Il crivello quadratico è un algoritmo per la fattorizzazione di interi $n \in \mathbb{Z}$, di complessità probabilistica subesponenziale in $\log n$. È basato sul seguente fatto:

Sia n un numero composto dispari. Supponiamo che esistano interi $a, b \in \mathbb{Z}$ per cui vale

$$a^2 \equiv b^2 \bmod n. \tag{1}$$

Allora $gcd(n, a+b)$ e $gcd(n, a-b)$ sono possibili fattori non banali di n.

Dim. Abbiamo che

$$a^2 \equiv b^2 \bmod n \Leftrightarrow a^2 - b^2 = (a+b)(a-b) \equiv 0 \bmod n \Leftrightarrow n \mid (a+b)(a-b).$$

Se p è un divisore primo di n, allora p divide $(a+b)$ e $\gcd(n, a+b) > 1$, oppure p divide $(a-b)$ e $\gcd(n, a-b) > 1$. (Per avere fattori non banali bisogna che $a \not\equiv \pm b \bmod n$).

Esempio 1. Sia $n = 5959$. Dalla relazione $80^2 \equiv 441 \equiv 21^2 \bmod 5959$, con $a = 80$, $b = 21$, $a + b = 101$ e $a - b = 59$, si ottengono i due fattori non banali di $n = 59 \cdot 101$ mediante

$$\gcd(59, 5959) = 59 \qquad \gcd(101, 5959) = 101.$$

Esempio 2. Sia $n = 1649$. Consideriamo le relazioni

$$41^2 \equiv 32, \quad 42^2 \equiv 115, \quad 43^2 \equiv 200 \qquad \bmod 1649.$$

Nessuno fra 32, 115 e 200 è un quadrato modulo n. Ma moltiplicando fra loro la prima e la terza relazione otteniamo

$$41^2 \cdot 43^2 \equiv (41 \cdot 43)^2 \equiv 114^2 \equiv 32 \cdot 200 \equiv 6400 \equiv 80^2 \qquad \bmod 1649.$$

Per $a = 114$,
$b = 80$,
$a + b = 194$ e
$a - b = 34$, troviamo i fattori non banali di $n = 17 \cdot 97$ mediante

$$\gcd(34, 1649) = 17, \qquad \gcd(194, 1649) = 97.$$

Esempio 3. Sia $n = 91$. Consideriamo le relazioni

$$21^2 \equiv 7 \cdot 11, \quad 29^2 \equiv 2 \cdot 11, \quad 14^2 \equiv 2 \cdot 7 \qquad \bmod 91.$$

Nessuno fra $7 \cdot 11$, $2 \cdot 11$ e $2 \cdot 7$ è un quadrato modulo 91: ognuno di essi infatti si decompone in fattori primi con esponenti dispari. Ma se moltiplichiamo queste tre relazioni fra loro, troviamo

$$21^2 \cdot 29^2 \cdot 14^2 \equiv (21 \cdot 29 \cdot 14)^2 \equiv 2^2 \cdot 7^2 \cdot 11^2 \equiv (2 \cdot 7 \cdot 11)^2 \qquad \bmod 91.$$

Per $a = 21 \cdot 29 \cdot 14 \equiv 63 \mod 91$,
$b = 2 \cdot 7 \cdot 11 \equiv 63 \mod 91$,
$a + b = 126 \equiv 35 \mod 91$, e
$a - b = 0$, troviamo un fattore non banale di 91 calcolando

$$\gcd(35, 91) = 7, \quad \gcd(0, 91) = 91.$$

Il crivello quadratico consiste nel produrre in modo sistematico relazioni del tipo (1), generalizzando la situazione dell'Esempio 3.

Si fissano $B \in \mathbb{Z}_{>0}$ "smoothness bound";
$F = \{l_1, \dots l_\alpha \text{ primi}, l_i \leq B,\ n \text{ è un quadrato modulo } l_i\}$ "factor base".

Vedremo in seguito come mai la factor base F contiene solo i primi $l \leq B$, per cui n è un quadrato modulo l.

• Sia $x \in \mathbb{Z}$ un intero e sia $s \equiv x^2 \mod n$ (con $0 \leq s < n$) la classe resto del suo quadrato modulo n. Se s è B-smooth (*qui di seguito, con un abuso di linguaggio, chiamiamo B-smooth gli interi che si decompongono nei primi della factor base*), si decompone come $s = l_1^{e_1} l_2^{e_2} \dots l_\alpha^{e_\alpha}$, e produce la relazione

$$x^2 \equiv s \equiv l_1^{e_1} l_2^{e_2} \dots l_\alpha^{e_\alpha} \mod n.$$

Supponiamo di aver creato A relazioni, con $A \geq \alpha$

$$\begin{aligned} x_1^2 \equiv & s_1 \equiv l_1^{e_{11}} l_2^{e_{12}} \dots l_\alpha^{e_{1\alpha}} \\ x_2^2 \equiv & s_2 \equiv l_1^{e_{21}} l_2^{e_{22}} \dots l_\alpha^{e_{2\alpha}} \\ & \vdots \quad \vdots \quad \vdots \quad \vdots \\ x_A^2 \equiv & s_A \equiv l_1^{e_{A1}} l_2^{e_{A2}} \dots l_\alpha^{e_{A\alpha}}. \end{aligned} \tag{2}$$

