TEN 2008. Il metodo delle curve ellittiche *ECM*

Sia $n$ un numero composto e sia $p$ un suo divisore primo. Il metodo di fattorizzazione delle curve ellittiche ricalca in parte il metodo $p-1$ di Pollard: invece del gruppo $\mathbb{Z}_p^*$, sfrutta il gruppo $E(\mathbb{Z}_p)$ dei punti di una curva ellittica $E$ su $\mathbb{Z}_p$. Il metodo $p-1$ di Pollard fallisce se $n$ non ha fattori primi $p$ per cui l'ordine $\#\mathbb{Z}_p^* = p-1$ del gruppo $\mathbb{Z}_p^*$ è $B$-smooth. Il metodo delle curve ellittiche fallisce per una data curva $E$ se $n$ non ha fattori primi $p$ per cui l'ordine $\#E(\mathbb{Z}_p)$ del gruppo $E(\mathbb{Z}_p)$ è $B$-smooth. Ma questo metodo ha il vantaggio che sullo stesso $\mathbb{Z}_p$ ci sono diverse curve ellittiche e quindi diversi gruppi $E(\mathbb{Z}_p)$ a disposizione. Se l'ordine del gruppo dei punti di una data curva $E(\mathbb{Z}_p)$ non è $B$-smooth, possiamo tentare con un'altra.

**Metodo delle curve ellittiche ECM.**

Sia $n$ un numero intero. Sia $E$ una curva ellittica su $\mathbb{Z}_n$

$$Y^2 = X^3 + AX + B, \qquad \Delta = 4A^3 + 27B^2 \in \mathbb{Z}_n^*.$$

Anche quando $n$ non è primo, i punti di $E(\mathbb{Z}_n)$ si possono sommare e duplicare con le stesse formule. Anche in questo caso per sommare o duplicare punti di $E(\mathbb{Z}_n)$ è necessario calcolare l'inverso moltiplicativo di un certo intero $a$ modulo $n$ (se si sommano punti distinti, $a = x_2 - x_1$ è la differenza delle ascisse di tali punti; se si duplica un punto, $a = 2y_1$ è due volte l'ordinata di tale punto). Ogni volta che questo inverso non esiste il risultato della somma o della duplicazione in questione è *un* punto all'infinito di $E(\mathbb{Z}_n)$ (vedi Esercizio ??). Questa circostanza si manifesta attraverso $\gcd(a,n) > 1$.
*Notare che* $\gcd(a,n)$ *è un possibile fattore non banale di* $n$ *!!*

Stimiamo la probabilià che questo accada partendo dalla seguente osservazione:

Sia $p$ un numero primo e sia $E(\mathbb{Z}_p)$ il gruppo dei punti di una curva ellittica su $\mathbb{Z}_p$. Se $k$ è un multiplo intero di $\#E(\mathbb{Z}_p)$, dal Teorema di Lagrange segue che

$$k \cdot P = O \quad \text{in} \quad E(\mathbb{Z}_p), \quad \text{per ogni } P \in E(\mathbb{Z}_p),$$

dove $O$ indica l'elemento neutro, o punto all'infinito, del gruppo $E(\mathbb{Z}_p)$. Questo significa che nel calcolo di $k \cdot P$ appare un intero $a$ che non è invertibile modulo $p$, per cui vale $\gcd(a,p) > 1$.

Sia $n$ un intero, sia $E$ una curva ellittica su $\mathbb{Z}_n$ e sia $P$ un punto di $E(\mathbb{Z}_n)$. Se $p$ è un divisore primo di $n$, allora

$$\#E(\mathbb{Z}_p) \cdot P \in \{\text{insieme dei punti all'infinito di } E(\mathbb{Z}_n)\}.$$

Per quanto osservato sopra infatti,

$$\#E(\mathbb{Z}_p) \cdot P = O \qquad \text{in } E(\mathbb{Z}_p);$$

quindi nel calcolo di $\#E(\mathbb{Z}_p) \cdot P$ in $E(\mathbb{Z}_n)$ appare un intero $a$ con $\gcd(a,p) > 1$. Poiché $p$ divide $n$, vale anche $\gcd(a,n) > 1$ e $\#E(\mathbb{Z}_p) \cdot P$ è un punto all'infinito in $E(\mathbb{Z}_n)$.

