TEN 2017. Esercizi 6. Curve ellittiche su $\mathbb{Z}_p$.

Per controllare gli esercizi e sperimentare nuovi esempi, potete usare PARI/GP: vedi file ECpari.rtf.

1. Sia data l'equazione $E: \quad Y^2 = X^3 + 2X + 1$ 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 $E: \quad Y^2 = X^3 + 2X + 1$ 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 $E: \quad Y^2 = X^3 + X$.
   (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 $p \equiv 1 \bmod 4$.
   (c) Concludere che in questi casi il gruppo $(E(\mathbb{Z}_p), +)$ non può essere ciclico.

4. Considerare l'equazione $E: \quad Y^2 = X^3 + X$ 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.