I prodotti $s_j = l_1^{e_{j1}} l_2^{e_{j2}} \dots l_\alpha^{e_{j\alpha}}$ generalmente non sono quadrati (gli esponenti e_{ji} dei primi della factor base non sono necessariamente tutti pari!). Ma possiamo ottenere un quadrato moltiplicando fra loro un certo numero di queste relazioni (fino a rendere pari tutti gli esponenti dei primi della factor base). Per decidere quali, scriviamo

$$\prod_{j=1}^{A} x_j^{2\epsilon_j} \equiv \prod_{j=1}^{A} s_j^{\epsilon_j} = \prod_{j=1}^{A} (l_1^{e_{j1}} l_2^{e_{j2}} \dots l_\alpha^{e_{j\alpha}})^{\epsilon_j} = \prod_{i=1}^{\alpha} l_i^{e_{1i}\epsilon_1 + e_{2i}\epsilon_2 + \dots + e_{Ai}\epsilon_A}, \qquad \epsilon_j \in \{0, 1\}. \tag{3}$$

Nella formula qui sopra l'indice $i = 1, \dots, \alpha$ parametrizza i primi della factor base, $j = 1, \dots, A$ parametrizza le relazioni, il cofficiente ϵ_j indica quali relazioni vengono effettivamente usate nel prodotto: infatti se $\epsilon_j = 0$, si ha $x_j^{2\epsilon_j} = 1$, cioè la relazione j-sima non viene contata.
Vogliamo determinare i coefficienti $\epsilon_1, \dots, \epsilon_A$ in modo che il prodotto a destra nella (3) sia un quadrato: questo avviene se e solo se tutti gli esponenti $e_{1i}\epsilon_1 + e_{2i}\epsilon_2 + \dots + e_{Ai}\epsilon_A$, con $i = 1, \dots, \alpha$, sono pari, ossia se e solo se $\epsilon_1, \dots, \epsilon_A$ soddisfano il sistema lineare omogeneo (generalmente molto sparso)

$$\begin{cases} e_{11}X_1 + e_{21}X_2 + \dots + e_{A1}X_A \equiv 0 \\ e_{12}X_1 + e_{22}X_2 + \dots + e_{A2}X_A \equiv 0 \\ \vdots \quad \vdots \quad \vdots \\ e_{1\alpha}X_1 + e_{2\alpha}X_2 + \dots + e_{A\alpha}X_A \equiv 0 \end{cases} \mod 2.$$

Osserviamo che per $A > \alpha$ lo spazio delle soluzioni del sistema ha dimensione positiva su $\mathbb{Z}_2$ (ci sono più incognite che equazioni). Per ogni elemento $(E_1, \dots, E_A)$ di una base di tale spazio otteniamo una congruenza della forma $a^2 \equiv b^2 \mod n$, con

$$a = \prod_j x_j^{2\epsilon_j}, \quad b = \prod_{i=1}^{\alpha} l_i^{(e_{1i}E_1 + e_{2i}E_2 + \dots + e_{Ai}E_A)/2},$$

e possiamo cercare fattori non banali di n calcolando $\gcd(a + b, n)$ e $\gcd(a - b, n)$.

Descriviamo ora l'idea chiave del crivello quadratico per produrre le relazioni (2) in modo efficiente. Come dice la parola *crivello* (setaccio) consiste nel setacciare un array di interi modulo n per individuare quelli fra essi che sono B-smooth *senza doverli fattorizzare*. Gli interi dell'array sono creati da noi in modo da massimizzare la probabilità che siano B-smooth.

Il crivello.

Sia n il numero da fattorizzare.
Sia $B \in \mathbb{Z}_{>0}$ uno *smoothness bound* fissato e sia $F = \{l_1, l_2, \ldots, l_\alpha\}$ la *factor base* associata, composta dai numeri primi minori o uguali a B con la proprietà che n è un quadrato modulo l_i.
Sia M un intero positivo fissato.

L'array da setacciare è costituito da $2M$ interi della forma

$$a(j) := (X_0 + j)^2 - n, \qquad \text{dove } X_0 = [\sqrt{n}] \text{ ed il parametro } j \text{ varia in } [-M, M]. \tag{4}$$

Poiché n è molto più grande di M, per $j > 0$, si ha $0 < a(j) << n$. Per $j < 0$, si ha $-n << a(j) << n$.