*Il problema è costruire un elemento* $a$ *con* $gcd(a,n) > 1$*, senza conoscere* $p$*.*
Questo è possibile per fattori primi particolari: quelli per cui esiste una curva ellittica il cui gruppo dei punti $E(\mathbb{Z}_p)$ su $\mathbb{Z}_p$ è $B$-smooth.

Fissiamo allora un intero $B$.
Sia $k = \Pi p_i^{\alpha_i}$ il prodotto di tutti i numeri primi $p_i \le B$ tali che $p_i^{\alpha_i} \le B$, con $\alpha_i > 0$ massimo.
Se $p$ è un divisore primo di $n$, e l'ordine del gruppo $\#E(\mathbb{Z}_p)$ dei punti di una curva ellittica $E$ su $\mathbb{Z}_p$ è $B$-smooth allora $\#E(\mathbb{Z}_p) \mid k$ e vale

$$k \cdot P = O \quad \text{in} \quad E(\mathbb{Z}_p).$$

In particolare, nel calcolo $k \cdot P$ appare un elemento $a$ con $\gcd(a,p) > 1$ e a maggior ragione $\gcd(a,n) > 1$. Verosimilmente $\gcd(a,n)$ è un fattore non banale di $n$.

**L'algoritmo.**

Sia $n$ il numero da fattorizzare.

Fissati $B$ e $k$ come sopra, costruiamo $E$ una curva ellittica $E$ a caso su $\mathbb{Z}_n$ con un punto $P$ su di essa, nel modo seguente: †

prendiamo un punto a caso

$$P = (X_0, Y_0) \in \mathbb{Z}_n \times \mathbb{Z}_n,$$

prendiamo un coefficiente a caso

$$A \in \mathbb{Z}_n,$$

e consideriamo la curva

$$E: \quad Y^2 = X^3 + AX + B, \qquad \text{con } B = Y_0^2 - X_0^3 - AX_0 \in \mathbb{Z}_n;$$

controlliamo che $\gcd(\Delta, n) = 1$, ossia che il discriminante $\Delta = 4A^3 + 27B^2 \in \mathbb{Z}_n^*$.

CALCOLIAMO

$$k \cdot P \quad \text{su } E(\mathbb{Z}_n).$$

Se durante il calcolo di $k \cdot P$ appare un intero $a$ che non ammette inverso moltiplicativo modulo $n$, e se $1 < \gcd(a,n) < n$, abbiamo un fattore non banale di $n$;
se invece $k \cdot P = Q$ è un punto "al finito" in $E(\mathbb{Z}_n)$, il primo ciclo dell'algoritmo ha fallito;
in tal caso, ripartiamo da una nuova coppia $(E, P)$.

Cerchiamo adesso di valutare le probabilità di successo di trovare un fattore di $n$ con questo algoritmo.

• *Se con questo metodo troviamo un fattore primo $p$ di $n$, che tipo di fattore è ?*

Sappiamo che un ciclo dell'algoritmo individua un fattore primo $p$ di $n$ se il gruppo dei punti $E(\mathbb{Z}_p)$ della curva ellittica usata $E$ ha ordine $B$-smooth.
Viceversa, un fattore primo $p$ individuato in un ciclo di questo algoritmo è con grossa probabilità un primo per cui il gruppo dei punti $E(\mathbb{Z}_p)$ della curva ellittica usata $E$ ha ordine $B$-smooth.
Supponiamo infatti che nel calcolo di $k \cdot P$ in $E(\mathbb{Z}_n)$ compaia un intero $a$ che non è invertibile modulo $n$, per cui $\gcd(a,n) > 1$. Allora esiste un fattore primo $p$ di $n$ per cui vale $\gcd(a,p) > 1$. Questo implica che $k \cdot P = O$ in $E(\mathbb{Z}_p)$. Ciò significa che l'ordine di $P$ nel gruppo $E(\mathbb{Z}_p)$ divide $k$ ed è quindi $B$-smooth. Verosimilmente anche l'ordine del gruppo $\#E(\mathbb{Z}_p)$ è $B$-smooth. †

• *Dato un primo $p$, qual è la probabilità che il gruppo $E(\mathbb{Z}_p)$ dei punti di una curva ellittica $E$ a caso su $\mathbb{Z}_p$ abbia ordine $B$-smooth?*

Dobbiamo richiamare alcuni fatti dalla teoria delle curve ellittiche:

† Osserviamo che se $n$ è un intero grande, determinare un punto $P$ su una data curva ellittica $E(\mathbb{Z}_n)$ è un problema non banale: richiede di determinare una radice quadrata modulo $n$ e ciò "in pratica" equivale a fattorizzare $n$ (vedi: $http://www.math.clemson.edu/faculty/Gao/crypto\_mod/node3.html$).

