Teoria Elementare dei Numeri (Schoof) 2^o compito 2 marzo 2007, ore 10:00–12:00.

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. (a) Esiste un elemento in $\mathbf{Z}_{35}^*$ di ordine 8? Se esiste, esibirne uno.
   (b) Esiste un elemento in $\mathbf{Z}_{35}^*$ di ordine 6? Se esiste, esibirne uno.

   L'elemento $\overline{9}$ di $\mathbf{Z}_{35}^*$ ha ordine 6. In $\mathbf{Z}_{35}^*$ non esistono elementi di ordine 8: infatti, supponiamo che $x \in \mathbf{Z}$ con $\mathrm{mcd}(x, 35) = 1$ soddisfi $x^8 \equiv 1 \pmod{35}$. Affermiamo che in realtà $x^4 \equiv 1 \pmod{35}$. Il piccolo teorema di Fermat ci dice che $x^4 \equiv 1 \pmod 5$. Resta da far vedere che anche $x^4 \equiv 1 \pmod 7$. Dal piccolo teorema di Fermat per il primo 7, abbiamo che $x^6 \equiv 1 \pmod 7$. Siccome $x^8 \equiv 1 \pmod{35}$ implica che $x^8 \equiv 1 \pmod 7$, segue che $x^2 \equiv 1 \pmod 7$ e quindi anche che $x^4 \equiv 1 \pmod 7$.

2. Sia E la curva di equazione $Y^2 = X^3 - 2X + 1$ su $\mathbf{Z}_{13}$.
   (a) Controllare che si tratta di una curva ellittica.
   (b) Far vedere che i punti $P = (3, 3)$ e $Q = (5, 5)$ stanno sulla curva e calcolarne la somma.

   Il discriminante della curva è uguale a $4 \cdot (-8) + 27 \cdot 1$ e non si annulla modulo 13. Si tratta quindi di una curva ellittica. Usando le solite formula di addizione si calcola che $P + Q = (6, 7)$.

3. Sia E la curva $Y^2 = X^3 - X + 2$ su $\mathbf{Z}_7$.
   (a) Dimostrare che si tratta di una curva ellittica.
   (b) Esibire tutti i punti di E con coordinate in $\mathbf{Z}_7$ (ce ne sono nove).
   (c) Esibire, se esiste, un punto di ordine 9 in $E(\mathbf{Z}_7)$.

   Il discriminante della curva è uguale a $4 \cdot (-1) + 27 \cdot 4$ e non si annulla modulo 7. Si tratta quindi di una curva ellittica. I nove punti in $E(\mathbf{Z}_7)$ sono il punto all'infinito e i punti $(0, \pm 3)$, $(1, \pm 3)$, $(2, \pm 1)$ e $(-1, \pm 3)$. Ogni punto diverso da $(-1, \pm 3)$ e dal punto all'infinito ha ordine 9. Per esempio, si ha che $(0, 3) + (0, 3) = (1, 3)$, dimostrando che $(0, 3)$ non ha ordine 3. Siccome l'ordine di ogni punto divide 9, concludiamo che $(0, 3)$ ha ordine 9.

4. Descrivere il "metodo $p - 1$" per fattorizzare numeri interi. Quanto tempo ci si mette asintoticamente per trovare un fattore primo p di un numero naturale dato n con questo metodo? Spiegare la risposta.

   Si sceglie un elemento $\overline{x} \in \mathbf{Z}_n^*$ a caso e si calcola $\overline{y} = \overline{x}^M$ dove M ha la forma

   $$M = \prod_{\substack{q \text{ primo} \\ q^{a(q)} < B}} q^{a(q)}.$$

   dove B è un certo limite prescelto. Adesso $\mathrm{mcd}(y - 1, n)$ è un fattore di n. In pratica, si riesce a fattorizzare n in questo modo se n ha un fattore primo p con la proprietà che i divisori primi di $p-1$ sono tutti minori di B. Il tempo del calcolo è proporzionale a B. Il caso peggiore si ha quando per ogni divisor primo p di n il numero $p - 1$ ha un divisore primo grosso. In ogni caso, il tempo che ci mette è minore di una certa costante per p. Se n non è primo, si ha che $p \leq \sqrt{n}$.

5. Sia p un numero primo dispari.
   (a) Far vedere che 2 è un quadrato modulo p per $p = 7, 17, 23$, ma non è un quadrato modulo p per $p = 3, 5, 11$.
   (b) Dimostrare che 2 è un quadrato modulo p se e solo se $p \equiv \pm 1 \pmod 8$.

Questo è l'ultimo esercizio del 5^o foglio di esercizi ed è stato fatto in classe.

Per $p = 7, 17, 23$ si ha che $2^{(p-1)/2} \equiv +1 \pmod p$, dimostrando che 2 è quadrato modulo p. Infatti, si ha che $3^2 \equiv 2 \pmod 7$, $6^2 \equiv 2 \pmod{17}$ e $5^2 \equiv 2 \pmod{23}$. D'altraparte, per $p = 3, 5, 11$ si ha che $2^{(p-1)/2} \equiv -1 \pmod p$, dimostrando che 2 non è quadrato modulo p.

Sia $S = \{1, 2, \ldots, \frac{p-1}{2}\}$. Calcoliamo il prodotto P degli elementi dell'insieme $T = \{2a : a \in S\} = \{2, 4, \ldots, (p-1)\}$. Abbiamo che

$$P \;=\; \prod_{a \in S} 2a \;=\; 2^{\frac{p-1}{2}} \prod_{a \in S} a.$$

Poi osserviamo che S è unione disgiunta dei due sottoinsiemi $S_1 = \{2a : 1 \leq a < \frac{p}{4}\}$ e $S_2 = \{p - 2a : \frac{p}{4} < a \leq \frac{p-1}{2}\}$. Infatti, entrambi sono contenuti in S e hanno intersezione vuota. Il fatto che $\#S_1 + \#S_2 = \#S$ ci fa concludere. Questo fatto implica che

$$\prod_{a \in S} a \;=\; \prod_{b \in S_1} b \cdot \prod_{b \in S_2} b \;\equiv\; \prod_{1 \leq a < \frac{p}{4}} 2a \cdot \prod_{\frac{p}{4} < a \leq \frac{p-1}{2}} (p - 2a) \;\equiv\; (-1)^{\#S_2} \prod_{a \in S} 2a \pmod p.$$

Sostituendo questo nella espressione sopra vediamo che 2 è quadrato modulo p se e solo se $\#S_2$ è pari. Questo succede se e solo se $p \equiv \pm 1 \pmod 8$, come richiesto.