Teoria Elementare dei Numeri (Schoof) 1^o compito 3 dicembre 2007, ore 16:00–18:00.

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 n un numero di tre cifre in base 10. Supponiamo che $n \equiv 3 \pmod 7$, $n \equiv 2 \pmod{11}$ e $n \equiv 1 \pmod{13}$. Determinare n.

   Questo esercizio è una piccola variazione dell'esercizio 7 sul primo foglio. La risposta è 794.

2. Sia p un numero primo. Dimostrare: per ogni $\overline{x} \in \mathbf{Z}_p^*$ si ha che $\overline{x}$ è quadrato in $\mathbf{Z}_p^*$ se e solo se $\overline{x}^{(p-1)/2} = \overline{1}$ in $\mathbf{Z}_p^*$.

   Questo esercizio è l'esercizio 9 (b) del terzo foglio.

3. (a) Calcolare una radice primitiva g modulo 23.
   (b) Calcolare il logaritmo discreto di $\overline{2} \in \mathbf{Z}_{23}^*$ rispetto a g.

   Una radice primitiva modulo 23 è $g = 5$. Siccome $5^2 \equiv 2 \pmod{23}$ abbiamo che $\log_5(2) = 2$.

4. Sia E la curva di equazione $Y^2 = X^3 + X + 4$ modulo 13. Sia P il punto $(9, 1)$.
   (a) Controllare che si tratta di una curva ellittica e che P sta sulla curva.
   (b) Calcolare l'ordine di P.

   Il discriminante $4 + 27 \cdot 4^2 \equiv 7 \pmod{13}$ non è zero. Si tratta quindi di una curva ellittica. Il punto P sta sulla curva. Si calcola che $2P = (7, -4)$, $4P = (0, -2)$ e $8P = (9, 1)$. Siccome $8P = P$, l'ordine del punto P è uguale a 7.

5. Sia $x \in \mathbf{Z}$ e sia $n = x^4 + 1$.
   (a) Calcolare n per $x = 1, 2, 3, 4$.
   (b) Dimostrare: se x è dispari, allora n è divisibile per 2, ma non per 4.
   (c) Dimostrare che i divisori primi dispari di n sono sempre congrui a 1 (mod 8).

   (a) Per $n = 1, 2, 3, 4$ abbiamo che $x = 2, 17, 82$ e 257.
   (b) Se x è dispari, abbiamo che $n = x^4 + 1 \equiv 1 + 1 \equiv 0 \pmod 2$. D'altra parte, siccome per ogni $x \in \mathbf{Z}$ dispari si ha che $x^2 \equiv 1 \pmod 4$, abbiamo che $x^4 + 1 \equiv 1 + 1 \equiv 2 \pmod 4$. Vediamo che 4 non divide $x^4 + 1$.
   (c) Sia p un primo che divide $n = x^4 + 1$. Allora $x^4 \equiv -1 \pmod p$. Questo implica che $x^8 \equiv 1 \pmod p$ e, siccome p è dispari, che l'ordine di $x \pmod p$ è uguale a 8. Concludiamo che 8 divide $\#\mathbf{Z}_p^*$. In altre parole $p \equiv 1 \pmod 8$, come richiesto.