† Se l'ordine del gruppo $\#E(\mathbb{Z}_p)$ fosse il prodotto di primi $p_i \le B$ e di un numero grosso $Q$, il punto $P$ avrebbe ordine piccolo in $E(\mathbb{Z}_p)$, il che è poco probabile.

Il Teorema di Hasse stabilisce che fissato $p$, per una qualunque curva ellittica $E$ su $\mathbb{Z}_p$ l'ordine del gruppo $E(\mathbb{Z}_p)$ appartiene all'intervallo

$$(p+1-2\sqrt{p}, p+1-2\sqrt{p}).$$

Il Teorema di Deuring stabilisce che per ogni $m$ in tale intervallo esistono curve ellittiche $E(\mathbb{Z}_p)$ di ordine $m$ ed il loro numero al variare di $m$ è grossomodo lo stesso. Il Teorema di Lenstra dice che il numero $N(E)$ di curve ellittiche su $\mathbb{Z}_p$ con la proprietà che $\#E(\mathbb{Z}_p)$ è $B$-smooth può essere stimato come

$$N(E) \sim \#S \cdot p^{3/2},$$

dove $\#S$ è il numero di interi $B$-smooth compresi nell'intervallo $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$. Tenendo conto che ci sono circa $p^2$ curve ellittiche su $\mathbb{Z}_p$, la probabilità di trovare una curva ellittica su $\mathbb{Z}_p$ con ordine $B$-smooth può essere stimata come

$$\frac{N(E)}{p^2} \sim \frac{\#S}{p^2} p^{3/2} = \frac{\#S}{\sqrt{p}}. \tag{1}$$

In altre parole, la probabilità di trovare una curva ellittica su $\mathbb{Z}_p$ con la proprietà che $\#E(\mathbb{Z}_p)$ è $B$-smooth è paragonabile a quella di trovare un numero $B$-smooth nell'intervallo $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$: se in tale intervallo ci sono "abbastanza" numeri $B$-smooth, allora ci sono anche "abbastanza" curve ellittiche su $\mathbb{Z}_p$ che hanno ordine $B$-smooth. Stimiamo adesso il numero di interi $B$-smooth nell'intervallo $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$

$$\#S = \psi(p+1+2\sqrt{p}, B) - \psi(p+1-2\sqrt{p}, B),$$

mediante la funzione di Dickman $\psi(x, B)$ (vedi Crandall-Pomerance, Sez.1.4.5). Ponendo $B = (p+1+2\sqrt{p})^{1/u}$ e $B = (p+1-2\sqrt{p})^{1/v}$, per opportuni $u$, $v$, per il teorema di Dickman abbiamo

$$\#S \sim (p+1+2\sqrt{p})u^{-u} - (p+1-2\sqrt{p})v^{-v}.$$

Poiché l'ordine di grandezza di $p+1\pm 2\sqrt{p}$ è all'incirca $p$, possiamo sostituire $u$ e $v$ con $w$, determinato da $B = p^{1/w}$, cosí che

$$\#S \sim 4\sqrt{p}w^{-w}, \qquad w \sim \frac{\ln p}{\ln B}.$$

La stima (1) diventa adesso

$$\frac{N(E)}{p^2} \sim \frac{4\sqrt{p}w^{-w}}{p^2} p^{3/2} \sim \frac{1}{w^w}.$$

CONCLUSIONE: *fissato un primo p, la probabilità che il gruppo dei punti di una curva ellittica a caso E su $\mathbb{Z}_p$ abbia ordine B-smooth è almeno*

$$\frac{1}{w^w}, \qquad \text{con} \quad w \sim \frac{\ln p}{\ln B}. \tag{2}$$

Osserviamo che la relazione (2) indica che *con maggiore probabilità troviamo prima i fattori più piccoli di n*. Questo dipende dal fatto che fissato $B$, i numeri $B$-smooth si diradano a mano a mano che crescono, e lo stesso vale anche per le curve ellittiche con ordine $B$-smooth.

