Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2008/2009
TN1 - Introduzione alla teoria dei numeri
Prima prova di valutazione intermedia
6 aprile 2009

*Cognome*_____ *Nome*_____

*Numero di matricola*_____

Avvertenza: Svolgere ogni esercizio nello spazio assegnato, senza consegnare altri fogli e **giustificando tutte le affermazioni fatte**. E' consentito l'uso di libri, appunti e calcolatrici.

1. Trovare, al variare del parametro λ ($0 \leq \lambda \leq 4$), le soluzioni del seguente sistema lineare in due variabili:

$$\begin{cases} \lambda X + 3Y \equiv 1 \pmod 5 \\ 2X - \lambda Y \equiv 4 \pmod 5 \end{cases}$$

Soluzione

$-\lambda^2 - 6 \equiv 0 \pmod 5$ per $\lambda = 2, 3$; allora per $\lambda = 0,\ 1,\ 4$, il sistema ammette una ed una sola soluzione (mod 5) data da:

$x \equiv (-\lambda^2 + 4)^{-1}(-\lambda + 3) \pmod 5$ e $y \equiv (-\lambda^2 + 4)^{-1}(4\lambda + 3) \pmod 5$

da cui si ottiene:

per $\lambda = 0$ l'unica soluzione $x \equiv 2 \pmod 5$ e $y \equiv 2 \pmod 5$;

per$\lambda = 1$ l'unica soluzione $x \equiv 4 \pmod 5$ e $y \equiv 4 \pmod 5$;

per $\lambda = 4$ l'unica soluzione $x \equiv 3 \pmod 5$ e $y \equiv 3 \pmod 5$.

Per$\lambda = 2$ il sistema diventa

$$\begin{cases} 2X + 3Y \equiv 1 \pmod 5 \\ 2X + 3Y \equiv 4 \pmod 5 \end{cases}.$$

che non ha soluzioni.

Per$\lambda = 3$ il sistema diventa

$$\begin{cases} 3X & + & 3Y & \equiv & 1 & (\text{mod } 5) \\ 2X & + & 2Y & \equiv & 4 & (\text{mod } 5) \end{cases}.$$

cioè $X + Y \equiv 2 \pmod 5$ che ha 5 soluzioni (mod 5): $x_1 \equiv 2 \pmod 5$ e $y_1 \equiv 0 \pmod 5$; $x_2 \equiv 1 \pmod 5$ e $y_2 \equiv 1 \pmod 5$; $x_3 \equiv 0 \pmod 5$ e $y_3 \equiv 2 \pmod 5$; $x_4 \equiv 4 \pmod 5$ e $y_4 \equiv 3 \pmod 5$; $x_5 \equiv 3 \pmod 5$ e $y_5 \equiv 4 \pmod 5$.

2. Quali tra le seguenti funzioni aritmetiche sono moltiplicative? Quali totalmente moltiplicative? Motivare le risposte.

   (a) $f(n) = \begin{cases} 1 & \text{se } n \text{ è un quadrato perfetto} \\ 0 & \text{altrimenti} \end{cases}$;

   (b) $f(n) = n^3$;

   (c) $f(n) = \big|\{p \text{ primo} \mid p|n\}\big|$;

   (d) $f(n) = n - 1$.

   Soluzione

   (a) f è moltiplicativa poiché il prodotto di due numeri coprimi è un quadrato perfetto se e solo se lo è ciascuno di essi. f non è totalmente moltiplicativa poiché ad esempio $1 = f(4) \neq f(2)f(2) = 0$.

   (b) f è totalmente moltiplicativa poiché per ogni $n, m \in \mathbb{N}$ si ha $f(nm) = (nm)^3 = n^3m^3$.

   (c) f non è moltiplicativa poiché ad esempio $f(6) = 2 \neq f(2)f(3) = 1$.

   (d) f non è moltiplicativa poiché ad esempio $f(6) = 5 \neq f(2)f(3) = 2$.

