Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2008/2009
TN1 - Introduzione alla teoria dei numeri
Appello A
8 giugno 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. Sia p un numero primo dispari. Provare che per ogni $n \geqslant 1$ si ha:

$$[(p-1)!]^{p^{n-1}} \equiv -1 \pmod{p^n}.$$

Soluzione

Per induzione su n;

base dell'induzione: per $n = 1$ si ha che $(p-1)! \equiv -1 \pmod{p}$ per il teorema di Wilson;

passo induttivo: sia $n \geqslant 1$ e sia vero che $[(p-1)!]^{p^{n-1}} \equiv -1 \pmod{p^n}$; da qui segue che $[(p-1)!]^{p^{n-1}} = -1 + kp^n$ con $k \in \mathbb{Z}$; allora

$$[(p-1)!]^{p^n} = \{[(p-1)!]^{p^{n-1}}\}^p = (-1+kp^n)^p = (-1)^p + \binom{p}{1} kp^n + - \binom{p}{2} (kp^n)^2 + \cdots - \binom{p}{p-1} (kp^n)^{p-1} + (kp^n)^p;$$

poiché p divide $\binom{p}{h}$ per ogni $1 \leqslant h \leqslant p-1$, si ha che

$[(p-1)!]^{p^n} \equiv -1 \pmod{p^{n+1}}$.

2. Risolvere, se possibile, il seguente sistema lineare in tre indeterminate:

$$\begin{cases} X + 2Y + 3Z \equiv 1 \pmod 7 \\ Y + 2Z \equiv 3 \pmod 7 \\ 2X + 5Z \equiv 4 \pmod 7 \end{cases}.$$

Soluzione

La matrice dei coefficienti

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 2 & 0 & 5 \end{pmatrix}$$

ha determinante congruo a 0 (mod 7); poiché $\det \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = 1$, la matrice dei coefficienti ha rango 2 (mod 7); la matrice completa

$$\begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & 1 & 2 & 3 \\ 2 & 0 & 5 & 4 \end{pmatrix}$$

ha anche essa rango 2 poiché $\det \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 3 \\ 2 & 0 & 4 \end{pmatrix} = 14 \equiv 0 \pmod 7$; pertanto il sistema ammette 7 soluzioni incongruenti (mod 7) che si ottengono nel seguente modo: per ogni $\lambda \in \mathbb{Z}$ si risolve il sistema di Cramer:

$$\begin{cases} X + 2Y \equiv 1 - 3\lambda \pmod 7 \\ Y \equiv 3 - 2\lambda \pmod 7 \end{cases}$$

ottenendo le soluzioni $(\lambda - 5,\ 3 - 2\lambda,\ \lambda)$

3. (a) Sapendo che 3 è una radice primitiva modulo 17, verificare che 3 è anche una radice primitiva modulo 34.
   (b) Trovare tutte le radici primitive modulo 34.
   (c) Risolvere le seguenti congruenze:
      i. $X^{14} \equiv 15 \pmod{34}$;
      ii. $5^X \equiv 29 \pmod{34}$.

Soluzione

(a) Poiché 3 è una radice primitiva modulo 17, si ha che $3^{\varphi(17)} = 3^{\varphi(34)} \equiv 1 \pmod{17}$ da cui, essendo banalmente $3^{\varphi(34)} \equiv 1 \pmod{2}$, si ha che $3^{\varphi(34)} \equiv 1 \pmod{34}$; inoltre se $3^h \equiv 1 \pmod{34}$, allora $3^h \equiv 1 \pmod{17}$ da cui $16 = \varphi(17) = \varphi(34)$ divide l; pertanto 16 è l'ordine di 3 modulo 34.