• *Qual è la complessità di un ciclo di questo algoritmo?*

- Assegnare una curva ellittica $E$ su $\mathbb{Z}_n$, con un punto $P \in E(\mathbb{Z}_n)$:
  dare a caso $X_0, Y_0, A$ e calcolare $B = Y_0^2 - X_0^3 - AX_0 \mod n$ $\qquad \mathcal{O}(\ln^2 n)$
- calcolare $k \cdot P$ mediante $\ln k$ "duplicazioni succesive", modulo $n$:
  scrivere $k = a_{m-1}2^{m-1} + \ldots + a_1 2 + a_0$ in forma binaria, e calcolare
  $P$
  $+2P$ $\qquad \mathcal{O}(\ln^3 n)$ (la complessità di questo calcolo è dominata dal $\gcd(2Y_0, n)$)
  $+2(2P)$ $\qquad \mathcal{O}(\ln^3 n)$

$\vdots$
$+2 \ldots (2P)$ $\quad \mathcal{O}(\ln^3 n)$
Totale: $\mathcal{O}(\ln k \ln^3 n)$

CONCLUSIONE: la complessità di un ciclo di questo algoritmo si stima come

$$\mathcal{O}(\ln^2 n) + \mathcal{O}(\ln k \ln^3 n) \quad \sim \quad \mathcal{O}(\ln k \ln^3 n) = \mathcal{O}(B \ln^3 n),$$

ossia è lineare in $B$ (ricordiamo che $B \sim \ln k$ (dal Teorema dei Numeri Primi)).

• *Sia $p$ un primo. Determiniamo ora qual è il bound $B$ ottimale per determinare un fattore di $n$ dell'ordine di grandezza di $p$.*

Per la discussione precedente, $w^w$ tentativi "probabilmente" produrranno una curva $E$ su $\mathbb{Z}_p$ con gruppo $E(\mathbb{Z}_p)$ di ordine $B$-smooth, e la complessità dei calcoli su ogni singola curva è dell'ordine di $B \ln^3 n$.
In totale, esprimendo $B$ come $B = p^{1/w}$, la complessità del calcolo che "probabilmente" produrrà un fattore $p$ risulta dunque

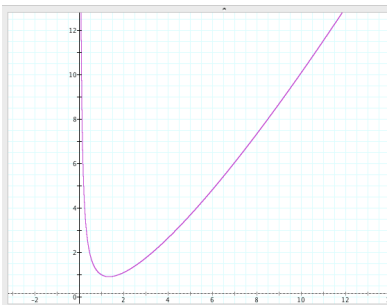
$$w^w \cdot B \ln^3 n \quad \sim \quad w^w p^{1/w} \ln^3 n \qquad \text{dove } w = \frac{\ln p}{\ln B}.$$

Stimiamo qual è il bound $B$ che minimizza il lavoro per determinare $p$, cercando il minimo della funzione

$$w \;\mapsto\; w^w p^{1/w} \ln^3 n, \qquad w = \frac{\ln p}{\ln B} \tag{3}$$

o meglio del suo logaritmo:

$$w \;\mapsto\; \ln(w^w p^{1/w} \ln^3 n) = w \ln w + \frac{1}{w} \ln p + 3 \ln(\ln n) \quad \sim \quad w \ln w + \frac{1}{w} \ln p.$$



Il grafico approssimativo della funzione $w \ln w + \frac{1}{w} \ln p$.

La funzione $w \;\mapsto\; w \ln w + \frac{1}{w} \ln p$ tende all'infinito per $w \to 0^+$ e per $w \to \infty$.
La sua derivata si annulla in $w$ se e solo se $w$ soddisfa l'equazione

$$1 + \ln w - \frac{1}{w^2} \ln p = 0 \quad \Leftrightarrow \quad w^2 \ln(we) = \ln p \quad \Leftrightarrow \quad (ew)^2 \ln(ew)^2 = 2e^2 \ln p.$$

Poniamo $x = (ew)^2$ e approssimiamo $x \sim \frac{y}{\ln y}$ con $y = x \ln x = 2e^2 \ln p$. Otteniamo

$$(ew)^2 = \frac{2e^2 \ln p}{\ln(2e^2 \ln p)} \;\sim\; \frac{2e^2 \ln p}{\ln(\ln p)}.$$

Ne segue che il lavoro per ottenere un fattore dell'ordine di grandezza di $p$ è minimizzato da

$$w_0 = \sqrt{\frac{2\ln p}{\ln(\ln p)}}.$$

Di conseguenza, per ottenere un fattore dell'ordine di grandezza di $p$ con $w^w$ curve, la scelta ottimale di $B$ si può stimare con

$$B_{best} = e^{\frac{\ln p}{w_0}} = e^{\sqrt{\frac{\ln p \ln\ln p}{2}}}.$$

OSSERVAZIONE: Sia $p$ un primo fissato. Il lavoro per determinare $p$ tende all'infinito per $w \to 0^+$, ossia per $B \to \infty$ (gestire un bound grosso richiede calcoli pesanti) oppure per $w \to +\infty$, ossia per $B \to 0^+$ (in questo caso il bound è piccolo rispetto a $p$ ed è necessario tentare con molte curve).