3. Determinare il più piccolo intero positivo soluzione del seguente sistema di congruenze lineari:

$$\begin{cases} 3X \equiv 5 & (\text{mod } 8) \\ 2X \equiv 3 & (\text{mod } 9) \\ 7X \equiv 6 & (\text{mod } 13) \\ 4X \equiv 1 & (\text{mod } 5) \end{cases}$$

   Soluzione

   Il sistema per il teorema cinese dei resti ammette una ed una sola soluzione modulo $8 \cdot 9 \cdot 13 \cdot 5 = 4680$.

Il sistema dato è equivalente al sistema:

$$\begin{cases} X \equiv 7 \pmod 8 \\ X \equiv 6 \pmod 9 \\ X \equiv 12 \pmod{13} \\ X \equiv 4 \pmod 5 \end{cases}$$

$N_1 = 9 \cdot 13 \cdot 5 = 585$; $N_1 \equiv 1 \pmod 8$; pertanto un inverso aritmetico di N_1 modulo 8 è $x_1 = 1$.

$N_2 = 8 \cdot 13 \cdot 5 = 520$; $N_2 \equiv 7 \pmod 9$; pertanto un inverso aritmetico di N_2 modulo 9 è $x_2 = 4$.

$N_3 = 8 \cdot 9 \cdot 5 = 360$; $N_3 \equiv 9 \pmod{13}$; pertanto un inverso aritmetico di N_3 modulo 13 è $x_3 = 3$.

$N_4 = 8 \cdot 9 \cdot 13 = 936$; $N_4 \equiv 1 \pmod 5$; pertanto un inverso aritmetico di N_4 modulo 5 è $x_4 = 1$.

Una soluzione del sistema è data da:

$x = 7{\cdot}585{\cdot}1{+}6{\cdot}520{\cdot}4{+}12{\cdot}360{\cdot}3{+}4{\cdot}936{\cdot}1 = 4095{+}12480{+}12960{+}3744 = 33279;$

Pertanto

$$\{y \in \mathbb{Z} \mid y \text{ è soluzione del sistema } \} = \{33279 + k4680 \mid k \in \mathbb{Z}\}.$$

Dividendo x per 4680 si ottiene $x = 7 \cdot 4680 + 519$.

519 è pertanto il più piccolo intero positivo soluzione del sistema dato.

4. Determinare tutte le (eventuali) soluzioni della seguente congruenza polinomiale:

$$f(X) = X^{12} + 3X^{10} + 4X^7 + X + 1 \equiv 0 \pmod{225}$$

Soluzione

$225 = 3^2 \cdot 5^2$. Risolvere la congruenza data è equivalente a risolvere il sistema

$$\begin{cases} f(X) \equiv 0 \pmod{3^2} \\ f(X) \equiv 0 \pmod{5^2} \end{cases}$$

Si ha che $f'(X) = 12X^{11} + 30X^9 + 28X^6 + 1$.

Il polinomio $f(X)$ è equivalente a $X^2 + 2X + 1 \pmod 3$; la congruenza $X^2 + 2X + 1 \equiv 0 \pmod 3$ ha come unica soluzione $(\mod 3)$ $y = -1$; $f'(-1) = -13 \equiv 2 \pmod 3$, pertanto $y = -1$ è soluzione non singolare di $f(X) \equiv 0 \pmod 3$; inoltre $f(-1) = 0$; la congruenza $2T \equiv 0 \pmod 3$ ha

come soluzione $t = 0$; pertanto $x = -1 + 0 = -1$ è l'unica soluzione della congruenza $f(X) \equiv 0 \pmod{3^2}$.

Osservazione importante: da $f(-1) = 0$ segue che -1 è soluzione di $f(X) \equiv 0 \pmod{n}$ per ogni $n \geqslant 2$.

Oppure la congruenza $X^2 + 2X + 1 \equiv 0 \pmod 3$ ha come soluzione $y = 2$; $f'(X)$ è equivalente a $X^2+1 \pmod 3$ da cui $f'(2) \equiv 2 \pmod 3$; $f(2) = 7683$; $-\frac{7683}{3} \equiv 1 \pmod 3$; la congruenza $2T \equiv 1 \pmod 3$ ha come soluzione $t = 2$; pertanto $x = 2 + 3 \cdot 2 = 8$ è l'unica soluzione della congruenza $f(X) \equiv 0 \pmod{3^2}$.

