Teoria Elementare dei Numeri (Schoof) 2^o compito 18 febbraio 2008, ore 11:00–13:00.

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

Risolvere gli esercizi negli spazi predisposti. Accompagnare le risposte con spiegazioni *chiare ed essenziali*. Consegnare SOLO QUESTO FOGLIO. Ogni esercizio vale 6 punti.

1. Sia E la curva di equazione $Y^2 = X^3 + X + 4$ su $\mathbf{Z}_7$. Sia P il punto $(0, 2)$.
   (a) Controllare che si tratta di una curva ellittica e che P sta sulla curva.
   (b) Calcolare l'ordine di P nel gruppo $E(\mathbf{Z}_7)$.

   Il discriminante di E non è congruo a zero modulo 7 e le coordinate del punto P soddisfano l'equazione. Questo implica la parte (a). Abbiamo che $2P = P + P = (4, 4)$, $4P = 2P + 2P = (6, 3)$ e $8P = 4P + 4P = (4, 3)$. Siccome il punto $(4, 3)$ è l'inverso di $(4, 4)$, abbiamo che $8P = -2P$ e quindi $10P = 0$. L'ordine di P è dunque un divisore di 10. L'ordine non è 1 o 2 perché né P né $2P$ è il punto all'infinito. L'ordine di P non è neanche 5 perché $4P \neq -P$. L'ordine di P è quindi uguale a 10.

2. (Numeri di Fermat) Per ogni numero naturale n, si definisce l'ennesimo numero di Fermat come $F_n = 2^{2^n} + 1$. Far vedere che ogni divisore primo p di F_n soddisfa $p \equiv 1 \pmod{2^{n+1}}$.

   Questo è il primo esercizio del terzo foglio.

3. (a) Dimostrare che 2 è una radice primitiva modulo il numero primo 59.
   (b) Calcolare il logaritmo discreto di $\overline{3} \in \mathbf{Z}_{59}^*$ rispetto alla radice primitiva 2.

   Abbiamo che $59 - 1 = 2 \cdot 29$. L'ordine di 2 divide $59 - 1$. Siccome $2^2 \not\equiv 1 \pmod{59}$, basta controllare che $2^{29} \not\equiv 1 \pmod{59}$. Ecco il calcolo: $2^7 = 128 \equiv 10 \pmod{59}$ e quindi $2^{14} \equiv 100 \equiv -18 \pmod{59}$. Vediamo così che $2^{29} = 648 \equiv -1 \pmod{59}$.

   Raccogliamo relazioni moltiplicative modulo 59 fra numeri primi piccoli. Si spara (quasi) a caso. Abbiamo che $2^2 \cdot 3 \cdot 5 = 60 \equiv 1 \pmod{59}$ e $2^6 = 64 \equiv 5 \pmod{59}$. Prendendo logaritmi in base 2 otteniamo le equazioni $2 + \log 3 + \log 5 \equiv 0 \pmod{58}$ e $6 \equiv \log 5 \pmod{58}$. Eliminando $\log 5$ troviamo che $\log 3 \equiv -8 \pmod{58}$.

4. Sia φ la funzione di Eulero.
   (a) Calcolare $\varphi(2008)$.
   (b) Scrivere il gruppo $\mathbf{Z}_{2008}^*$ come prodotto di gruppi ciclici.

   La fattorizzazione di 2008 come prodotto di numeri primi è $2^3 \cdot 251$. Abbiamo che $\varphi(2008) = 1000$. Per il Teorema cinese, il gruppo $\mathbf{Z}_{2008}^*$ è isomorfo a $\mathbf{Z}_{251}^* \times \mathbf{Z}_8^*$. Il gruppo $\mathbf{Z}_{251}^*$ è ciclico di ordine 250. Il gruppo $\mathbf{Z}_8^*$ è isomorfo a $\mathbf{Z}_2 \times \mathbf{Z}_2$. Abbiamo quindi che $\mathbf{Z}_{2008}^* \cong \mathbf{Z}_{250} \times \mathbf{Z}_2 \times \mathbf{Z}_2$.

5. Sia p un numero primo dispari e sia $x = (\frac{p-1}{2})!$ (fattoriale).
   (a) Per $p = 3, 5, 7, 11, 13$ calcolare $x^2 \pmod{p}$.
   (b) Calcolare $x^2 \pmod{p}$ in generale. Spiegare la risposta.

   Per $p = 3, 5, 7, 11, 13$ si ha che $x^2 \equiv +1, -1, +1, +1, -1 \pmod{p}$. Si sa che $(p-1)! \equiv -1 \pmod{p}$. In altre parole, il prodotto degli interi fra 1 e $p-1$ è congruo a $-1 \pmod{p}$. Adesso dividiamo l'insieme dei numeri fra 1 e $p-1$ in due parti: l'insieme A dei numeri fra 1 e $\frac{p-1}{2}$ e l'insieme B dei numeri fra $\frac{p+1}{2}$ e $p-1$. Ogni $j \in B$, si può scrivere come $j = p - i$ per un $i \in A$. Abbiamo quindi

$$\begin{aligned}(p-1)! = \prod_{i\in A} i \prod_{j\in B} j &= \prod_{i=1}^{\frac{p-1}{2}} i \prod_{i=1}^{\frac{p-1}{2}} (p-i), \\ \equiv \prod_{i=1}^{\frac{p-1}{2}} i \prod_{i=1}^{\frac{p-1}{2}} (-i) &\equiv \left(\prod_{i=1}^{\frac{p-1}{2}} i\right)^2 (-1)^{\frac{p-1}{2}}. \pmod{p}\end{aligned}$$

   Vediamo quindi che il numero $x = (\frac{p-1}{2})!$ ha la proprietà che $x^2 \equiv 1 \pmod{p}$ quando $p \equiv 3 \pmod{4}$ mentre $x^2 \equiv -1 \pmod{p}$ quando $p \equiv 1 \pmod{4}$.