Logaritmo discreto

Trovare x in:

$$a^x \equiv b \mod p$$

ha sempre soluzione se a e un generatore, ma non è noto a priori l'ordine in cui gli elementi sono generati ($a^x \bmod p$ non è monotona crescente).

Il miglior algoritmo conosciuto su macchine tradizionali ha complessità $O(2^{\sqrt{b \log b}})$ (subesponenziale). Sfrutta la struttura di campo di $\mathbb{Z}/p\mathbb{Z}$, perciò non è applicabile su curve ellittiche (che non sono campi), ed è il motivo per cui il logaritmo discreto su curve ellittiche è più difficile. Polinomiale su macchine quantistiche.