Esempio di CRIVELLO QUADRATICO.

 n = 87463 da fattorizzare.
 (n congruo a 1 modulo 8)

Fissiamo B = 40
{2, 3, 5, 7, 11, 13,17,19, 23, 29, 31, 37} = lista dei primi < 40
F={2, 3, 13, 17, 19, 29} = factor base
(poiche' n non e' un quadrato modulo 5, 7, 11, 23, 31, 37, questi primi non fanno parte della factor base).

Fissiamo   X_0= [sqrt{n}]= 295
Fissiamo   M=35
consideriamo i numeri interi della forma

a(j)=(X_0+j)^2-n, al variare di j in [-35,35],

e li mettiamo in un array.
Successivamente setacceremo questo array in cerca di numeri B-smooth, o meglio di numeri che si fattorizzano nei primi della factor base F.

L'array: e' formato da 70 interi non consecutivi, sparsi nell'intervallo della retta reale [-19863, 21437].
I numeri al centro dell'array sono quelli piu' piccoli in modulo;
ad ogni modo la maggior parte di essi hanno 5 cifre decimali, ossia sono dell'ordine di grandezza di 2MX_0.

a(-35)=(260)^2-n=-19863 [-1, 1; 3, 2; 2207, 1]
a(-34)=(261)^2-n=-19342 [-1, 1; 2, 1; 19, 1; 509, 1]
a(-33)=(262)^2-n=-18819 [-1, 1; 3, 3; 17, 1; 41, 1]
a(-32)=(263)^2-n=-18294 [-1, 1; 2, 1; 3, 1; 3049, 1]
a(-31)=(264)^2-n=-17767 [-1, 1; 109, 1; 163, 1]
a(-30)=(265)^2-n=-17238 [-1, 1; 2, 1; 3, 1; 13, 2; 17, 1]
a(-29)=(266)^2-n=-16707 [-1, 1; 3, 1; 5569, 1]
a(-28)=(267)^2-n=-16174 [-1, 1; 2, 1; 8087, 1]
a(-27)=(268)^2-n=-15639 [-1, 1; 3, 1; 13, 1; 401, 1]
a(-26)=(269)^2-n=-15102 [-1, 1; 2, 1; 3, 2; 839, 1]
a(-25)=(270)^2-n=-14563 [-1, 1; 14563, 1]
a(-24)=(271)^2-n=-14022 [-1, 1; 2, 1; 3, 2; 19, 1; 41, 1]
a(-23)=(272)^2-n=-13479 [-1, 1; 3, 1; 4493, 1]
a(-22)=(273)^2-n=-12934 [-1, 1; 2, 1; 29, 1; 223, 1]
a(-21)=(274)^2-n=-12387 [-1, 1; 3, 1; 4129, 1]
a(-20)=(275)^2-n=-11838 [-1, 1; 2, 1; 3, 1; 1973, 1]
a(-19)=(276)^2-n=-11287 [-1, 1; 11287, 1]
a(-18)=(277)^2-n=-10734 [-1, 1; 2, 1; 3, 1; 1789, 1]
a(-17)=(278)^2-n=-10179 [-1, 1; 3, 3; 13, 1; 29, 1]
a(-16)=(279)^2-n=-9622 [-1, 1; 2, 1; 17, 1; 283, 1]
a(-15)=(280)^2-n=-9063 [-1, 1; 3, 2; 19, 1; 53, 1]
a(-14)=(281)^2-n=-8502 [-1, 1; 2, 1; 3, 1; 13, 1; 109, 1]
a(-13)=(282)^2-n=-7939 [-1, 1; 17, 1; 467, 1]
a(-12)=(283)^2-n=-7374 [-1, 1; 2, 1; 3, 1; 1229, 1]
a(-11)=(284)^2-n=-6807 [-1, 1; 3, 1; 2269, 1]
a(-10)=(285)^2-n=-6238 [-1, 1; 2, 1; 3119, 1]
a(-9)=(286)^2-n=-5667 [-1, 1; 3, 1; 1889, 1]
a(-8)=(287)^2-n=-5094 [-1, 1; 2, 1; 3, 2; 283, 1]
a(-7)=(288)^2-n=-4519 [-1, 1; 4519, 1]
a(-6)=(289)^2-n=-3942 [-1, 1; 2, 1; 3, 3; 73, 1]
a(-5)=(290)^2-n=-3363 [-1, 1; 3, 1; 19, 1; 59, 1]
a(-4)=(291)^2-n=-2782 [-1, 1; 2, 1; 13, 1; 107, 1]
a(-3)=(292)^2-n=-2199 [-1, 1; 3, 1; 733, 1]
a(-2)=(293)^2-n=-1614 [-1, 1; 2, 1; 3, 1; 269, 1]
a(-1)=(294)^2-n=-1027 [-1, 1; 13, 1; 79, 1]
a(0)=(295)^2-n=-438 [-1, 1; 2, 1; 3, 1; 73, 1]
a(1)=(296)^2-n=153 [3, 2; 17, 1]
a(2)=(297)^2-n=746 [2, 1; 373, 1]
a(3)=(298)^2-n=1341 [3, 2; 149, 1]
a(4)=(299)^2-n=1938 [2, 1; 3, 1; 17, 1; 19, 1]
a(5)=(300)^2-n=2537 [43, 1; 59, 1]
a(6)=(301)^2-n=3138 [2, 1; 3, 1; 523, 1]
a(7)=(302)^2-n=3741 [3, 1; 29, 1; 43, 1]
a(8)=(303)^2-n=4346 [2, 1; 41, 1; 53, 1]
a(9)=(304)^2-n=4953 [3, 1; 13, 1; 127, 1]
a(10)=(305)^2-n=5562 [2, 1; 3, 3; 103, 1]
a(11)=(306)^2-n=6173 Mat([6173, 1])
a(12)=(307)^2-n=6786 [2, 1; 3, 2; 13, 1; 29, 1]
a(13)=(308)^2-n=7401 [3, 1; 2467, 1]
a(14)=(309)^2-n=8018 [2, 1; 19, 1; 211, 1]
a(15)=(310)^2-n=8637 [3, 1; 2879, 1]
a(16)=(311)^2-n=9258 [2, 1; 3, 1; 1543, 1]
a(17)=(312)^2-n=9881 [41, 1; 241, 1]
a(18)=(313)^2-n=10506 [2, 1; 3, 1; 17, 1; 103, 1]
a(19)=(314)^2-n=11133 [3, 2; 1237, 1]
a(20)=(315)^2-n=11762 [2, 1; 5881, 1]
a(21)=(316)^2-n=12393 [3, 6; 17, 1]
a(22)=(317)^2-n=13026 [2, 1; 3, 1; 13, 1; 167, 1]
a(23)=(318)^2-n=13661 [19, 1; 719, 1]

