Ordine di una curva ellittica

Numero di punti della curva, contando anche O.

Non c'è un modo veloce per determinarlo: in una curva $E_p(a, b)$ si valuta $x^3 + ax + b$ in tutti gli x possibili contando i risultati che sono residui quadratici modulo p (che in tutto sono $\frac{p-1}{2}$).

Per il teorema di Hasse, se n è l'ordine della curva allora:

$$|n - (p + 1)| \leq 2\sqrt{p}$$

quindi $n \sim p$.

Ordine di un punto

ord P è il più piccolo intero positivo n tale che $nP = O$.