Crittografia (Schoof) 3^o compito 21 settembre 2010, ore 10:00–12:00.

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

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

1. Sia p un numero primo. Il gruppo $\mathbf{Z}_{p^2}^*$ è ciclico: un generatore g di $\mathbf{Z}_{p^2}^*$ si chiama *radice primitiva* di $\mathbf{Z}_{p^2}^*$. Dati $x \in \mathbf{Z}_{p^2}^*$ e una radice primitiva $g \in \mathbf{Z}_{p^2}^*$, *il logaritmo discreto* di x rispetto alla radice primitiva g è per definizione ogni $m \in \mathbf{Z}$ tale che $x = g^m$.
   Determinare una radice primitiva g di $\mathbf{Z}_{25}^*$. Calcolare il logaritmo discreto (rispetto alla radice primitiva g) di $\overline{11} \in \mathbf{Z}_{25}^*$.

2. (a) Sia $p > 2$ un primo e sia q un divisore di $2^p - 1$. Dimostrare che $q \equiv 1 \pmod{2p}$.
   (b) Fattorizzare 2047 in fattori primi.

3. Sia E la curva di equazione $Y^2 = X^3 + X + 4$ su $\mathbf{Z}_7$.
   (a) Verificare che si tratta di una curva ellittica.
   (b) Esibire un punto di ordine 5 in $E(\mathbf{Z}_7)$.

4. Siano $p, q, r \in \mathbf{Z}_{>0}$. Supponiamo che q sia un primo. Dimostrare che se valgono
   - $p < q^2$,
   - $r^q \equiv 1 \pmod{p}$,
   - $\mathrm{mcd}(r-1, p) = 1$,

   allora anche p è primo.

1. L'elemento $2 \in \mathbf{Z}_{25}^*$ ha ordine $20 = \#\mathbf{Z}_{25}^*$ e quindi è una radice primitiva. Si ha che $2^{16} = 16^4 = (1+15)^4 \equiv 1 + 4 \cdot 15 \equiv 11 \pmod{25}$ e quindi il logaritmo di 11 rispetto all radice primitiva 2 è uguale a 16.

2. Se q è un primo che divide $2^p - 1$, allora l'ordine di $2 \in \mathbf{Z}_q^*$ è uguale a p e quindi p divide $q - 1 = \#\mathbf{Z}_q^*$. Questo dimostra che $q \equiv 1 \pmod{p}$. Poiché q è dispari si ha $q \equiv 1 \pmod{2}$ e quindi per il Teorema cinese vale anche $q \equiv 1 \pmod{2p}$. Concludiamo che il divisore d, essendo prodotto di primi q, è anche congruo a 1 (mod $2p$).

3. Il discriminante è $4 - 4^2 \not\equiv 0 \pmod{7}$ e si tratta quindi di una curva ellittica. I punti di $E(\mathbf{Z}_7)$ sono ∞, $(0, \pm 2)$, $(2, 0)$, $(4, \pm 3)$ e $(-1, \pm 3)$ e $(-2, \pm 1)$. Questo implica che $E(\mathbf{Z}_7) \cong \mathbf{Z}_{10}$. Poiché il punto $P = (0, 2)$ soddisfa $P + P = (4, 4)$, il quale non è zero, concludiamo che il punto $(4, 4)$ ha ordine 5 come richiesto.

4. Sia d un divisore primo di p. Allora si ha che $r^q \equiv 1 \pmod{d}$ mentre $r \not\equiv 1 \pmod{d}$. Ne segue che l'ordine di $r \in \mathbf{Z}_d^*$ è q e quindi che q divide $\#\mathbf{Z}_d^*$. Questo implica che $\sqrt{p} < r < d$ e quindi che ogni divisore primo di p è $> \sqrt{p}$. Concludiamo che p è primo.