Osserviamo che sulla retta reale, gli interi dell'array

$$\ldots \quad \ldots \quad (X_0 - 2)^2 - n, \quad (X_0 - 1)^2 - n, \quad X_0^2 - n, \quad (X_0 + 1)^2 - n, \quad (X_0 + 2)^2 - n, \quad \ldots \quad \ldots \tag{5}$$

non sono consecutivi, ma sono sparsi all'interno dell'intervallo $[(X_0 - M)^2 - n, (X_0 + M)^2 - n]$.
La scelta di prendere $X_0 = [\sqrt{n}]$ è suggerita dall'esigenza di massimizzare la probabilità che $a(j) := (X_0 + j)^2 - n$ sia B-smooth (precisamente: *che si fattorizzi nei primi della factor base*). Infatti, se $X_0 = [\sqrt{n}]$, gli elementi dell'array sono centrati in $X_0^2 - n \sim \sqrt{n}$ e dunque più piccoli possibile in modulo.

Il crivello funziona così:

siano $l_1, \ldots, l_\alpha$ i primi della factor base.

- Se un elemento dell'array $a(j)$ è divisibile per l_1, viene diviso per l_1 e sostituito col quoziente $a(j)/l_1$, se è divisibile per l_1^2 viene sostituito col quoziente $a(j)/l_1^2$ (cioè $a(j)/l_1$ viene ulteriormente diviso per l_1), ..., se è divisibile per $l_1^{k_1}$ viene sostituito col quoziente $a(j)/l_1^{k_1}$ (cioè $a(j)/l_1^{k_1-1}$ viene ulteriormente diviso per l_1);
- Se un numero dell'array $a(j)$ è divisibile per l_2, viene sostituito col quoziente $a(j)/l_2$, se è divisibile per l_2^2 viene sostituito col quoziente $a(j)/l_2^2$, ..., se è divisibile per $l_2^{k_2}$ viene sostituito col quoziente $a(j)/l_2^{k_2}$;

e così via fino a che i primi della factor base e le loro potenze non sono esauriti.
Le posizioni dell'array che alla fine della procedura contengono 1 sono quelle che all'inizio contenevano numeri B-smooth.

L'idea chiave dell'algoritmo sta nel modo in cui si individuano gli elementi dell'array che sono divisibili per un certo l_j^k, una volta che se ne è localizzato uno. Essa si basa sui seguenti fatti:

(1) Un primo $p > 2$ divide $a(j) = (X_0 + j)^2 - n$ se e solo se $(X_0 + j)^2 \equiv n \mod p$, ossia se e solo se n è un quadrato modulo p e al tempo stesso $\overline{X_0 + j}$ è una radice quadrata di $\bar{n}$ in $\mathbb{Z}_p^*$.

Per definizione n è un quadrato modulo p se esiste un intero r tale che $r^2 \equiv n \mod p$. Se n è un quadrato modulo p ed $n \not\equiv 0 \mod p$, allora esistono due famiglie infinite di interi che soddisfano la congruenza $x^2 \equiv n \mod p$:

$$r + kp, \quad k \in \mathbb{Z}, \qquad s + hp, \quad h \in \mathbb{Z},$$

dove $\bar{r}$ ed $\bar{s} = \overline{-r}$ sono le due radici quadrate di $\bar{n}$ in $\mathbb{Z}_p^*$, ossia le due classi $\mathbb{Z}_p^*$ che soddisfano l'equazione $\bar{x}^2 = \bar{n}$. Le classi $\bar{r}$ ed $\bar{s} = \overline{-r}$ in $\mathbb{Z}_p^*$ possono essere determinate in modo efficiente con l'algoritmo di Shanks-Tonelli (vedi Nota sulle radici modulo p e p^k). (Nel nostro caso è evidente che $n \not\equiv 0 \mod p$, altrimenti avremmo un fattore di n).

(2) Siano j_1 e j_2 interi per cui $a(j_1) = (X_0 + j_1)^2 - n$ ed $a(j_2) = (X_0 + j_2)^2 - n$ sono divisibili per p, con $X_0 + j_1 \equiv r \mod p$ e $X_0 + j_1 \equiv s \equiv -r \mod p$. Allora tutti e soli gli elementi dell'array che sono divisibili per p sono dati da

$$a(j_1 + kp),\ k \in \mathbb{Z}, \quad \text{e} \quad a(j_2 + hp),\ h \in \mathbb{Z}.$$

In altre parole, tutti gli elementi nell'array divisibili per p si ottengono facendo fare a j salti di ampiezza p a partire da j_1 e da j_2

$$\dots a(j_1 - 3p),\ a(j_1 - 2p),\ a(j_1 - p),\ a(j_1),\ a(j_1 + p),\ a(j_1 + 2p),\ a(j_1 + 3p), \dots$$

$$\dots a(j_2 - 3p),\ a(j_2 - 2p),\ a(j_2 - p),\ a(j_2),\ a(j_2 + p),\ a(j_2 + 2p),\ a(j_2 + 3p), \dots$$

(3) Sia p un primo e sia $m > 0$. La potenza p^m divide $a(j) = (X_0+j)^2-n$ se e solo se $(X_0+j)^2 \equiv n \mod p^m$, ossia se e solo se n è un quadrato modulo p^m e al tempo stesso $\overline{X_0 + j}$ è una radice quadrata di $\bar{n}$ in $\mathbb{Z}^*_{p^m}$.

