Version: 18. 12. 2019,1150

Esempio di CRIVELLO QUADRATICO

Sia $n = 1100017$ l'intero da fattorizzare ($n \equiv 1 \bmod 8$).
Fissiamo $B = 20$ smoothness bound.
La factor base è data da

$$F = \{2, 3, 7, 13, 17\} \cup \{-1\},$$

in quanto n non è un quadrato modulo i primi 5, 11, 19.
Basta verificare che $n^{(5-1)/2} \equiv 4 \not\equiv 1 \bmod 5$, $n^{(11-1)/2} \equiv 10 \not\equiv 1 \bmod 11$ e $n^{(19-1)/2} \equiv 18 \not\equiv 1 \bmod 19$.
Vedremo in seguito che è utile inserire anche -1 nella factor base.

Fissiamo $X_0 = [\sqrt{n}] = 1048$, $M = 25$
e consideriamo gli interi della forma

$$a(j) = (X_0 + j)^2 - n, \quad \text{al variare di } j \in [-M, M],$$

e li mettiamo in un array. L'array contiene 50 interi non consecutivi, sparsi nell'intervallo della retta reale $[-53488, 51312]$. La maggior parte di essi hanno 5 cifre decimali, ossia sono dell'ordine di grandezza di $2M\sqrt{n}$. Gli elementi più piccoli in modulo si trovano al centro dell'array. Successivamente setacceremo questo array in cerca degli elementi che si fattorizzano nei primi della factor base (B-smooth con un abuso di linguaggio).

$a(-25) = 1023^2 - n = -53488 = -2^4 * 3343.$
$a(-24) = 1024^2 - n = -51441 = -3 * 13 * 1319.$
$a(-23) = 1025^2 - n = -49392 = -2^4 * 3^2 * 7^3.$
$a(-22) = 1026^2 - n = -47341 = -7 * 6763.$
$a(-21) = 1027^2 - n = -45288 = -2^3 * 3^2 * 17 * 37.$
$a(-20) = 1028^2 - n = -43233 = -3 * 14411.$
$a(-19) = 1029^2 - n = -41176 = -2^3 * 5147.$
$a(-18) = 1030^2 - n = -39117 = -3 * 13 * 17 * 59.$
$a(-17) = 1031^2 - n = -37056 = -2^6 * 3 * 193.$
$a(-16) = 1032^2 - n = -34993 = -7 * 4999.$
$a(-15) = 1033^2 - n = -32928 = -2^5 * 3 * 7^3.$
$a(-14) = 1034^2 - n = -30861 = -3^5 * 127.$
$a(-13) = 1035^2 - n = -28792 = -2^3 * 59 * 61.$
$a(-12) = 1036^2 - n = -26721 = -3^2 * 2969.$
$a(-11) = 1037^2 - n = -24648 = -2^3 * 3 * 13 * 79.$
$a(-10) = 1038^2 - n = -22573 = -22573.$
$a(-9) = 1039^2 - n = -20496 = -2^4 * 3 * 7 * 61.$
$a(-8) = 1040^2 - n = -18417 = -3 * 7 * 877.$
$a(-7) = 1041^2 - n = -16336 = -2^4 * 1021.$
$a(-6) = 1042^2 - n = -14253 = -3 * 4751.$
$a(-5) = 1043^2 - n = -12168 = -2^3 * 3^2 * 13^2.$
$a(-4) = 1044^2 - n = -10081 = -17 * 593.$
$a(-3) = 1045^2 - n = -7992 = -2^3 * 3^3 * 37.$
$a(-2) = 1046^2 - n = -5901 = -3 * 7 * 281.$
$a(-1) = 1047^2 - n = -3808 = -2^5 * 7 * 17.$
$a(0) = 1048^2 - n = -1713 = -3 * 571.$
$a(1) = 1049^2 - n = 384 = 2^7 * 3.$
$a(2) = 1050^2 - n = 2483 = 13 * 191.$
$a(3) = 1051^2 - n = 4584 = 2^3 * 3 * 191.$
$a(4) = 1052^2 - n = 6687 = 3^2 * 743.$
$a(5) = 1053^2 - n = 8792 = 2^3 * 7 * 157.$
$a(6) = 1054^2 - n = 10899 = 3^2 * 7 * 173.$