(b) Le radici primitive modulo 34 sono $\varphi(\varphi(34)) = \varphi(16) = 8$ e sono del tipo 3^h con $1 \leqslant h \leqslant 16$ e MCD(16,h)=1; sono pertanto

$$3,\ 3^3,\ 3^5,\ 3^7,\ 3^9,\ 3^{11},\ 3^{13},\ 3^{15}.$$

(c) Poiché $\mathrm{MCD}(16, 14) = 2$ divide $\mathrm{ind}_3\ 15 = 6$, la congruenza è risolubile ed ha due soluzioni incongruenti (mod 34) che si ottengono passando agli indici e risolvendo la congruenza lineare

$$14 \cdot \mathrm{ind}_3\ X \equiv 6 \pmod{16}$$

quest'ultima ha come soluzioni non congrue (mod 16) 5 e 13; poiché $5 = \mathrm{ind}_3\ 5$ e $13 = \mathrm{ind}_3\ 29$, si ha che 5 e 29 sono le soluzioni non congrue (mod 34) della congruenza data.

(d) Passando agli indici si ottiene:

$$(\mathrm{ind}_3\ 5)X \equiv \mathrm{ind}_3\ 29 \pmod{16}$$

cioè

$$5X \equiv 13 \pmod{16}$$

che ha una sols soluzione (mod 16): 9.

4. Si consideri la congruenza quadratica

$$X^2 + 4X + 2 \equiv 0 \pmod{p} \qquad (*)$$

(a) Determinare i numeri primi p per i quali la congruenza $(*)$ è risolubile.

(b) Trovare le soluzioni della conguenza

$$X^2 + 4X + 2 \equiv 0 \pmod{31 \cdot 17^2}$$

Soluzione

(a) Per $p = 2$ la congruenza quadratica $X^2 \equiv 0$ è risolubile.

Sia p un primo dispari; la congruenza $(*)$ è equivalente alla congruenza $Y^2 \equiv 8 \pmod{p}$ che è risolubile, essendo MCD(4,p)=1, se e solo se $\left(\frac{2}{p}\right) = 1$, cioè se e solo se $\left(\frac{2}{p}\right) = 1$, cioè se e solo se $p \equiv 1, 7 \pmod{8}$.

(b) La congruenza $X^2 + 4X + 2 \equiv 0 \pmod{31 \cdot 17^2}$ è risolubile se e solo se $X^2 + 4X + 2 \equiv 0 \pmod{31}$ e $X^2 + 4X + 2 \equiv 0 \pmod{17^2}$ sono risolubili; $X^2 + 4X + 2 \equiv 0 \pmod{17^2}$ è risolubile se e solo se $X^2 + 4X + 2 \equiv 0 \pmod{17}$ è risolubile; essendo $31 \equiv 7 \pmod{8}$ e $17 \equiv 1 \pmod{8}$, per il punto precedente entrambe le congruenze sono risolubili e la congruenza $(*)$ ha 4 soluzioni.

La congruenza $Y^2 \equiv 8 \pmod{31}$ ha come soluzioni incongruenti (mod 31) 15 e 16; considerando $2X + 4 \equiv 15 \pmod{31}$ e $2X + 4 \equiv 16 \pmod{31}$ si ottengono le soluzioni incongruenti (mod 31) della congruenza $X^2 + 4X + 2 \equiv 0 \pmod{31}$: 21 e 6.

La congruenza $Y^2 \equiv 8 \pmod{17}$ ha come soluzioni incongruenti (mod 17) 5 e 12; considerando $2X + 4 \equiv 5 \pmod{17}$ e $2X + 4 \equiv 12 \pmod{17}$, si ottengono le soluzioni incongruenti (mod 17) della congruenza $X^2 + 4X + 2 \equiv 0 \pmod{17}$: 9 e 4.

Sollevando 9 si ottiene: $22T \equiv -7 \pmod{17}$ da cui $t = 2$ e $x := 9 + 2 \cdot 17 = 43$.

Sollevando 4 si ottiene $12T \equiv -2 \pmod{17}$ da cui $t = 14$ e $x := 4 + 14 \cdot 17 = 242$.