Per definizione n è un quadrato modulo p^m se esiste un intero r tale che $r^2 \equiv n \mod p^m$. Se n è un quadrato modulo p^m ed $n \not\equiv 0 \mod p^m$, allora esistono due famiglie infinite di interi che soddisfano la congruenza $x^2 \equiv n \mod p^m$:

$$r + kp^m,\ k \in \mathbb{Z}, \qquad s + hp^m,\ h \in \mathbb{Z},$$

dove $\bar{r}$ ed $\bar{s} = \overline{-r}$ sono le due soluzioni dell'equazione $\bar{x}^2 = \bar{n}$ in $\mathbb{Z}^*_{p^m}$. Le classi $\bar{r}$ ed $\bar{s} = \overline{-r}$ in $\mathbb{Z}^*_{p^m}$ possono essere determinate in modo efficiente con l'algoritmo di Shanks-Tonelli e il Lemma di Hensel (vedi Nota sulle radici modulo p e p^k). (Nel nostro caso è evidente che $n \not\equiv 0 \mod p^m$, altrimenti avremmo un fattore di n).

(4) Siano j_1 e j_2 interi per cui $a(j_1) = (X_0 + j_1)^2 - n$ ed $a(j_2) = (X_0 + j_2)^2 - n$ sono divisibili per p^m, con $X_0 + j_1 \equiv r \mod p^m$ e $X_0 + j_1 \equiv s \equiv -r \mod p^m$. Allora tutti e soli gli elementi dell'array che sono divisibili per p^m sono dati da

$$a(j_1 + kp^m),\ k \in \mathbb{Z}, \quad \text{e} \quad a(j_1 + hp^m),\ h \in \mathbb{Z}.$$

In altre parole, tutti gli elementi nell'array divisibili per p^m si ottengono facendo fare a j salti di ampiezza p^m a partire da j_1 e da j_2

$$\dots a(j_1 - 3p^m),\ a(j_1 - 2p^m),\ a(j_1 - p^m),\ a(j_1),\ a(j_1 + p^m),\ a(j_1 + 2p^m),\ a(j_1 + 3p^m), \dots$$

$$\dots a(j_2 - 3p^m),\ a(j_2 - 2p^m),\ a(j_2 - p^m),\ a(j_2),\ a(j_2 + p^m),\ a(j_2 + 2p^m),\ a(j_2 + 3p^m), \dots$$

(5) Sia p un primo della factor base. Se $2M < p^m$, l'array conterrà al più un elemento divisibile per p^m. Quindi non ha senso setacciare l'array per potenze di p superiori ad m.

(6) Conviene trattare a parte il primo $p = 2$ in base alle seguenti osservazioni:

(i) Un intero n dispari è un quadrato modulo 2 ed è il quadrato di un numero dispari. In particolare, un intero della forma $(X_0 + j)^2 - n$ è divisibile per 2 se e solo se $(X_0 + j)$ è dispari, ossia

$$\begin{cases} j = 1 + 2k,\ k \in \mathbb{Z}, \text{ se } X_0 \equiv 0 \mod 2 \text{ è pari} \\ j = 2h,\ h \in \mathbb{Z}, \text{ se } X_0 \equiv 1 \mod 2 \text{ è dispari.} \end{cases}$$

(ii) Sia n un intero dispari:

$$\begin{cases} \text{se } n \equiv 3, 7 \mod 8, \text{ allora } (X_0 + j)^2 - n \text{ è divisibile al più per 2;} \\ \text{se } n \equiv 5 \mod 8, \text{ allora } (X_0 + j)^2 - n \text{ è divisibile al più per 2 e per } 2^2 = 4; \\ \text{se } n \equiv 1 \mod 8, \text{ allora } (X_0 + j)^2 - n \text{ è divisibile per } 2^3 = 8 \text{ e possibilmente per } 2^k, \text{ con } k \geq 4; \end{cases}$$

(Vedi Nota su radici modulo p e p^k su come applicare il Lemma di Hensel nel caso $p = 2$ ed estrarre le radici quadrate modulo 2^m).