$a(7) = 1055^2 - n = 13008 = 2^4 * 3 * 271.$
$a(8) = 1056^2 - n = 15119 = 13 * 1163.$
$a(9) = 1057^2 - n = 17232 = 2^4 * 3 * 359.$
$a(10) = 1058^2 - n = 19347 = 3 * 6449.$
$a(11) = 1059^2 - n = 21464 = 2^3 * 2683.$
$a(12) = 1060^2 - n = 23583 = 3 * 7 * 1123.$
$a(13) = 1061^2 - n = 25704 = 2^3 * 3^3 * 7 * 17.$
$a(14) = 1062^2 - n = 27827 = 27827.$
$a(15) = 1063^2 - n = 29952 = 2^8 * 3^2 * 13.$
$a(16) = 1064^2 - n = 32079 = 3 * 17^2 * 37.$
$a(17) = 1065^2 - n = 34208 = 2^5 * 1069.$
$a(18) = 1066^2 - n = 36339 = 3 * 12113.$
$a(19) = 1067^2 - n = 38472 = 2^3 * 3 * 7 * 229.$
$a(20) = 1068^2 - n = 40607 = 7 * 5801.$
$a(21) = 1069^2 - n = 42744 = 2^3 * 3 * 13 * 137.$
$a(22) = 1070^2 - n = 44883 = 3^2 * 4987.$
$a(23) = 1071^2 - n = 47024 = 2^4 * 2939.$
$a(24) = 1072^2 - n = 49167 = 3^4 * 607.$
$a(25) = 1073^2 - n = 51312 = 2^4 * 3 * 1069.$

Il crivello. Setacciamo l'array in cerca degli elementi $a(j)$ che si decompongono nei primi della factor base, *senza fattorizzarli*. Osserviamo che se un primo p divide $a(j) = (X_0 + j)^2 - n$, allora $(X_0 + j)^2 \equiv n \bmod p$. Dunque n deve essere un quadrato modulo p. Inoltre, se $k \in \mathbb{Z}_{ge1}$, si ha che n è un quadrato modulo p^k se e solo se è un quadrato modulo p Le radici quadrate di n modulo p si trovano con l'algoritmo di Shaks-Tonelli. A partire da queste si trovano quelle modulo p^2, $p^3, \ldots, p^k$ con il Lemma di Hensel.

• $l_1 = 2$
Cerchiamo gli elementi dell'array divisibili per 2. Abbiamo

$$a(j) = (X_0 + j)^2 - n \equiv 0 \bmod 2 \quad \Leftrightarrow \quad (X_0 + j)^2 \equiv n \bmod 2,$$

ossia $X_0 + j$ è una radice quadrata di n modulo 2. Nel nostro caso specifico $n \equiv 1 \bmod 2$ e le radici quadrate di 1 modulo 2 sono $r_1 = r_2 = 1$. Inoltre $X_0 \equiv 0 \bmod 2$. Ne segue che

$$j = r_1 - X_0 = 1 + 2k,\ k \in \mathbb{Z},$$

e gli elementi dell'array divisibili per 2 corrispondono ai valori dispari di j

$$\ldots\ldots a(-5),\ a(-3),\ a(-1),\ a(1),\ a(3),\ a(5), \ldots\ldots$$

• $l_1^2 = 2^2 = 4$
Abbiamo

$$a(j) = (X_0 + j)^2 - n \equiv 0 \bmod 4 \quad \Leftrightarrow \quad (X_0 + j)^2 \equiv n \bmod 4,$$

ossia $X_0 + j$ è una radice quadrata di n modulo 4. Poiche' $n \equiv 1 \bmod 4$, le radici quadrate di 1 modulo 4 sono $r_1 = 1$ ed $r_2 = 3$ e $X_0 \equiv 0 \bmod 2$, troviamo che gli elementi dell'array divisibili per 4 corrispondono alle due famiglie

$$j = r_1 - X_0 = 1 + 4k,\ k \in \mathbb{Z}, \quad \text{e} \quad j = r_2 - X_0 = 3 + 4h,\ h \in \mathbb{Z},$$

e sono

$$\ldots a(-10),\ a(-7),\ a(-3),\ a(1),\ a(5),\ a(9),\ a(13), \ldots$$

$$\ldots a(-9),\ a(-5),\ a(-1),\ a(3),\ a(7),\ a(11),\ a(15), \ldots$$

In generale sono un sottoinsieme degli elementi divisibili per 2; in questo caso particolare coincidono con gli elementi divisibili per 2: dipende dal fatto che $n \equiv 1 \bmod 8$ (vedi esercizio ???).