La siguiente tabla muestra los valores óptimos de B1 según la cantidad de dígitos del factor y la cantidad esperada de curvas usando ese límite. Estos valores son promedios.

| Dígitos | Valor de B1 | Curvas esperadas |
|---|---|---|
| 15 | 2000 | 25 |
| 20 | 11000 | 90 |
| 25 | 50000 | 300 |
| 30 | 250000 | 700 |
| 35 | 1 000000 | 1800 |
| 40 | 3 000000 | 5100 |
| 45 | 11 000000 | 10600 |
| 50 | 43 000000 | 19300 |
| 55 | 110 000000 | 49000 |
| 60 | 260 000000 | 124000 |
| 65 | 850 000000 | 210000 |
| 70 | 2900 000000 | 340000 |

Este programa usa 25 curvas con límite B1 = 2000, 300 curvas con límite B1 = 50000, 1675 curvas con límite B1 = 1000000 y finalmente usa curvas con límite B1 = 11000000 hasta encontrar todos los factores.

Una tabella dal sito Alpertron.

CONCLUSIONE: *Scegliendo il bound ottimale*

$$B_{best} = e^{\sqrt{\frac{\ln p \ln\ln p}{2}}},$$

*la complessità del calcolo che "probabilmente" produrrà un fattore dell'ordine di grandezza di $p$ si può stimare con*

$$w_0^{w_0} p^{1/w_0} = w_0^{w_0} B_{best} = e^{\sqrt{2\ln p \ln\ln p}}.$$

*Tenuto conto che verosimilmente troveremo prima i fattori più piccoli di $n$, la complessità probabilistica di questo algoritmo è subesponenziale nel numero di cifre del fattore più piccolo di $n$.*

Caso peggiore: $p = \sqrt{n}$ e $w^w p^{1/w} = e^{\sqrt{\ln n \ln\ln n}} \sim e^{\sqrt{\ln n}}$.

**Esempio.** Supponiamo di voler fattorizzare $n = 77$.
Consideriamo la curva ellittica $E: \quad Y^2 = X^3 - X + 3$ su $\mathbb{Z}_n$, con $\Delta = -4 + 27 \cdot 9 \equiv 8 \in \mathbb{Z}_{77}^*$,
ed il punto $P = (2, 3) \in E$.
Fissiamo $B = 3$ e prendiamo $k = B! = 6$.
Calcoliamo $6P$ in $E(\mathbb{Z}_{77})$.

$2P$:
indichiamo con $m$ il coefficiente angolare della "retta tangente" alla curva in $P$;

$$m = (3 \cdot 4 - 1)6^{-1} = -11, \qquad 2P = (40, 47);$$

(abbiamo potuto fare il calcolo perchè $\gcd(6, 77) = 1$)
$4P$:
indichiamo con $m$ il coefficiente angolare della "retta tangente" alla curva in $2P$;

$$m = (3 \cdot 40^2 - 1)94^{-1} = 6, \qquad 4P = (33, 5);$$

(abbiamo potuto fare il calcolo perchè $\gcd(94, 77) = 1$)
$6P = 2P + 4P$: indichiamo con $m$ il coefficiente angolare della "retta secante" per $2P$ e $4P$;

$$m = -42(-7)^{-1}, \qquad \gcd(-7, 77) = 7 \neq 1 \quad !!!!!!??????$$

Poiché $\gcd(-7, 77) = 7 \neq 1$, non possiamo calcolare $(-7)^{-1}$ in $\mathbb{Z}_{77}$, dunque neanche $m$. In compenso abbiamo trovato un fattore di $n = 77$!!!

Cosa è successo ??
È successo che $77 = 7 \cdot 11$. Il gruppo $E(\mathbb{Z}_7)$ ha 6 elementi, il punto $P$ ha ordine 6 nel gruppo $E(\mathbb{Z}_7)$ e dunque $6P = \infty$ in $E(\mathbb{Z}_7)$ (il gruppo $E(\mathbb{Z}_{11})$ invece ha 13 elementi).

