Teoria Elementare dei Numeri (Schoof) 3^o compito 11 giugno 2008, ore 10:00–12:00.

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

Risolvere gli esercizi. Accompagnare le risposte con spiegazioni *chiare ed essenziali*. Ogni esercizio vale 7.5 punti.

1. Sia E la curva di equazione $Y^2 = X^3 + X + 1$ su $\mathbf{Z}_5$.
   (a) Controllare che si tratta di una curva ellittica.
   (b) Esibire i punti di $E(\mathbf{Z}_5)$ che hanno ordine 3.

   Il discriminante della curva è uguale a $4 + 27 \not\equiv 0 \pmod 5$ e si tratta quindi di una curva ellittica. Il gruppo $E(\mathbf{Z}_5)$ ha 9 elementi. Solo i due punti $(2, \pm 1)$ hanno ordine 3.

2. Esibire gli elementi di ordine 3 del gruppo $\mathbf{Z}_{91}^*$.

   Si ha che $91 = 7 \cdot 13$. Le soluzioni della congruenza $x^3 \equiv 1 \pmod 7$ sono $x \equiv 1, 2$ e $4 \pmod 7$. Similmente le soluzioni della congruenza $x^3 \equiv 1 \pmod{13}$ sono $x \equiv 1, 3$ e $9 \pmod{13}$. Le soluzioni della equazione $x^3 \equiv 1 \pmod{91}$ si ottengono applicando il Teorema Cinese del resto. In questo modo troviamo $3 \times 3 = 9$ soluzioni e quindi $9 - 1 = 8$ elementi di ordine 8. Essi sono le classi $9, 16, 22, 29, 53, 74, 79, 81 \pmod{91}$.

3. Supponiamo che $n \in \mathbf{Z}$ abbia la proprietà che $\mathrm{mcd}(n, 10) = 1$. Spiegare perché n divide un numero che ha tutte le cifre uguali. (Per esempio 37 divide 111).

   Sia $k = \#\mathbf{Z}_n^*$. Per il Teorema di Lagrange l'elemento $\overline{10} \in \mathbf{Z}_n^*$ ha la proprietà che $\overline{10}^k = \overline{1}$ in $\mathbf{Z}_n^*$. In altre parole, il numero n divide $10^k - 1 = 9999\ldots999$ come richiesto.

4. Esibire una radice primitiva g modulo 47 e calcolare il logaritmo di $2 \in \mathbf{Z}_{47}^*$ rispetto alla radice primitiva g.

   La più piccola radice primitiva modulo 47 è $g = \overline{5}$. Per calcolare il logaritmo discreto di $\overline{2} \in \mathbf{Z}_{47}^*$ cerchiamo relazioni moltiplicative fra i numeri piccoli. Abbiamo che $50 \equiv 3 \pmod{47}$ e quindi $2\log 5 + \log 2 \equiv \log 3 \pmod{46}$. Similmente, $48 \equiv 1 \pmod{47}$ ci da che $\log 3 + 4\log 2 \equiv 0 \pmod{46}$. Combinando, si ha che $5\log 2 \equiv -2\log 5 \pmod{46}$ e quindi $\log 2 = -2/5 \equiv 18 \pmod{46}$.