Proseguiamo con le altre potenze di 2: vista l'ampiezza dell'intervallo non andremo oltre $l_1^8 = 256$. Di elementi divisibili per 256 ce ne potrebbe essere al più uno...

• $l_2 = 3$
Cerchiamo gli elementi dell'array divisibili per 3. Abbiamo

$$a(j) = (X_0 + j)^2 - n \equiv 0 \bmod 3 \quad \Leftrightarrow \quad (X_0 + j)^2 \equiv n \bmod 3,$$

ossia $X_0 + j$ è una radice quadrata di n modulo 3.

Poiche' $n \equiv 1 \bmod 3$, le radici quadrate di 1 modulo 3 sono $r_1 = 1$ ed $r_2 = 2$. Inoltre $X_0 \equiv 1 \bmod 3$, per cui che gli elementi dell'array divisibili per 3 corrispondono alle due famiglie

$$j = r_1 - X_0 = 3k,\ k \in \mathbb{Z}, \quad \text{e} \quad j = r_2 - X_0 = 1 + 3h,\ h \in \mathbb{Z},$$

e sono

$$\dots a(-9),\ a(-6),\ a(-3),\ a(0),\ a(3),\ a(6),\ a(9), \dots$$
$$\dots a(-8),\ a(-5),\ a(-2),\ a(1),\ a(4),\ a(7),\ a(10), \dots$$

$$\dots \quad \dots \quad \dots$$
$$\dots \quad \dots \quad \dots$$

Un altro esempio...

• $l_3 = 7$
Abbiamo $n \equiv 2 \bmod 7$ e $X_0 \equiv 5 \bmod 7$, da cui

$$(X_0 + j)^2 \equiv n \bmod 7 \quad \Leftrightarrow \quad (5 + j)^2 \equiv 2 \bmod 7.$$

Poiche' le radici quadrate di 2 modulo 7 sono $r_1 = 3$ e $r_2 = 4$, abbiamo due famiglie di elementi $a(j)$ divisibili per 7, parametrizzate rispettivamente da

$$j = r_1 - X_0 = 5 + 7k,\ k \in \mathbb{Z}, \quad \text{e} \quad j = r_2 - X_0 = 4 + 7h,\ h \in \mathbb{Z}:$$

$$a(-23),\ a(-16),\ a(-9),\ a(-2),\ a(5),\ a(12),\ a(19),$$
$$a(-24),\ a(-17),\ a(-8),\ a(-1),\ a(6),\ a(13),\ a(20).$$

• $l_3^2 = 7^2 = 49$
Abbiamo $n \equiv 16 \bmod 49$ e $X_0 \equiv 19 \bmod 49$, da cui

$$(X_0 + j)^2 \equiv n \bmod 49 \quad \Leftrightarrow \quad (19 + j)^2 \equiv 16 \bmod 49.$$

Poiche' le radici quadrate di 2 modulo 49 sono $r_1 = 4$ e $r_2 = 45$, abbiamo due famiglie di elementi $a(j)$ divisibili per 49, parametrizzate rispettivamente da

$$j = r_1 - X_0 = 34 + 49k,\ k \in \mathbb{Z}, \quad \text{e} \quad j = r_2 - X_0 = 26 + 49h,\ h \in \mathbb{Z}:$$

$$a(-15),$$
$$a(-23).$$

$\dots \quad \dots \quad \dots$

$\dots \quad \dots \quad \dots$

Alla fine troviamo questi numeri fattorizzabili nei primi della factor base $F = \{2, 3, 7, 13, 17\} \cup \{-1\}$:

$a(-1) = 1047^2 - n = -3808 = -2^5 * 7 * 17.$
$a(-5) = 1043^2 - n = -12168 = -2^3 * 3^2 * 13^2.$
$a(-15) = 1033^2 - n = -32928 = -2^5 * 3 * 7^3.$
$a(-23) = 1025^2 - n = -49392 = -2^4 * 3^2 * 7^3.$
$a(1) = 1049^2 - n = 384 = 2^7 * 3.$
$a(13) = 1061^2 - n = 25704 = 2^3 * 3^3 * 7 * 17.$
$a(15) = 1063^2 - n = 29952 = 2^8 * 3^2 * 13.$

a cui corrispondono le relazioni

$1047^2 \equiv -2^5 * 7 * 17 \bmod n$
$1043^2 \equiv -2^3 * 3^2 * 13^2 \bmod n$
$1033^2 \equiv -2^5 * 3 * 7^3 \bmod n$
$1025^2 \equiv -2^4 * 3^2 * 7^3 \bmod n$
$1049^2 \equiv 2^7 * 3 \bmod n$
$1061^2 \equiv 2^3 * 3^3 * 7 * 17 \bmod n$
$1063^2 \equiv 2^8 * 3^2 * 13 \bmod n.$