a(24)=(319)^2-n=14298 [2, 1; 3, 1; 2383, 1]
a(25)=(320)^2-n=14937 [3, 1; 13, 1; 383, 1]
a(26)=(321)^2-n=15578 [2, 1; 7789, 1]
a(27)=(322)^2-n=16221 [3, 1; 5407, 1]
a(28)=(323)^2-n=16866 [2, 1; 3, 2; 937, 1]
a(29)=(324)^2-n=17513 [83, 1; 211, 1]
a(30)=(325)^2-n=18162 [2, 1; 3, 2; 1009, 1]
a(31)=(326)^2-n=18813 [3, 1; 6271, 1]
a(32)=(327)^2-n=19466 [2, 1; 9733, 1]
a(33)=(328)^2-n=20121 [3, 1; 19, 1; 353, 1]
a(34)=(329)^2-n=20778 [2, 1; 3, 1; 3463, 1]
a(35)=(330)^2-n=21437 [13, 1; 17, 1; 97, 1]

IL CRIVELLO:

Per curiosità' localizziamo i numeri dell'arra che sono divisibili per 17:

p=17
quando e' che (X_0+j)^2-n e' divisibile per 17?

(X_0+j)^2=n mod 17 se e solo se X_0+j e' una radice quadrata di n, modulo 17.
n=87463 =15 modulo 17, e le radici quadrate di n=87463 in Z_17 sono 7 e 10.
quindi X_0+j e' una radice quadrata di n, modulo 17 se e solo se
X_0+j =7+ 17k, con k in Z oppure X_0+j =10+ 17h, con h in Z.
poiche' X_0= 295=6 mod 17, sono i numeri

a(j), per j= 1+ 17k, con k in Z oppure a(j), per j= 4+17h, con h in Z

a(-33), a(-16), a(1), a(18), a(35)
a(-30), a(-13), a(4), a(21)

