Teoria Elementare dei Numeri | Appello 1 | 3 febbraio 2009, ore 9:30–11:30.

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

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare e sintetiche*. NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 7,5 punti.

1. Calcolare $\varphi(2009)$, spiegando quali proprietà della funzione φ di Eulero sono state usate.

Sol. Fattorizzando 2009 troviamo: $2009 = 7^2 \cdot 41$, da cui segue che

$$\varphi(2009) = \varphi(7^2)\varphi(41) = 7^2(1 - \frac{1}{7})(41 - 1) = 1680.$$

In generale,

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p}),$$

dove p varia tra i divisori primi distinti di n.

2. Sia $E(\mathbf{Z}_{11})$ la curva di equazione $Y^2 = X^3 - 4X + 1$.
   (a) Verificare che $E(\mathbf{Z}_{11})$ è una curva ellittica e che $P = (1, 3)$ sta sulla curva.
   (b) Calcolare l'ordine di P.

Sol. (a) Il discriminante della curva risulta $27B^2 + 4A^3 \equiv 5 \cdot 1 + 4(-4)^3 \equiv 2 \not\equiv 0 \mod 11$. Dunque si tratta di una curva ellittica. Sostituendo le coordinate di P nell'equazione di $E(\mathbf{Z}_{11})$ troviamo

$$9 \equiv -2 \mod 11,$$

per cui P appartiene a $E(\mathbf{Z}_{11})$.

(b) Sia $P = (x_1, y_1) = (1, 3)$. Calcoliamo $2P$:
$m = (3x_1^2 + A)(2y_1)^{-1} \equiv 9 \mod 11$, da cui $2P = (x_2, y_2) = (m^2 - 2x_1, m(x_1 - x_2) - y_1) \equiv (2, 10)$;
calcoliamo $3P = P + 2P$:
$m = (y_2 - y_1)(x_2 - x_1)^{-1} \equiv 7 \mod 11$, da cui $3P = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1) \equiv (2, 1)$. Poiché $2P$ e $3P$ hanno la stessa ascissa, ma diversa ordinata, sono uno inverso dell'altro nel gruppo dei punti della curva. In altre parole $2P + 3P = 5P = (\infty, \infty)$. L'ordine di P è 5: osserviamo che 5 è il più piccolo multiplo di P uguale al punto all'infinito....

3. Sia $p = 41$.
   (a) Determinare una radice primitiva $\bar{g}$ in $\mathbf{Z}_{41}^*$.
   (b) Calcolare $log(2)$ rispetto alla radice $\bar{g}$.

(a) $\bar{g}$ è una radice primitiva se e solo se $\bar{g}^{40/d} \not\equiv 1 \mod 41$, per ogni d divisore primo di 40 (ossia $d = 2$ e $d = 5$). Verifichiamo che $\bar{7}$ è una radice primitiva: infatti $\bar{7}^8 \equiv 37 \not\equiv 1$ e $\bar{7}^{20} \equiv 40 \not\equiv 1$ modulo 41. Calcoliamo $log(2)$ con il metodo baby-step-giant-step.
Fissiamo $m \sim \sqrt{41} \sim 6$.
Baby-steps:

$$\bar{7}^0 \equiv 1, \quad \bar{7}^1 \equiv 7, \quad \bar{7}^2 \equiv 8, \quad \bar{7}^3 \equiv 15, \quad \bar{7}^4 \equiv 23, \quad \bar{7}^5 \equiv 38$$

$$\bar{7}^{-6} \equiv 39$$

Giant-steps:

$$\bar{2} \cdot \bar{7}^0 \equiv 2, \quad 2 \cdot \bar{7}^{-6} \equiv 37, \quad 2 \cdot \bar{7}^{-12} \equiv 8,$$

da cui $\bar{7}^2 \equiv 2 \cdot \bar{7}^{-12}$ e $log(2) = 14$.

4. Sia $p > 1$ un primo. Determinare $(p - 1)!$ modulo p, (ossia il resto della divisione di $(p - 1)!$ per p).

Vedi EAL 2008, Esercizi 4, n.20.