Dim. di (ii): Dal punto (i) abbiamo che $x = (X_0 + j)$ è dispari. Dunque si può scrivere come $x = 2m + 1$, con $m \in \mathbb{Z}$.
- Se $n \equiv 3, 7 \mod 8$, calcolando $x^2 - n$ troviamo rispettivamente $4m^2 + 4m + 1 - 3 - 8M = 4m(m+1) - 2 - 8M$ e $4m^2 + 4m + 1 - 7 - 8M = 4m(m+1) - 6 - 8M$, con $M \in \mathbb{Z}$. Entrambe le espressioni sono divisibili al più per 2.
- Se $n \equiv 5 \mod 8$, calcolando $x^2 - n$ troviamo $4m^2 + 4m + 1 - 5 - 8M = 4m(m+1) - 4 - 8M$, con $M \in \mathbb{Z}$. Questa espressione è divisibile al più per 4.
- $n \equiv 1 \mod 8$, calcolando $x^2 - n$ troviamo $4m^2 + 4m + 1 - 1 - 8M = 4m(m+1) - 8M$, con $M \in \mathbb{Z}$. Questa espressione è evidentemente divisibile per 8 e possibilmente per 2^k, con $k \geq 4$.

Complessità probabilistica del crivello quadratico.

Sia n l'intero da fattorizzare;
sia B un *ordine di smoothness* fissato;
sia F la *factor base* associata, di cardinalità $\#F = \alpha \sim \frac{1}{2}\frac{B}{\ln B} \sim \frac{1}{2}B$;
sia $X_0 = [\sqrt{n}\,] \sim \sqrt{n}$;
sia $M \in \mathbb{Z}_{>0}$ intero che determina la cardinalità dell'array di sieving.

(1) La prima fase del crivello quadratico (*fase di sieving*) consiste nell'individuare i numeri B-smooth nell'array di sieving formato dagli interi $a(j) = (X_0 + j)^2 - n$, con $j \in [-M, M]$. Osserviamo che si tratta di $2M$ numeri sparsi all'interno dell'intervallo della retta reale

$$[(X_0 - M)^2 - n,\, (X_0 + M)^2 - n] \;\sim\; [-2\sqrt{n}M,\, 2\sqrt{n}M]. \tag{6}$$

Cominciamo con lo stimare l'ordine di grandezza di M affinché l'array contenga un numero sufficiente di interi B-smooth, o equivalentemente affinché l'intervallo (6) contenga un numero sufficiente di interi B-smooth della forma $a(j) = (X_0 + j)^2 - n$.

Per semplicità assumiamo che gli $a(j)$ siano distribuiti uniformemente all'interno dell'intervallo. Osserviamo che la maggioranza di essi ha un valore assoluto dell'ordine di $2M\sqrt{n}$. Scrivendo $M = n^\epsilon$ per un $\epsilon > 0$, la probabilità di pescare un intero B-smooth all'interno dell'intervallo $[(X_0 - M)^2 - n,\, (X_0 + M)^2 - n]$, può essere stimata come

$$w^{-w}, \qquad \text{con} \quad w = \frac{\ln(2M\sqrt{n})}{\ln B} \sim \frac{\ln(n^{\frac{1}{2}+\epsilon})}{\ln B} = (\frac{1}{2} + \epsilon)\frac{\ln n}{\ln B}.$$

Ne segue che al variare di $j \in [-M, M]$ gli interi B-smooth fra gli $a(j)$ dovrebbero essere circa

$$2Mw^{-w}, \qquad w = (\frac{1}{2} + \epsilon)\frac{\ln n}{\ln B}.$$

Avendo bisogno di almeno $\alpha \sim B/2$ numeri B-smooth, dovremo prendere

$$M \sim w^w \frac{B}{4} \sim w^w B, \qquad w \sim (\frac{1}{2} + \epsilon)\frac{\ln n}{\ln B}. \tag{7}$$

Complessità della fase di sieving.

Per ogni primo p della factor base, dobbiamo calcolare:

le radici quadrate di n modulo p;
$\frac{2M}{p}$ divisioni per p;
le radici quadrate di n modulo p^2;
$\frac{2M}{p^2}$ divisioni per p^2;

$\vdots \qquad\qquad \vdots$

le radici quadrate di n modulo p^k;
$\frac{2M}{p^k}$ divisioni per p^k.

Nella stima della complessità della fase di sieving trascuriamo il calcolo delle radici quadrate di n modulo $p,\ p^2, \ldots, p^k, \ldots$, che risulta comunque dominato dal resto: ad esempio, calcolare $\sqrt{n} \mod p$ è polinomiale in $\log p$, una volta trovato un non-quadrato in $\mathbb{Z}_p^*$ (che di fatto si trova).

