Ottavio G. Rizzo – Milano

Secondo Convegno Italiano di Teoria dei Numeri
Parma, 13–15 Novembre 2003

Sia E un monoide addittivo e supponiamo di voler calcolare $12P$ dove $P \in E$. Il metodo più ovvio è calcolare

$$12P = \underbrace{P + P + \cdots + P}_{12 \text{ volte}}$$

È chiaro, però, che undici addizioni sono troppe: possiamo ad esempio calcolare

$$12P = 2\big(2(2P + P)\big)$$

con solo tre raddoppi ed un'addizione. È facile convincersi che questa decomposizione è strettamente connessa con la *catena d'addizione* $1, 2, 3, 6, 12$; dove ogni termine è ottenuto come somma di due termini precedenti. Se E è un gruppo, abbiamo a disposizione anche le sottrazioni, in questo modo possiamo calcolare, ad esempio

$$15P = 2\big(2(2P + P) + P\big) + P = 2 \cdot 2 \cdot 2 \cdot 2P - P$$

con quattro raddoppi ed una sottrazione piuttosto che tre raddoppi e tre addizioni. Questo è conveniente, però, solo nei casi in cui l'inversione è gratuita, ad esempio il gruppo dei punti razionali di una curva ellittica.

Se occorre calcolare multipli molto grossi di P, ad esempio se si usa il metodo di fattorizzazione degli interi basato sulle curve ellittiche o nelle applicazioni crittografiche, è importante ridurre al minimo il numero di operazioni, cioè trovare una catena il più corta possibile. Questo problema è estremamente difficile e normalmente ci si accontenta di trovare, rapidamente, una catena sufficientemente breve.

Illustrerò alcuni dei metodi principali, con i relativi vantaggi e svantaggi: binario, 2^m-ario, finestre scorrevoli, NAF. Tempo permettendo, illustrerò anche alcuni metodi recentissimi che sfruttano le proprietà del Frobenius in particolari classi di curve ellittiche (curve di Koblitz).

Presenterò infine dei risultati preliminari sul numero di operazioni richieste dalle finestre scorrevoli.