Adesso cerchiamo $\epsilon_1, \dots, \epsilon_7$ in $\{0, 1\}$ in modo che il prodotto delle relazioni

$$(1047^2)^{\epsilon_1} \cdot (1043^2)^{\epsilon_2} \cdot \cdot (1063^2)^{\epsilon_7}$$

$$= (-2^5 \cdot 7 \cdot 17)^{\epsilon_1} \cdot (-2^3 \cdot 3^2 \cdot 13^2)^{\epsilon_2} \cdot . \cdot (2^8 \cdot 3^2 \cdot 13)^{\epsilon_7}$$

$$= (-1)^{(\epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4)} \cdot 2^{(5\epsilon_1+3\epsilon_2+5\epsilon_3+4\epsilon_4+7\epsilon_6+3\epsilon_6+8\epsilon_7)} \cdot 3^{2\epsilon_2+\epsilon_3+2\epsilon_4+3\epsilon_5+3\epsilon_6+2\epsilon_7} \cdot$$
$$\cdot 7^{\epsilon_1+3\epsilon_3+3\epsilon_4+\epsilon_6} \cdot 13^{2\epsilon_2+\epsilon_7} \cdot 17^{\epsilon_1+\epsilon_6}$$

sia un quadrato, ossia tutti gli esponenti a destra dell'ultima uguaglianza siano pari. Si ottiene un sistema lineare omogeneo a coefficienti in $\mathbb{Z}_2$, di 6 equazioni nelle incognite $\epsilon_1, \dots, \epsilon_7$

$$\begin{cases} \epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 \equiv 0 \\ 5\epsilon_1 + 3\epsilon_2 + 5\epsilon_3 + 4\epsilon_4 + 7\epsilon_5 + 3\epsilon_6 + 8\epsilon_7 \equiv 0 \\ 2\epsilon_2 + \epsilon_3 + 2\epsilon_4 + \epsilon_5 + 3\epsilon_6 + 2\epsilon_7 \equiv 0 \\ \epsilon_1 + 3\epsilon_3 + 3\epsilon_4 + +\epsilon_6 \equiv 0 \\ 2\epsilon_2 + \epsilon_7 \equiv 0 \\ \epsilon_1 + \epsilon_6 \equiv 0, \end{cases}$$

con matrice dei coefficienti modulo 2

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Tale sistema ha uno spazio delle soluzioni di dimensione ≥ 1, precisamente

$$\mathrm{span}_{\mathbb{Z}_2}\{\begin{pmatrix}0\\0\\1\\1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\\1\\0\\1\\0\end{pmatrix}\}.$$

Dalla prima soluzione otteniamo che il prodotto fra la terza, la quarta e la quinta relazione produce la congruenza quadratica

$$(1033 * 1025 * 1049)^2 \equiv (2^8 * 3^2 * 7^3)^2 \bmod n;$$

dalla seconda otteniamo che il prodotto fra la prima, la seconda, la terza, la quarta e la sesta relazione produce la congruenza quadratica

$$(1047 * 1043 * 1033 * 1025 * 1061)^2 \equiv (2^{10} * 3^4 * 7^4 * 13 * 17)^2 \bmod n.$$

Nel primo caso,

$$a = 1033 * 1025 * 1049 \equiv 790272, \quad b = 2^8 * 3^2 * 7^3 \equiv 790272 \mod n,$$

$$\gcd(a - b, n) = 1100017, \quad \gcd(a + b, n) = 1.$$

Fallimento!!

Nel secondo caso,

$$a = 1047 * 1043 * 1033 * 1025 * 1061 \equiv 676456, \quad b = 2^{10} * 3^4 * 7^4 * 13 * 17 \equiv 148054 \bmod n,$$

$$\gcd(a - b, n) = 547, \quad \gcd(a + b, n) = 2011.$$

Successo!!
Infatti $1100017 = 547 * 2011$.