TEN 2018. Esercizi 4.

Per questi esercizi è necessario PARI/GP.

1. Sia $p = 10000000019$ e sia data l'equazione $E: \quad Y^2 = X^3 + X + 7806879540$.
   (a) Verificare che E definisce una curva ellittica su $\mathbb{Z}_p$.
   (b) Calcolare $\#E(\mathbb{Z}_p)$ e verificare che appartiene all'intervallo di Hasse.
   (c) Enunciare il teorema di Lagrange per $(E(\mathbb{Z}_p), +)$.
   (d) Verificare che $P = (5776216132, 9201595107)$ appartiene a $E(\mathbb{Z}_p)$.

2. Sia $p = 10739$ e sia data l'equazione $E: \quad Y^2 = X^3 + X + 3985$.
   (a) Verificare che E definisce una curva ellittica su $\mathbb{Z}_p$.
   (b) Calcolare $\#E(\mathbb{Z}_p)$ e fattorizzarlo.
   (c) Verificare che $P = (6712, 5889)$ appartiene a $E(\mathbb{Z}_p)$.
   (d) Determinare l'ordine di P in $E(\mathbb{Z}_p)$.

3. Sperimentare col programma
   `http://www.mat.uniroma2.it/~geo2/TEN/EC-examples.txt`.

4. Ripetere i comandi del file qui sotto (in PARI/GP) fino a fattorizzare n
   `http://www.mat.uniroma2.it/~geo2/TEN/ECM-fattorizza.txt`.
   Ridurre la curva modulo il fattore p così trovato e verificare che $E(\mathbb{Z}_p)$ ha ordine B-smooth.

5. Sperimentare col programma
   `http://www.mat.uniroma2.it/~geo2/TEN/ECM-aperto.txt`
   Per ogni curva E il cui ciclo non ha fattorizzato n, confrontare il fattore più grosso di $\#E(\mathbb{Z}_p)$ con lo smoothness bound $B1$ e il numero primo più grosso fra $B1$ e $B2$. Per ogni curva che fattorizza n, verificare che $\#E(\mathbb{Z}_p)$ è $B1$-smooth oppure è il prodotto di un intero $B1$-smooth e uno (uno solo!) dei primi fra $B1$ e $B2$.

6.

7.