Il polinomio $f(X)$ è equivalente a $X^4 + 4X^3 + 3X^2 + X + 1 \pmod 5$; la congruenza $X^4 + 4X^3 + 3X^2 + X + 1 \equiv 0 \pmod 5$ ha come soluzioni $y_1 = 1$, $y_2 = 3$ e $y_3 = 4$. Si osservi che $4 \equiv -1 \pmod 5$ e già sappiamo che -1 è soluzione di $f(X) \equiv 0 \pmod{5^2}$.

$f'(X)$ è equivalente a $2X^3 + 3X^2 + 1 \pmod 5$;

poiché $f'(1) \equiv 1 \pmod 5$, siamo nel caso di una soluzione non singolare; $f(1) = 10$; la congruenza $T \equiv 3 \pmod 5$ ha come soluzione $t = 3$; pertanto $x_1 = 1+5\cdot 3 = 16$ è l'unica soluzione della congruenza $f(X) \equiv 0 \pmod{5^2}$ determinata da y_1;

$f'(3) \equiv 2 \pmod 5$, siamo nel caso di una soluzione non singolare; $f(3) = 717340$; la congruenza $2T \equiv 2 \pmod 5$ ha come soluzione $t = 1$; pertanto $x_2 = 3+5\cdot 1 = 8$ è l'unica soluzione della congruenza $f(X) \equiv 0 \pmod{5^2}$ determinata da y_2;

$f'(4) \equiv 2 \pmod 5$, siamo nel caso di una soluzione non singolare; $f(4) = 19988485$; la congruenza $2T \equiv 3 \pmod 5$ ha come soluzione $t = 4$; pertanto $x_3 = 4+5\cdot 4 = 24$ è l'unica soluzione della congruenza $f(X) \equiv 0 \pmod{5^2}$ determinata da y_3;

lavorando con -1, si ha: $f'(-1) = -13 \equiv 2 \pmod 5$; siamo nel caso di una soluzione non singolare; $f(-1) = 0$; la congruenza $2T \equiv 0 \pmod 5$ ha come soluzione $t = 0$; pertanto $x_3 = -1 + 0 = -1$ è l'unica soluzione della congruenza $f(X) \equiv 0 \pmod{5^2}$ determinata da y_3.

Riassumendo, la congruenza $f(X) \equiv 0 \pmod{3^2}$ ha una sola soluzione (mod 9): 8 cui è talvolta da preferire, per semplicità di calcoli, -1;

La congruenza $f(X) \equiv 0 \pmod{5^2}$ ha tre soluzioni non congrue (mod 25): 16, 8 e -1.

Le soluzioni della congruenza data si ottengono risolvendo i sistemi:

(a)

$$\begin{cases} X \equiv 8 & \pmod 9 \\ X \equiv 16 & \pmod{25} \end{cases}$$

che ha come unica soluzione (mod 225)
$z_1 = 8 \cdot 25 \cdot 4 + 16 \cdot 9 \cdot 14 = 2816 \equiv 116 \pmod{225}$;

considerando il sistema equivalente

$$\begin{cases} X \equiv -1 \pmod 9 \\ X \equiv 16 \pmod{25} \end{cases}$$

si ottiene la soluzione:
$z_1 = -1 \cdot 25 \cdot 4 + 16 \cdot 9 \cdot 14 = 1916 \equiv 116 \pmod{225}$;

(b)

$$\begin{cases} X \equiv 8 \pmod 9 \\ X \equiv 8 \pmod{25} \end{cases}$$

che ha come unica soluzione (mod 225)
$z_2 = 8$;

(c)

$$\begin{cases} X \equiv -1 \pmod 9 \\ X \equiv -1 \pmod{25} \end{cases}$$

che ha come unica soluzione (mod 225)
$z_3 = -1 \pmod{225}$.

Concludendo, le soluzioni della congruenza data (mod 225) sono $z_1 = 116$, $z_2 = 8$ e $z_3 = -1$.

5. (a) Trovare tutte le radici primitive modulo 18.
   (b) Risolvere le seguenti congruenze:
      i. $X^{10} \equiv 13 \pmod{18}$;
      ii. $13X^{15} \equiv 5 \pmod{18}$;
      iii. $7^X \equiv 13 \pmod{18}$.