Il numero di divisioni è stimabile da sopra con

$$2M \sum_{a=1}^{\infty} \frac{1}{p^a} \;=\; 2M \frac{1}{p-1}$$

Sommando rispetto ai primi della factor base, otteniamo un numero di divisioni dell'ordine di

$$2M \sum_{p \le B} \frac{1}{p} \;\sim\; 2M \ln(\ln B),$$

dove abbiamo stimato $\sum_{p \le B} \frac{1}{p} \sim \ln(\ln B)$.
Vedi Nota $\sum_{p<X} \frac{1}{p} = \log\log X + O(1)$.

Poiché la complessità di ognuna delle divisioni richieste si può maggiorare con $\log n \log B$, la *complessità della fase di sieving* si può stimare come

$$\mathcal{O}(2M \ln(\ln B) \cdot \ln n \ln B) =$$

$$= \mathcal{O}(n^{(\frac{1}{2}+\epsilon)\frac{1}{w}} w^w \ln B \cdot \ln(\ln B) \cdot \ln n) \sim$$

$$\sim \mathcal{O}(n^{(\frac{1}{2}+\epsilon)\frac{1}{w}} w^w \cdot \ln n), \qquad w = (\frac{1}{2}+\epsilon)\frac{\ln n}{\ln B},$$

dove abbiamo posto $M \sim B w^w$, con $B = n^{(\frac{1}{2}+\epsilon)\frac{1}{w}}$.

(2) La seconda fase del crivello quadratico consiste nel risolvere un sistema lineare $\alpha \times \alpha$, a coefficienti in $\mathbb{Z}_2$, con $\alpha \sim B/2$. La *complessità della risoluzione del sistema* mediante l'eliminazione di Gauss si stima con $\mathcal{O}(B^3)$. D'altra parte, dato che si tratta di un sistema molto sparso, non è irrealistico usare la stima

$$\mathcal{O}(B^2).$$

TOTALE:

$$\mathcal{O}(n^{(\frac{1}{2}+\epsilon)\frac{1}{w}} w^w \cdot \ln n \;+\; B^2), \qquad w = (\frac{1}{2}+\epsilon)\frac{\ln n}{\ln B}.$$

Parametri ottimali. Cerchiamo ora di determinare i parametri ottimali per la fase di sieving. Si tratta di minimizzare la funzione

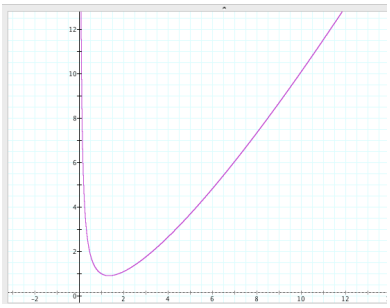
$$F(w) = n^{(\frac{1}{2}+\epsilon)\frac{1}{w}} \cdot w^w \cdot \ln n,$$

al variare di $w = (\frac{1}{2}+\epsilon)\frac{\ln n}{\ln B}$ in $\mathbb{R}^+$.
Poichè il logaritmo è una funzione monotona, possiamo passare al logaritmo e minimizzare la funzione $G\colon \mathbb{R}^+ \to \mathbb{R}$

$$G(w) = \ln F(w) = (\frac{1}{2}+\epsilon)\frac{1}{w}\ln n + w \ln w + \ln n \;\sim\; (\frac{1}{2}+\epsilon)\ln n \frac{1}{w} + w \ln w,$$

$$= \frac{a}{w} + w \ln w, \qquad \text{con} \quad a = (\frac{1}{2}+\epsilon)\ln n, \quad w = (\frac{1}{2}+\epsilon)\frac{\ln n}{\ln B}$$

(vedi anche la Nota "Smooth numbers estimates" per uno studio dettagliato di F).



Il grafico approssimativo della funzione $G(w) = \frac{a}{w} + w \ln w$.

Osserviamo che $\lim_{w\to 0^+} G(w) = \lim_{w\to+\infty} G(w) = +\infty$.
- il primo caso corrisponde ad aver scelto B troppo grosso: avere una factor base molto grossa appesantisce sia la fase di sieving che la risoluzione sistema;
- il secondo caso corrisponde ad aver scelto B troppo piccolo rispetto ad n e dunque a dover ingrandire a dismisura l'array di sieving per trovarvi un numero adeguato di interi B-smooth).

Calcolando la derivata di G, troviamo che ha un unico punto di minimo in $w_0 \sim \sqrt{\frac{\ln n}{\ln(\ln n)}}$:

Si ha $G'(w) = -\frac{a}{w^2} + \ln w + 1$, da cui $G'(w) = 0 \;\Leftrightarrow\; a = w^2(\ln w + 1) = w^2 \ln we \;\Leftrightarrow\; 2e^2 a = (ew)^2 \ln(we)^2$.
Poniamo $x := (ew)^2$. L'equazione precedente diventa $2e^2 a = x \ln x$.
Poniamo $y := x \ln x$ e approssimiamo $x \sim \frac{y}{\ln y}$.
Otteniamo

$$(ew)^2 = e^2 w^2 \sim \frac{2e^2 a}{\ln(2e^2 a)} \sim \frac{2e^2(\frac{1}{2}+\epsilon)\ln n}{\ln(2e^2(\frac{1}{2}+\epsilon)\ln n)}.$$