**La seconda fase.**

Siano $n$, $B$, $k$ come sopra.
Siano $(E, P)$ una curva ellittica su $\mathbb{Z}_n$ ed un punto su di essa.
Se dal calcolo

$$k \cdot P = Q$$

su $E(\mathbb{Z}_n)$ si è ottenuto un punto "al finito" (nel corso del calcolo di $k \cdot P$ nessuna inversione modulo $n$ ha prodotto fattori non banali di $n$), questo ciclo dell'algoritmo ha fallito.
Questo succede se per nessun fattore primo $p$ di $n$ la curva $E(\mathbb{Z}_p)$ ha ordine $B$-smooth.

Nella seconda fase dell'algoritmo si dovrebbero individuare fattori primi $p$ di $n$ per cui l'ordine della stessa curva $E$ su $\mathbb{Z}_p$ sia della forma

$$\#E(\mathbb{Z}_p) = q \cdot m,$$

dove $m$ è un numero $B$-smooth e $q$ è numero primo in un intervallo $[B_1, B_2]$, con $B_1 = B$. Si parte dal punto "al finito" $Q$ prodotto dalla prima fase su $E$ e si calcolano in $E(\mathbb{Z}_n)$ tutti i multipli

$$q_1 \cdot Q, \quad q_2 \cdot Q, \quad \dots \quad q_i \cdot Q, \quad \dots$$

al variare dei primi $q_i$ nell'intervallo $[B_1, B_2]$. Infatti, se per un certo $i$ il calcolo di

$$q_i \cdot Q = q_i k \cdot P$$

provoca un problema di inversione modulo $n$ e individua un fattore non banale di $n$, vuol dire che per qualche fattore primo $p$ di $n$

$$q_i \cdot Q = q_i k \cdot P = O \qquad \text{su} \quad E(\mathbb{Z}_p);$$

verosimilmente

$$\#E(\mathbb{Z}_p) \quad \text{divide} \quad q_i k$$

e dunque $\#E(\mathbb{Z}_p) = q_i \cdot m$ è il prodotto di un primo $q_i \in [B_1, B_2]$ per un numero $B$-smooth $m$.

**L'algoritmo**.

Un modo economico per completare questa seconda fase è il seguente:

PRECALCOLO a monte del programma:

- fissare un secondo bound $B_2$;
- enumerare tutti i primi $q_1, q_2, \dots, q_\alpha$ nell'intervallo $[B_1, B_2]$, con $B = B_1$;
- precalcolare tutti gli incrementi $\delta_i = q_{i+1} - q_i$, per $i = 1, \dots, \alpha$;
- sia $M = \max_i \delta_i$ l'ampiezza massima degli incrementi $\delta_i$.

Osserviamo che al variare di $i = 1, \dots, \alpha$, gli incrementi $\delta_i$ sono relativamente "piccoli" e molti di essi coincidono: dal Teorema dei Numeri Primi, si stima infatti che nell'intervallo $[B_1, B_2]$, di ampiezza $B_2 - B_1$ ci sono all'incirca $\pi(B_2) - \pi(B_1) \sim \frac{B_2}{\ln B_2} - \frac{B_1}{\ln B_1}$ numeri primi...

PRECALCOLO a monte della seconda fase di ogni ciclo:

Sia $Q$ il punto al finito prodotto dalla prima fase (fallita) dell'algoritmo su una curva $E$;

- precalcolare i tutti i possibili multipli $m \cdot Q$, al variare di $m = 2, \dots, M$ pari ;
  in questo modo ci siamo calcolati di fatto tutti i punti

$$R_i := \delta_i Q, \quad \text{su } E(\mathbb{Z}_n).$$

- calcolare in successione

$$Q_1 = q_1 \cdot Q,$$
$$Q_2 = Q_1 + R_1 = Q_1 + \delta_1 Q = q_1 Q + (q_2 - q_1)Q = q_2 Q$$
$$\dots\dots$$
$$Q_i = Q_{i-1} + R_{i-1} = q_{i-1} Q + \delta_{i-1} Q = q_{i-1} Q + (q_i - q_{i-1}) \cdot Q = q_i Q$$
$$\dots\dots$$

Se alla fine dei calcoli troviamo ancora un punto al finito, anche la fase 2 di questo ciclo ha fallito. Iniziamo un nuovo ciclo cambiando curva.