Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2008/2009
TN1 - Introduzione alla teoria dei numeri
Seconda prova di valutazione intermedia
4 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. Si consideri la congruenza quadratica:

$$X^2 \equiv 825 \pmod{4624} \qquad (*)$$

   (a) Verificare che la congruenza $(*)$ è risolubile e deterrminare il numero delle sue soluzioni.

   (b) Trovare le soluzioni della congruenza $(*)$.

Soluzione

(a) $4624 = 2^4 \cdot 17^2$. Poiché $825 \equiv 1 \bmod(8)$, la congruenza $X^2 \equiv 825 \pmod{2^4}$ è risolubile ed ha esattamente quattro soluzioni incongruenti modulo 2^4. Inoltre 17 non divide 825 e $\left(\frac{825}{17}\right) = \left(\frac{9}{17}\right) = 1$; pertanto la congrueenza $X^2 \equiv 825 \pmod{17^2}$ è risolubile ed ha esattamente due soluzioni incongruenti modulo 17^2. In conclusione la congruenza data è risolubile ed ha esattamente otto soluzioni incongruenti modulo 4624.

(b) La congruenza $X^2 \equiv 825 \equiv 9 \pmod{2^4}$ ha come soluzioni (incongruenti modulo 2^4) $3,\ -3,\ 3 + 2^3 = 11,\ -3 + 2^3 = 5$.
La congruenza $X^2 \equiv 825 \equiv 247 \pmod{17^2 = 289}$ ha due soluzioni che si ottengono nel seguente modo: $X^2 \equiv 825 \equiv 9 \pmod{17}$ ha come soluzioni (incongruenti modulo 17) $3,\ -3$; in ogni caso, $9 = 247 - 14 \cdot 17$; risolvendo la congruenza lineare $6T \equiv 14 \pmod{17}$ si

ottiene $t = 8$ da cui $x = 3+8\cdot 17 = 139$ è soluzione di $X^2 \equiv 825 \equiv 247 \pmod{17^2 = 289}$; l'ulteriore soluzione si può ottenere analogamente considerando la congruenza lineare $-6T \equiv 14 \pmod{17}$, dalla cui soluzione $t = 9$ si ha $x = -3 + 9 \cdot 17 = 150$, oppure, più banalmente, osservando che essa è $-139 \equiv 150 \pmod{289}$.

Considerando il sistema

$$\begin{cases} X \equiv 3 & \pmod{2^4} \\ X \equiv 139 & \pmod{17^2} \end{cases}$$

si ottiene 2451 come soluzione della congruenza $(*)$;

dal sistema

$$\begin{cases} X \equiv 3 & \pmod{2^4} \\ X \equiv 150 & \pmod{17^2} \end{cases}$$

si ottiene 3907 come soluzione della congruenza $(*)$;

dal sistema

$$\begin{cases} X \equiv 5 & \pmod{2^4} \\ X \equiv 139 & \pmod{17^2} \end{cases}$$

si ottiene 3029 come soluzione della congruenza $(*)$;

dal sistema

$$\begin{cases} X \equiv 5 & \pmod{2^4} \\ X \equiv 150 & \pmod{17^2} \end{cases}$$

si ottiene 4485 come soluzione della congruenza $(*)$;

per le altre quattro soluzioni basta considerare $-2451 \equiv 2173$, $-3907 \equiv 717$, $-3029 \equiv 1595$ e $-4485 \equiv 139$.

In conclusione, le soluzioni incongruenti modulo 4624 della congruenza $(*)$ sono:

$$139,\ \ 717,\ \ 1595,\ \ 2173,\ \ 2451,\ \ 3029,\ \ 3907,\ \ 4485.$$

2. (a) Calcolare il simbolo di Jacobi $\left(\frac{509}{32901}\right)$, sapendo che 509 e 997 sono numeri primi.
   (b) Stabilire se la congruenza quadratica $X^2 \equiv 509 \bmod(32901)$ è risolubile.

Soluzione

(a) $32901 = 3 \cdot 11 \cdot 997$;

$$\left(\frac{509}{32901}\right) := \left(\frac{509}{3}\right) \cdot \left(\frac{509}{11}\right) \cdot \left(\frac{509}{997}\right) =$$

$$= \left(\frac{2}{3}\right)\cdot\left(\frac{3}{11}\right)\cdot\left(\frac{997}{509}\right) = (-1)\cdot 1\cdot\left(\frac{488}{509}\right) = (-1)\cdot\left(\frac{2}{509}\right)\cdot\left(\frac{61}{509}\right) =$$
$$= (-1)\cdot(-1)\cdot\left(\frac{509}{61}\right) = \left(\frac{21}{61}\right) = \left(\frac{7}{61}\right)\cdot\left(\frac{3}{61}\right) = \left(\frac{61}{7}\right) = \left(\frac{5}{7}\right) = -1.$$

Oppure:

$$\left(\frac{509}{32901}\right) = (-1)^{\frac{508}{2}\frac{32900}{2}}\left(\frac{32901}{509}\right) = \left(\frac{325}{509}\right) = \left(\frac{13}{509}\right) = \left(\frac{509}{13}\right) = \left(\frac{2}{13}\right) = -1.$$

(b) Poiché $\left(\frac{509}{32901}\right) = -1$, la congruenza $X^2 \equiv 509 \bmod(32901)$ non è risolubile.

