Crittografia (Schoof) 1^o compito 28 giugno 2010, ore 16:00–18:00.

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

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

1. Determinare una radice primitiva g di $\mathbf{Z}_{47}^*$. Calcolare il logaritmo discreto (rispetto alla radice primitiva g) di $\overline{4} \in \mathbf{Z}_{47}^*$.

2. Sia $n \in \mathbf{Z}$ pari. Dimostrare che ogni divisore di $n^2 + 1$ è congruo a 1 (mod 4).

3. Sia E la curva di equazione $Y^2 = X^3 - X$ su $\mathbf{Z}_5$.
   (a) Verificare che si tratta di una curva ellittica.
   (b) Determinare la struttura del gruppo $E(\mathbf{Z}_5)$.

4. Sia $n \in \mathbf{Z}_{>1}$. Sia $a \in \mathbf{Z}$ e sia d un divisore di $n - 1$ tali che
   - $a^d \equiv 1 \pmod{n}$;
   - $\mathrm{mcd}(a^{d/q} - 1, n) = 1$ per ogni divisore primo q di d.

   Dimostrare che se $d > \sqrt{n}$, allora n è primo.

1. Questo è il primo esercizio del Foglio 4. Abbiamo solo che $p = 47$ invece di $p = 41$. Si verifica che 5 è una radice primitiva modulo 47 e che $5^{18} \equiv 2 \pmod{47}$. Il logaritmo discreto cercato è quindi uguale a $2 \cdot 18 = 36 \pmod{46}$.

2. Questo è il primo esercizio del Foglio 2. Se p è un divisore primo di $n^2 + 1$, allora $n^2 \equiv -1 \pmod{p}$. Poiché $p \neq 2$, questo implica che l'immagine di n nel gruppo $\mathbf{Z}_p^*$ ha ordine 4. Come consequenza si ha che 4 divide $p-1$. Poiché ogni divisore d di n^2+1 è prodotto di divisori primi, si ha che $d \equiv 1 \pmod{4}$.

3. Questo è una variazione del quarto esercizio del Foglio 3. Si verifica che il discriminante di E non si annulla modulo 5 e si tratta quindi di una curva ellittica. La curva E ha otto punti con coordinate in $\mathbf{Z}_5$ (incluso il punto all'infinito). I punti di ordine 2 sono tre (vale a dire i punti $(0, 0)$ e $(\pm 1, 0)$). L'unico gruppo abeliano di ordine 8 con tre elementi di ordine 2 è $\mathbf{Z}_4 \times \mathbf{Z}_2$. Abbiamo quindi che $E(\mathbf{Z}_5)$ è isomorfo a $\mathbf{Z}_4 \times \mathbf{Z}_2$.

4. Sia p un divisore primo di n. L'immagine di a nel gruppo $\mathbf{Z}_p^*$ ha ordine d. Questo implica che d divide $\#\mathbf{Z}_p^* = p - 1$ e quindi che $p > d$. Se $d > \sqrt{n}$, segue che $p > \sqrt{n}$. In altre parole, ogni divisore primo di n soddisfa $p > \sqrt{n}$. Questo implica che n è primo.