Equivalente di operazioni modulari su curve ellittiche

Se la curva è un gruppo abeliano:

$ab \bmod m$	$P + Q$
$a^b \bmod m$	kP
$\log_a b \bmod m$	trovare k da $Q = kP$ ($\log_P Q$)

Il logaritmo discreto su curve ellittiche è più difficile dell'equivalente problema in aritmetica modulare ($O(2^{b/2})$ contro $O(2^{\sqrt{b \log b}})$), e si conoscono solo algoritmi brute-force (puramente esponenziali). Non è comunque NP-hard e può essere risolto efficientemente su macchine quantistiche.