Quindi le soluzioni di $X^2 + 4X + 2 \equiv 0 \pmod{17^2}$ incongruenti (mod 17^2) sono: 43 e 242.

Considerando il sistema

$$\begin{cases} X \equiv 21 & \pmod{31} \\ X \equiv 43 & \pmod{17^2} \end{cases}$$

si ottiene 1199 come soluzione della congruenza $(*)$;

considerando il sistema

$$\begin{cases} X \equiv 21 & \pmod{31} \\ X \equiv 242 & \pmod{17^2} \end{cases}$$

si ottiene 3710 come soluzione della congruenza $(*)$;

considerando il sistema

$$\begin{cases} X \equiv 6 & \pmod{31} \\ X \equiv 43 & \pmod{17^2} \end{cases}$$

si ottiene 5245 come soluzione della congruenza $(*)$;
considerando il sistema

$$\begin{cases} X \equiv 6 & (\text{mod } 31) \\ X \equiv 242 & (\text{mod } 17^2) \end{cases}$$

si ottiene 7756 come soluzione della congruenza $(*)$.

5. (a) Sia p un primo dispari. Provare che se p divide $a^2 + b^2$ con a e b numeri interi primi tra loro, allora $p \equiv 1 \pmod 4$.
   (b) Utilizzando il punto (a), provare che ogni divisore positivo di una somma di due quadrati di interi primi tra loro è esso stesso una somma di due quadrati.

Soluzione

(a) Per ipotesi $a^2 \equiv -b^2 \pmod p$; inoltre p non divide a; se p dividesse a, dividendo $a^2 + b^2$, p dividerebbe anche b; analogamente p non divide b; si possono quindi considerare i simboli di Legendre $\left(\frac{a^2}{p}\right)$ e $\left(\frac{-b^2}{p}\right)$; si ha

$$1 = \left(\frac{a^2}{p}\right) = \left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{b^2}{p}\right) = \left(\frac{-1}{p}\right)$$

da cui segue che $p \equiv 1 \pmod 4$.

(b) Sia $d > 1$ un divisore di una somma di due quadrati di interi primi tra loro; poiché ogni divisore primo p di d è un divisore di una somma di due quadrati di interi primi tra loro, per il punto (a) si ha che $p \equiv 1 \pmod 4$ e pertanto somma di due quadrati. Essendo l'insieme dei numeri naturali positivi somma di due quadrati chiuso rispetto al prodotto, si ha che d è somma di due quadrati.

6. Si consideri la funzione moltiplicativa $F = \tau * \varphi$.
   (a) Calcolare $F(33)$ e $F^{-1}(33)$.
   (b) Sia f la funzione aritmetica determinata dalla formula di inversione di Möbius. Calcolare $f(33)$.

Soluzione

(a) $F(n) = \sum_{d|n} \tau(d)\varphi(\frac{n}{d})$ per ogni $n > 0$; pertanto

$$F(33) = \tau(1)\varphi(33) + \tau(3)\varphi(11) + \tau(11)\varphi(3) + \tau(33)\varphi(1) =$$

$$= 1 \cdot 20 + 2 \cdot 10 + 2 \cdot 2 + 4 \cdot 1 = 48$$

Inoltre $F^{-1} = \tau^{-1} * \varphi^{-1}$; pertanto

$$F^{-1}(33) = \tau^{-1}(1)\varphi^{-1}(33)+\tau^{-1}(3)\varphi^{-1}(11)+\tau^{-1}(11)\varphi^{-1}(3)+\tau^{-1}(33)\varphi^{-1}(1) =$$

$$= 1 \cdot 20 + (-2) \cdot (-10) + (-2) \cdot (-2) + 4 \cdot 1 = 48$$

(b) Si ha $f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d})$; pertanto

$$f(33) = F(1)\mu(33) + F(3)\mu(11) + F(11)\mu(3) + F(33)\mu(1) =$$

$$= 1 \cdot 1 + 4 \cdot (-1) + 12 \cdot (-1) + 48 \cdot 1 = 33$$