3}\right) = 1$, $\left(\frac{4}{11}\right) = 1$, $\left(\frac{4}{33}\right) = 1$ ◀
$\left(\frac{5}{3}\right) = -1$, $\left(\frac{5}{11}\right) = 1$, $\left(\frac{5}{33}\right) = -1$.
$\left(\frac{7}{3}\right) = 1$, $\left(\frac{7}{11}\right) = -1$, $\left(\frac{7}{33}\right) = -1$.
$\left(\frac{8}{3}\right) = -1$, $\left(\frac{8}{11}\right) = -1$, $\left(\frac{8}{33}\right) = 1$.
$\left(\frac{10}{3}\right) = 1$, $\left(\frac{10}{11}\right) = -1$, $\left(\frac{10}{33}\right) = -1$.
$\left(\frac{13}{3}\right) = 1$, $\left(\frac{13}{11}\right) = -1$, $\left(\frac{13}{33}\right) = -1$.
$\left(\frac{14}{3}\right) = -1$, $\left(\frac{14}{11}\right) = 1$, $\left(\frac{14}{33}\right) = -1$.
$\left(\frac{16}{3}\right) = 1$, $\left(\frac{16}{11}\right) = 1$, $\left(\frac{16}{33}\right) = 1$ ◀
$\left(\frac{17}{3}\right) = -1$, $\left(\frac{17}{11}\right) = -1$, $\left(\frac{17}{33}\right) = 1$.
$\left(\frac{19}{3}\right) = 1$, $\left(\frac{19}{11}\right) = -1$, $\left(\frac{19}{33}\right) = -1$.
$\left(\frac{20}{3}\right) = -1$, $\left(\frac{20}{11}\right) = 1$, $\left(\frac{20}{33}\right) = -1$.

$\left(\frac{23}{3}\right) = -1$, $\left(\frac{23}{11}\right) = 1$, $\left(\frac{23}{33}\right) = -1$.
$\left(\frac{25}{3}\right) = 1$, $\left(\frac{25}{11}\right) = 1$, $\left(\frac{25}{33}\right) = 1$ ◄
$\left(\frac{26}{3}\right) = -1$, $\left(\frac{26}{11}\right) = 1$, $\left(\frac{26}{33}\right) = -1$.
$\left(\frac{28}{3}\right) = 1$, $\left(\frac{28}{11}\right) = -1$, $\left(\frac{28}{33}\right) = -1$.
$\left(\frac{29}{3}\right) = -1$, $\left(\frac{29}{11}\right) = -1$, $\left(\frac{29}{33}\right) = 1$.
$\left(\frac{31}{3}\right) = 1$, $\left(\frac{31}{11}\right) = 1$, $\left(\frac{31}{33}\right) = 1$ ◄
$\left(\frac{32}{3}\right) = -1$, $\left(\frac{32}{11}\right) = -1$, $\left(\frac{32}{33}\right) = 1$.

I casi segnalati con ◄ sono i casi in cui la congruenza $X^2 - a \equiv 0 \pmod{33}$ è risolubile (cioè, i casi in cui entrambe le congruenze $X^2 - a \equiv 0 \pmod{3}$ e $X^2 - a \equiv 0 \pmod{11}$ sono risolubili).