

1. Sia data l'equazione $E: Y^2 = X^3 + 2X + 1$ e sia $p = 7$.
 - (a) Verificare che E definisce una curva ellittica su $\mathbb{Z}_7$.
 - (b) Determinare tutti i punti di $E(\mathbb{Z}_7)$.
 - (c) Che ordini possono avere i punti di $E(\mathbb{Z}_7)$?
 - (d) Che tipo di gruppo è $(E(\mathbb{Z}_7), +)$?
 - (e) Formulare il teorema di Lagrange per il gruppo abeliano $(E(\mathbb{Z}_7), +)$.
2. Sia data l'equazione $E: Y^2 = X^3 + 2X + 1$ e sia $p = 11$.
 - (a) Verificare che E definisce una curva ellittica su $\mathbb{Z}_{11}$.
 - (b) Determinare tutti i punti di $E(\mathbb{Z}_{11})$.
 - (c) Che ordini possono avere i punti di $E(\mathbb{Z}_{11})$?
 - (d) Che tipo di gruppo è $(E(\mathbb{Z}_{11}), +)$?
 - (e) Formulare il teorema di Lagrange per il gruppo abeliano $(E(\mathbb{Z}_{11}), +)$.
3. Sia data l'equazione $E: Y^2 = X^3 + X$.
 - (a) Verificare che E definisce una curva ellittica su $\mathbb{Z}_p$ per ogni primo $p > 2$.
 - (b) Sia $p > 2$. Verificare che il gruppo $E(\mathbb{Z}_p)$ ha tre punti di ordine 2 se e solo se -1 è un quadrato modulo p e che questo avviene se e solo se $p \equiv 1 \pmod{4}$.
 - (c) Concludere che in questi casi il gruppo $(E(\mathbb{Z}_p), +)$ non può essere ciclico.
4. Considerare l'equazione $E: Y^2 = X^3 + X$ su $\mathbb{Z}_5$.
 - (a) Determinare i punti di ordine 2 della curva ellittica E su $\mathbb{Z}_5$.
 - (b) Verificare che la somma di due punti (distinti) di ordine 2 è ancora un punto di ordine 2.
5. Tutti i compiti d'esame degli anni passati contengono esercizi (risolti) sulle curve ellittiche.

Per questi esercizi è necessario PARI/GP (vedi <http://www.mat.uniroma2.it/geo2/TEN/ECpari.rtf>)

6. Sia $p = 10000000019$ e sia data l'equazione $E: Y^2 = X^3 + X + 7806879540$.
 - (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 $E(\mathbb{Z}_p)$.
7. Sia $p = 10739$ e sia data l'equazione $E: Y^2 = X^3 + X + 3985$.
 - (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 $E(\mathbb{Z}_p)$.
8. Sperimentare col programma
<http://www.mat.uniroma2.it/geo2/TEN/EC-examples.txt>.
9. 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.
10. 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 $B2$.