Semplificando ricaviamo

$$w^2 \sim \frac{\ln n}{\ln e^2 + \ln(\ln n)} \sim \frac{\ln n}{\ln(\ln n)} \quad \Leftrightarrow \quad w_0 = \sqrt{\frac{\ln n}{\ln(\ln n)}}.$$

A w_0 corrispondono uno smoothness bound ottimale

$$B_{best} = n^{(\frac{1}{2}+\epsilon)\frac{1}{w_0}} \sim e^{(\frac{1}{2}+\epsilon)\sqrt{\ln n \cdot \ln(\ln n)}}$$

un'ampiezza ottimale

$$M_{best} \sim e^{(1+\epsilon)\sqrt{\ln n \cdot \ln(\ln n)}}$$

e una complessità ottimizzata

$$W_{best} \sim e^{(1+\epsilon)\sqrt{\ln n \cdot \ln(\ln n)}} \ln n \sim e^{(1+\epsilon)\sqrt{\ln n \cdot \ln(\ln n)}}.$$

• Facciamo vedere che nell'espressione della complessità ottimizzata, $\epsilon \to 0$ al tendere di $n \to \infty$.

Sia $w = \sqrt{\frac{\ln n}{\ln(\ln n)}}$ il punto di minimo ddella (parte significativa) della complessità del crivello.

Abbiamo $M = n^\epsilon = Bw^w$, con ϵ reale positivo e $w = (\frac{1}{2}+\epsilon)\frac{\ln n}{\ln B}$. Ricavando $B = n^{(\frac{1}{2}+\epsilon)\frac{1}{w}}$ da w e sostituendolo nell'espressione di M troviamo

$$n^\epsilon = n^{(\frac{1}{2}+\epsilon)\frac{1}{w}} w^w.$$

Passando ai logaritmi

$$\epsilon \ln n = (\frac{1}{2}+\epsilon)\frac{1}{w}\ln n + w \ln w \quad \Leftrightarrow \quad w\epsilon \ln n = (\frac{1}{2}+\epsilon)\ln n + w^2 \ln w$$

e sostituendo $w = \sqrt{\frac{\ln n}{\ln(\ln n)}}$, troviamo

$$\epsilon\sqrt{\frac{\ln n}{\ln(\ln n)}}\ln n = (1+\epsilon)\ln n.$$

Ne segue che per $n \to \infty$

$$\epsilon = \frac{1}{\sqrt{\frac{\ln n}{\ln(\ln n)}} - 1} \longrightarrow 0.$$

CONCLUSIONE: *asintoticamente* per $n \to \infty$, la complessità totale del crivello quadratico è data da

$$\mathcal{O}(e^{\sqrt{\ln n \cdot \ln(\ln n)}} \ln n \ + \ e^{\sqrt{\ln n \cdot \ln(\ln n)}} \ln n) = \mathcal{O}(e^{\sqrt{\ln n \cdot \ln(\ln n)}}),$$

dove il primo termine rappresenta la complessità ottimizzata della fase di sieving ed il secondo la risoluzione del sistema. Al "finito" la complessità totale del crivello quadratico è dominata dalla fase di sieving, ma al crescere di n il peso della risoluzione del sistema rispetto alla fase di sieving aumenta.

SIMPQS.

n intero da fattorizzare,
B=smoothness bound,
$F = \{l_i \leq B, \text{ primi, per cui } n \text{ è quadrato mod } l_i\}$=factor base.

Usiamo polinomi della forma

$$f(x) = ax^2 + 2bx + c, \qquad \text{con } b^2 - ac = n. \tag{$*$}$$

Precisamente:

• - $a = q_1 \cdot \ldots \cdot q_k \sim \sqrt{2n}/M$ *è prodotto di un certo numero di primi (fissati) della factor base (in particolare a è B-smooth);*

- b, con $|b| < a/2$, varia nell'insieme delle radici quadrate di n modulo $a = q_1 \cdot \ldots \cdot q_k$, della forma $\{\pm B_1 \pm \ldots \pm B_k\}$, dove ogni B_i è una soluzione particolare del sistema di congruenze

$$X^2 \equiv n \bmod q_i, \ldots\ldots, X^2 \equiv 0 \bmod q_j, \quad j \neq i, \quad i = 1, \ldots k.$$

Scegliere b di questa forma rende piu' facile il cambio di polinomio (usare "Gray code", vedi Crandall-Pomerance).
Le condizioni sull'ordine di grandezza di a e b servono a stimare l'ordine di grandezza degli elementi dell'array.

