Curve ellittiche

Curve algebriche su un campo K che hanno la forma:

$$E(a,b,c,d,e) = \{(x,y) \in K^2 \mid y^2 + ay + by = x^3 + cx^2 + dx + e\} \cup \{O\}$$

con $a, b, c, d, e \in K$. O è il punto all'infinito in direzione dell'asse y ed è l'elemento neutro per l'operazione di addizione (su $\mathbb{R}$ non serve aggiungerlo).

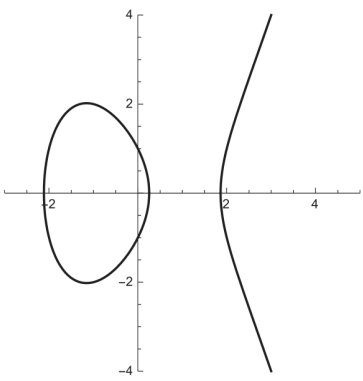
Se $\operatorname{char} K \neq 2, 3$ allora possiamo scrivere in forma normale di Weierstrass:

$$E(a,b) = \{(x,y) \in K^2 \mid y^2 = x^3 + ax + b\}.$$

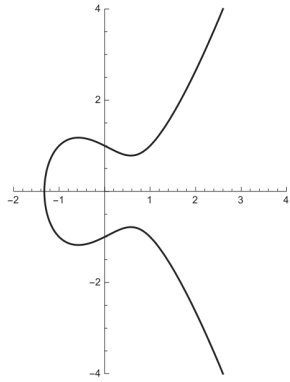
Come gruppo abeliano

Supponendo che $4a^3 + 27b^2 \neq 0$, ovvero se $x^3 + ax + b$ non ha radici multiple e quindi non ci sono cuspidi o nodi, i punti di una curva ellittica formano un gruppo abeliano.

Le curve che soddisfano questa condizione possono avere due forme:



(a) Curva $y^2 = x^3 - 4x + 1$



(b) Curva $y^2 = x^3 - x + 1$

Il primo caso si ha quando il polinomio in x ha 3 radici reali, l'altra quando ne ha una sola.

Su campi finiti

In crittografia si usano curve su campi finiti. Le curve su $\mathbb{F}_p$ si dicono *prime*, quelle su $\mathbb{F}_{2^n}$ *binarie* (hanno caratteristica 2 quindi non vale la forma normale di Weierstrass, non le vediamo).

Una curva su $\mathbb{F}_p$ è un insieme finito di punti nel primo quadrante e con simmetria rispetto a $y = p/2$.

$$E_p(a,b) = \{(a,b) \in \mathbb{Z}/p\mathbb{Z} \mid y^2 \bmod p = (x^3 + ax + b) \bmod p\} \cup \{O\}.$$

L'opposto di (x,y) è $(x, p-y)$. Se il discriminante (modulo p) non è 0 valgono le formule per la somma, interpretate nel contesto di $\mathbb{F}_p$.

Non tutte le curve garantiscono la stessa sicurezza, si usano quelle consigliate dal NIST (e.g. P-384).