3. (a) Stabilire quali dei seguenti numeri sono somma di due quadrati:
   i. 605;
   ii. 424589 (divisibile per 11 e 29);
   iii. 841639; (divisibile per 23, 37, 43).

   (b) Scrivere i numeri del punto precedente, quando possibile, come somma di due quadrati.

Soluzione

(a) $605 = 11^2\cdot 5$; poiché $5 \equiv 1 \pmod 4$, $5 = 2^2+1$ da cui $605 = 22^2+11^2$;

(b) $424589 = 11^4 \cdot 29$; poiché $29 \equiv 1 \pmod 4$, $29 = 5^2 + 2^2$ da cui $424589 = 605^2 + 242^2$;

(c) $841639 = 23^2\cdot 37\cdot 43$; poiché $43 \equiv 3 \pmod 4$, 841639 non è esprimibile come somma di due quadrati.

4. Sia $p \geqslant 5$ un numero primo. Provare che l'equazione $3X^2 + Y^2 = p$ ha soluzioni intere se e solo se $p \equiv 1 \pmod 3$.

(Sugg.: per $\Longrightarrow$ si consideri $\left(\frac{-3}{p}\right)$; per $\Longleftarrow$ si utilizzi il lemma di Thue.)

Soluzione

Ricordiamo che $\left(\frac{-3}{p}\right) = 1$ se $p \equiv 1 \pmod 3$ e $\left(\frac{-3}{p}\right) = -1$ se $p \equiv -1 \pmod 3$.

$\Longrightarrow$): siano $x, y \in \mathbb{Z}$ tale che $3x^2 + y^2 = p$; allora $3x^2 + y^2 \equiv 0 \pmod p$ da cui $y^2 \equiv -3x^2 \pmod p$; p non divide né x né y (in caso contrario p^2 sarebbe un divisore di p); inoltre $p \geqslant 5$, si possono pertanto considerare $\left(\frac{y^2}{p}\right)$ e $\left(\frac{-3x^2}{p}\right)$ e si ha:

$$1 = \left(\frac{y^2}{p}\right) = \left(\frac{-3x^2}{p}\right) = \left(\frac{-3}{p}\right)$$

allora $p \equiv 1 \pmod 3$.

$\Longleftarrow$): essendo $p \equiv 1 \pmod 3$, -3 è un residuo quadratico di p; esiste allora $a \in \mathbb{Z}$ primo con p tale che $a^2 \equiv -3 \pmod p$; per il lemma di Thue esistono $x_0,\ y_0 \in \mathbb{Z}$ tali che $ax_0 \equiv y_0 \pmod p$ con $0 < |x_0| < \sqrt{p}$ e $0 < |y_0| < \sqrt{p}$; pertanto $-3x_0^2 \equiv y_0^2 \pmod p$, cioè esiste $k \in \mathbb{Z}$ tale che $3x_0^2 + y_0^2 = kp$; per le limitazioni su x_0 e y_0, si ha che $1 \leqslant k \leqslant 3$.

Se $k = 1$, $(x_0,\ y_0)$ è una soluzione dell'equazione $3X^2 + Y^2 = p$.

Se $k = 2$, da $3x_0^2 + y_0^2 = 2p$, passando alle classi resto modulo 3, si avrebbe $y_0^2 \equiv 2 \pmod 3$ e ciò è assurdo, poiché i quadrati (mod 3) sono 0 e 1; pertanto k non può essere 2.

Se $k = 3$, da $3x_0^2 + y_0^2 = 3p$, segue che 3 divide y_0, per cui dividendo per 3 si ottiene $x_0^2 + 3(\frac{y_0}{3})^2 = p$ da cui $(\frac{y_0}{3}, x_0)$ è una soluzione dell'equazione $3X^2 + Y^2 = p$.

5. **(a)** Scrivere come frazione continuata $\frac{253}{436}$;

   (b) calcolarne tutte le convergenti;

   (c) dedurre le soluzioni dell'equazione diofantea $253X + 436Y = 2$.