- $c = (b^2 - n)/a$: dalla condizione $b \in \sqrt{n} \bmod a$, abbiamo che $b^2 \equiv n \bmod a$ ossia $b^2 - n = ka$, per $k \in \mathbb{Z}$. Ne segue che $(b^2 - n)/a$ è un intero.

• Gli elementi dell'array sono i valori di f in j:

$$A(j) := f(j) = aj^2 + 2bj + c.$$

• *Per ogni polinomio della forma (*), il setacciamento dell'array si fa con gli stessi primi $p \in F$. In altre parole, se un primo p divide $A(j)$, allora $p \in F$.*

Dim. : Per come sono stati scelti i coefficienti del polinomio f, l'elemento $A(j)$ può essere riscritto come $A(j) = a^{-1}((aj + b)^2 - n)$. Quindi

$$p \mid A(j) \quad \Leftrightarrow \quad p \mid a^{-1}((aj + b)^2 - n) \quad \Leftrightarrow \quad ap \mid ((aj + b)^2 - n).$$

Ne segue in particolare che

$$p \mid ((aj + b)^2 - n) \quad \Leftrightarrow \quad (aj + b)^2 \equiv n \bmod p,$$

cioè $p \in F$.

• *Gli elementi $A(j)$ che sono divisibili per un primo $p \in F$ si trovano cosi':*

$$p \mid A(j) = aj^2 + 2bj + c \quad \Leftrightarrow \quad aj^2 + 2bj + c \equiv 0 \bmod p$$

$$\Leftrightarrow \quad j \equiv -ba^{-1} \pm ra^{-1} \bmod p$$

dove $\pm r$ sono le radici quadrate di n modulo p (abbiamo sfruttato il fatto che $b^2 - ac = n$). Dunque ci sono due famiglie di elementi $A(j)$ divisibili per p, in corrispondenza di

$$j = (-ba^{-1} + ra^{-1}) + Kp, \quad K \in \mathbb{Z}$$

e di

$$j = (-ba^{-1} - ra^{-1}) + Hp, \quad H \in \mathbb{Z}.$$

Analogamente, si ricavano i valori di j a cui corrispondono elementi $A(j)$ divisibili per p^k:

$$p^k \mid A(j) = aj^2 + 2bj + c \quad \Leftrightarrow \quad j \equiv -ba^{-1} \pm sa^{-1} \bmod p^k,$$

dove $\pm s$ sono le radici quadrate di n modulo p^k. Le due famiglie di elementi $A(j)$ divisibili per p^k si trovano in corrispondenza di

$$j = (-ba^{-1} + sa^{-1}) + Kp^k, \quad K \in \mathbb{Z}$$

e di

$$j = (-ba^{-1} - sa^{-1}) + Hp^k, \quad H \in \mathbb{Z}.$$

Attenzione: le formule qui sopra hanno senso solo se p NON divide a. Quindi solo se stiamo setacciando per primi che non compaiono in $a = q_1 \cdot \ldots \cdot q_k$.

Se un primo $p > 2$ divide a e $\gcd(a, p^k) = p$, per ogni $k \geq 1$, allora $p \nmid b$ (altrimenti sarebbe un fattore di n) e vale

$$A(j) = aj^2 + 2bj + c \equiv 2bj + c \equiv 0 \bmod p \quad \Leftrightarrow \quad j \equiv -c(2b)_p^{-1} \bmod p,$$

dove $(2b)_p^{-1}$ indica un inverso modulo p.

Per trovare i valori di j per cui $A(j)$ è divisibile per p^k, applichiamo un certo numero di volte il Lemma di Hensel al polinomio $f(X) = aX^2 + 2bX + c$, con $f'(X) = 2aX + 2b$.

Ad esempio, se a $j_1 \equiv -c(2b)_p^{-1} \bmod p$ corrispondono gli elementi $A(j)$ divisibili per p, allora gli $A(j)$ divisibili per p^2 corrispondono a

$$j \equiv j_1 + f(j_1)f'(j_1)_p^{-1} \equiv -c(2b)_p^{-1} - 2ac^2b(2b)_p^{-2} + 2bcs_0p \bmod p^2,$$

dove $s_0 \in \mathbb{Z}$ è un intero che soddisfa $(2b)(2b)_p^{-1} \equiv 1 + s_0p \bmod p^2$.

• *Supponiamo che un certo $A(j_0)$ risulti B-smooth, cioè $A(j_0) = l_1^{e_1} \cdot \ldots \cdot l_\alpha^{e_\alpha}$. La relazione che si ottiene è data da*

$$(aj_0 + b)^2 \equiv l_1^{e_1} \cdot \ldots \cdot l_\alpha^{e_\alpha} \cdot a = l_1^{e_1} \cdot \ldots \cdot l_\alpha^{e_\alpha} \cdot q_1 \cdot \ldots \cdot q_k.$$

Nota: anche i primi q_i appartengono alla factor base F.