Teoria Elementare dei Numeri Appello 1 14 febbraio 2013, ore 11–13.

*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. *Sia* $p = 59$ *e sia* $E: \quad Y^2 = X^3 + 3X + 4$.
   *(a) Verificare che* $E$ *definisce una curva ellittica su* $\mathbf{Z}_{59}$ *e che* $P = (0, 2) \in E(\mathbf{Z}_{59})$.
   *(b) Calcolare* $2P = P + P$.
   *(c) Determinare l'intervallo di Hasse per* $p = 59$. *Determinare* $\#E(\mathbf{Z}_{59})$, *sapendo che* $3P$ *ha ordine 9.*

*Sol.* (a) Il discriminante della curva è dato da $\Delta = 4A^3 + 27B^2 = 4 \cdot 3^2 + 27 \cdot 4^2 \equiv 9 \not\equiv 0 \mod 59$. Di conseguenza $E(\mathbf{Z}_{59})$ è una curva ellittica.
Inoltre $P = (0, 2) \in E(\mathbf{Z}_{59})$ in quanto $2^2 \equiv 0^3 + 3 \cdot 0 + 4 \mod 59$.

(b) Calcoliamo $P + P$:
il coefficiente angolare della "tangente" alla curva in $P$ è dato da

$$m = (3 \cdot 0^2 + 3)(2 \cdot 2)^{-1} \equiv 3 \cdot 4^{-1} \equiv 3 \cdot 15 \equiv 45 \mod 59.$$

Le coordinate di $P + P$ sono date rispettivamente da:
$x = (45)^2 - 2 \cdot 0 \equiv 19 \mod 59$,
$y = -(45 \cdot 19 + 2) \equiv 28 \mod 59$.
Dunque $P + P = (19, 28) \in E(\mathbf{Z}_{59})$.

(c) Per $p = 59$, l'intervallo di Hasse $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$ si può approssimare con $[44, 76]$ (usando $\sqrt{p} \sim 8$).
Se $3P$ ha ordine 9, allora $9(3P) = 27P = \infty$. Ne segue che l'ordine di $P$ è 27: infatti $ord(P) \neq 1, 3$, perché $P, 3P \neq \infty$. Inoltre $ord(P) \neq 9$, perché altrimenti $3P$ avrebbe ordine 3 e non 9. Se l'ordine di $P$ è 27, allora l'ordine della curva è sua volta divisibile per 27. L'unico multiplo di 27 nell'intervallo di Hasse è 54. Conclusione $\#E(\mathbf{Z}_{59}) = 54$.

2. *Sia* $B = 100000$ *e sia* $N = 10^{1000}$. *Determinare quanti numeri* $B$*-smooth ci sono approssimativamente nell'intervallo* $[N - A, N + A]$, *con* $A = 10^{100}$.

*Sol.* Poiché $A << N$, la probabilità che un intero $x \in [N - A, N + A]$ sia $B$-smooth si può approssimare uniformemente con

$$u^{-u}, \qquad u = \ln N / \ln B.$$

Nel nostro caso risulta

$$u = \ln N / \ln B = (1000 \ln 10)/(5 \ln 10) = 200, \qquad u^{-u} \sim 6,22310^{-461} \sim 0.6223/10^{460},$$

cioè i numeri $B$-smooth dell'ordine di grandezza di $N$ sono meno di uno su $10^{460}$. Vista l'ampiezza del nostro intervallo, pari a $2A = 2 \cdot 10^{100}$, è probabile che al suo interno non si trovi alcun intero $B$-smooth.

3. *Sia* $p = 59$.
   *(a) Verificare che* $\bar{2}$ *è una radice primitiva in* $\mathbf{Z}_{59}$.
   *(b) Calcolare il logaritmo discreto* $\log_{\bar{2}} \bar{5}$.

*Sol.* (a) Abbiamo $p - 1 = 58 = 2 \cdot 29$. Si verifica facilmente che $\bar{2}^{58/28} = \bar{2}^2 \not\equiv \bar{1} \mod 59$ e similmente che $\bar{2}^{58/2} = \bar{2}^{29} \equiv -1 \not\equiv \bar{1} \mod 59$. Dunque $\bar{2}$ è una radice primitiva in $\mathbf{Z}_{59}$.

(b) Si ha che $64 = 2^6 \equiv 5 \mod 59$, da cui $\log_{\bar{2}} \bar{5} = 6 \log_{\bar{2}} \bar{2} = 6$.

4. *Sia* $n = 4633$. *Date le congruenze*

$$67^2 \equiv -144 \mod 4633, \qquad 64^2 \equiv -9 \mod 4633$$

*quali sono possibili fattori non banali di* $n$*?*

*Sol.* Moltiplicando fra loro le relazioni quadratiche

$$(67)^2 \equiv -144 = -(12)^2 \mod 4633, \qquad (68)^2 \equiv -9 = -(3)^2 \mod 4633$$

otteniamo

$$(67 \cdot 68)^2 \equiv (12 \cdot 3)^2 \mod 4633.$$

Poniamo $a = 67 \cdot 68 \equiv 4556 \mod 4633$ e $b = 36 \mod 4633$.
Possiamo allora cercare fattori non banali di 4633 fra $\gcd(a \pm b, 4633)$: infatti

$$\gcd(4556, 4633) = 41, \qquad \gcd(4520, 4633) = 113, \qquad 41 \cdot 113 = 4633.$$

5. *Calcolare* $\varphi(6039)$*, spiegando quali proprietà della funzione* $\varphi$ *di Eulero vengono usate.*

*Sol.* Poiché $6039 = 3^2 \cdot 11 \cdot 61$, abbiamo

$$\varphi(6039) = \varphi(3^2)\varphi(11)\varphi(61) = (3^2 - 3) \cdot 10 \cdot 60 = 3600.$$

Le proprietà di $\varphi$ che abbiamo usato sono:
- se $gcd(a, b) = 1$, allora $\varphi(ab) = \varphi(a)\varphi(b)$;
- se $a$ è primo, allora $\varphi(a) = a - 1$ e in generale $\varphi(a^k) = a^k - a^{k-1}$, per ogni $k \geq 1$.