Soluzione

(a) $18 = 2 \cdot 3^2$; U_{18} ha $\varphi(18) = 6$ elementi ed è per il Teorema di Gauss ciclico, cioè esistono radici primitive (mod 18); esse sono $\varphi(\varphi(18)) = \varphi(6) = 2$. Sappiamo che 2 è una radice primitiva (mod 3); poiché $2^3 = 8$ non congruo ad 1 (mod 9), si ha che 2 è una radice primitiva (mod 9); dal teorema di Gauss sappiamo che $2 + 9 = 11$ è una radice primitiva (mod 18); l'altra radice primitiva è $11^5 \equiv 5 \pmod{18}$.

(b) Si ha che $\text{ind}_5\ 1 = 6$, $\text{ind}_5\ 5 = 1$, $\text{ind}_5\ 7 = 2$, $\text{ind}_5\ 11 = 5$, $\text{ind}_5\ 13 = 4$ e $\text{ind}_5\ 17 = 3$.

(c) i. Poiché $\text{MCD}(\varphi(18) = 6, 10) = 2$ divide $\text{ind}_5\ 13 = 4$, la congruenza è risolubile ed ha due soluzioni che si ottengono passando agli indici e risolvendo la congruenza lineare

$$10 \cdot \text{ind}_5\ X \equiv 4 \pmod 6$$

quest'ultima ha come soluzioni non congrue (mod 6) 1 e 4; poiché $1 = \text{ind}_5\ 5$ e $4 = \text{ind}_5\ 13$, si ha che 5 e 13 sono le soluzioni non congrue (mod 18) della congruenza data.

ii. Da $1 = 7 \cdot 13 - 5 \cdot 18$ si ottiene che 7 è un inverso aritmetico di 13 (mod 18). La congruenza data è equivalente alla congruenza $X^{15} \equiv 17 \pmod{18}$; poiché $\text{MCD}(\varphi(18) = 6, 15) = 3$ divide $\text{ind}_5\ 17 = 3$, la congruenza è risolubile ed ha tre soluzioni; passando agli indici si ottiene la congruenza lineare

$$15 \cdot \text{ind}_5\ X \equiv 3 \pmod{6}$$

che ha come soluzioni non congrue (mod 6) 1, 3, 5; poiché $1 = \text{ind}_5\ 5$, $\text{ind}_5\ 17 = 3$ e $\text{ind}_5\ 11 = 5$, si ha che 5, 11 e 17 sono le soluzioni non congrue (mod 18) della congruenza data.

iii. Passando agli indici si ottiene:

$$(\text{ind}_5\ 7)X \equiv \text{ind}_5\ 13 \pmod{6}$$

cioè

$$2X \equiv 4 \pmod{6}$$

che ha come soluzioni non congrue (mod 6) 2 e 5.

6. Sia p un numero primo dispari; sia a un numero intero primo con p tale che $\text{ord}_p\ a = 3$. Provare che:

   (a) p non divide $1 + a$;

   (b) $1 + a + a^2 \equiv 0 \pmod{p}$;

   (c) $\text{ord}_p\ (1 + a) = 6$.

   Soluzione

   i. Se p dividesse $1+a$, allora $a \equiv -1 \pmod{p}$ e pertanto $\text{ord}_p\ a = 2$ contrariamente alla ipotesi che $\text{ord}_p\ a = 3$.

   ii. Poiché $\text{ord}_p\ a = 3$, $a^3 \equiv 1 \pmod{p}$ da cui $a^3 - 1 = (a-1)(1+a+a^2) \equiv 0 \pmod{p}$; non essendo $a - 1$ congruo a 0 (mod p) poichè $\text{ord}_p\ a = 3$, si ha che $1 + a + a^2 \equiv 0 \pmod{p}$.

   iii. Per il punto precedente $(1 + a)^2 = 1 + a + a^2 + a \equiv a \pmod{p}$; allora $(1+a)^6 \equiv a^3 \equiv 1 \pmod{p}$. Inoltre $(1+a)^3 \equiv (1+a)a \equiv -1 \pmod{p}$. Pertanto $\text{ord}_p\ (1 + a) = 6$.