Alla fine della fase di sieving troviamo questi numeri fattorizzabili nei primi della factor base F={2, 3, 7, 13,17 }:

a(-30) =265^2 - n = -17238 = -2 * 3 * 13^2 * 17.
a(-17) =278^2 - n = -10179 = -3^3 * 13 * 29.
a(1) =296^2 - n = 153 = 3^2 * 17.
a(4) = 299^2 - n = 1938 = 2 * 3 * 17 * 19.
a(12) =307^2 - n = 6786 = 2* 3^2 * 13 * 29.
a(21) =316^2 - n = 12393 = 3^6 * 17.

a cui corrispondono le relazioni

265^2 = -2 * 3 * 13^2 * 17 mod n
278^2 = -3^3 * 13 * 29 mod n
296^2 = 3^2 * 17 mod n
299^2 = 2 * 3 * 17 * 19 mod n
307^2 = 2* 3^2 * 13 * 29 mod n
316^2 = 3^6 * 17 mod n

OSSERVIAMO che, poiche' la cardinalita' della factor base e' 6+1=7 (includiamo anche -1 per tener conto del segno),
in linea di principio servono ALMENO 8 relazioni per essere sicuri di ottenere una relazione quadratica modulo n
(e poter tentare la fattorizzazione di n).
Vedremo qui di seguito che in questo caso particolare le 6 relazioni qui sopra sono sufficienti.

Cerchiamo esponenti epsilon_1,…., epsilon_6 in {0,1} in modo che il prodotto delle relazioni

(265^2)^epsilon_1 * (278^2) ^epsilon_2 * …… * (316^2)^epsilon_6=

(-2 * 3 * 13^2 *17)^epsilon_1 * (- 3^2 * 13 * 29)^epsilon_2* ….*(3^6 * 17)^epsilon_6=

(-1)^(epsilon_1+epsilon_2) *
  * 2^(epsilon_1+ epsilon_4+ epsilon_5) *
 ……. ……
 * 29^(epsilon_2+epsilon_5)=

=(-1)^E_1 * 2^E_2 * 3^E_3… * 29^E_6

si fattorizzi nei primi della factor base con tutti gli esponenti E_1,…., E_6 PARI.
Passando ai logaritmi, si ottiene un sistema lineare negli esponenti epsilon_1,…., epsilon_6.

epsilon_1+epsilon_2 =0 mod 2
epsilon_1+ epsilon_4+ epsilon_5 =0 mod 2
epsilon_1+3epsilon_2 +2epsilon_3 + epsilon_4+2epsilon_5 + 6epsilon_6 =0 mod 2
2epsilon_1+epsilon_2 +epsilon_5 =0 mod 2

epsilon_1+ +epsilon_3+ epsilon_4 +epsilon_6 =0 mod 2
+epsilon_4+ =0 mod 2
epsilon_2+ + epsilon_5 =0 mod 2

con matrice dei coefficienti :

1 1 0 0 0 0
1 0 0 1 1 0
1 3 2 1 2 6
2 1 0 0 1 0
1 0 1 1 0 1
0 0 0 1 0 0
0 1 0 0 1 0

modulo 2:

1 1 0 0 0 0
1 0 0 1 1 0
1 1 0 1 0 0
0 1 0 0 1 0
1 0 1 1 0 1
0 0 0 1 0 0
0 1 0 0 1 0

la matrice cosi' ottenuta e' la matrice dei coefficienti di un sistema lineare omogeneo 7x6….
e per nostra FORTUNA ha rango minore di 6, precisamente 5.
quindi un sistema il cui spazio delle soluzioni ha dimensione uno.

Risolvendo con l'eliminazione di Gauss su Z_2,
troviamo che una base per lo spazio delle soluzioni e' data dal vettore

1
1
1
0
1
0

Moltiplicando fra loro prima, seconda, terza e quinta,
troviamo la relazione quadratica

(265 * 278 * 296 * 307)^2 = 2^2 * 3^8 * 13^4 * 17^2 * 29^2 = (2 * 3^4 * 13^2 * 17 * 29)^2 mod n

x=265 * 278 * 296 * 307=34757 mod n
y=2 * 3^4 * 13^2 * 17 * 29= 28052 mod n

x+y=62809
x-y=6705

gcd(62809,n)=587
gcd(6705,n)=149

entrambi fattori non banali di n: SUCCESSO!!!