Soluzione

(a)

$$\begin{aligned} 436 &= 253 \cdot 1 + 183 \\ 253 &= 183 \cdot 1 + 70 \\ 183 &= 70 \cdot 2 + 43 \\ 70 &= 43 \cdot 1 + 27 \\ 43 &= 27 \cdot 1 + 16 \\ 27 &= 16 \cdot 1 + 11 \\ 16 &= 11 \cdot 1 + 5 \\ 11 &= 5 \cdot 2 + 1 \\ 5 &= 1 \cdot 5 + 0 \end{aligned}$$

Pertanto $\frac{253}{436} = [0; 1, 1, 2, 1, 1, 1, 1, 2, 5]$;

(b)

$$\begin{array}{lll} p_0 = 0 & q_0 = 1 & C_0 = 0 \\ p_1 = 1 & q_1 = 1 & C_1 = 1 \\ p_2 = 1 & q_2 = 2 & C_2 = \dfrac{1}{2} \\ p_3 = 3 & q_3 = 5 & C_3 = \dfrac{3}{5} \\ p_4 = 4 & q_4 = 7 & C_4 = \dfrac{4}{7} \\ p_5 = 7 & q_5 = 12 & C_5 = \dfrac{7}{12} \\ p_6 = 11 & q_6 = 19 & C_6 = \dfrac{11}{19} \\ p_7 = 18 & q_7 = 31 & C_7 = \dfrac{18}{31} \\ p_8 = 47 & q_8 = 81 & C_8 = \dfrac{47}{81} \\ p_9 = 253 & q_9 = 436 & C_9 = \dfrac{253}{436} \end{array}$$

(c) Da $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$ si ottiene $253 \cdot 81 - 436 \cdot 47 = 1$ da cui $253 \cdot 162 + 436 \cdot (-94) = 2$; pertanto $x_0 = 162$ e $y_0 = -94$ è una soluzione dell'equazione $253X + 436Y = 2$; la soluzione generale è data da $x = 162 + 436t$ e $y = -94 - 253t$ con $t \in \mathbb{Z}$.

6. Sia Λ la funzione di *von Mangoldt*, definita nel modo seguente:

$$\Lambda(n) := \begin{cases} \log(p) & \text{se } n = p^h,\ p \text{ numero primo },\ h \geq 1 \\ 0 & \text{altrimenti} \end{cases} .$$

Dimostrare che:

(a) $\log(n) = \sum_{d|n} \Lambda(d)$;

(b) $\Lambda(n) = \sum_{d|n} \left(\mu(d) \log\left(\frac{n}{d}\right) \right) = -\sum_{d|n} \left(\mu(d) \log(d) \right)$.

Soluzione

Per $n = 1$ sia (a) che (b) sono banalmente verificate; supponiamo pertanto che $n > 1$ e che $n = p_1^{h_1} \cdots p_t^{h_t}$ con p_j primo per $j = 1, \cdots, t$.

(a) $\log(n) = h_1 \log(p_1) + \cdots + h_t \log(p_t)$;
i divisori di n per i quali Λ è diversa da zero sono del tipo $p_j^{r_j}$ con $1 \leqslant r_j \leqslant h_j$ e $1 \leqslant j \leqslant t$. Per ogni $1 \leqslant j \leqslant t$ si ha

$$\Lambda(p_j) + \Lambda(p_j^2) + \cdots + \Lambda(p_j^{r_j}) + \cdots + \Lambda(p_j^{h_j}) = \log(p_j) + \log(p_j) + \cdots + \log(p_j) = h_j \log(p_j).$$

Pertanto

$$\sum_{d|n} \Lambda(d) = h_1 \log(p_1) + \cdots + h_t \log(p_t) = \log(n).$$

(b) Per il punto (a) le funzioni aritmetiche Λ e log sono tali che $\log(n) = \sum_{d|n} \Lambda(d)$; applicando la formula di inversione di Möbius si ha che

$$\Lambda(n) = \sum_{d|n} \Big(\mu(d) \log\big(\frac{n}{d}\big)\Big)$$

da cui, per una proprietà elementare di log si ha che:

$$\sum_{d|n} \Big(\mu(d) \log\big(\frac{n}{d}\big)\Big) = \sum_{d|n} \Big(\mu(d) \log(n)\big)\Big) - \sum_{d|n} \Big(\mu(d) \log(d)\Big) =$$

$$= \log(n) \sum_{d|n} \mu(d) - \sum_{d|n} \Big(\mu(d) \log(d)\Big)$$

essendo $n > 1$, si ha che $\sum_{d|n} \mu(d) = 0$; pertanto

$$\Lambda(n) = \sum_{d|n} \Big(\mu(d) \log\big(\frac{n}{d}\big)\Big) = -\sum_{d|n} \Big(\mu(d) \log(d)\Big).$$