Esempio di CRIVELLO QUADRATICO.

n = 1100017 da fattorizzare.
(n congruo a 1 modulo 8)

Fissiamo B = 20
{2, 3, 5, 7, 11, 13,17,19} = lista dei primi < 20
F={2, 3, 7, 13,17 } = factor base

infatti n non e' un quadrato modulo 5,11,19 perche'
n^(5-1)/2 = 4 mod 5
n^(11-1)/2 = 10 mod 11
n^(19-1)/2 = 18 mod 19

Fissiamo X_0= [sqrt{n}]= 1048
Fissiamo M=25
consideriamo i numeri interi della forma

a(j)=(X_0+j)^2-n, al variare di j in [-25,25],

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 50 interi non consecutivi, sparsi nell'intervallo della retta reale [-53488, 51312].
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(-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:

l_1=2
quali elementi a(j) = (X_0+j)^2-n sono divisibili per l_1=2 ?

(X_0+j)^2-n=0 mod 2 se e solo se (X_0+j)^2=n modulo 2, ossia se e solo se X_0+j e' una radice quadrata di n, mod 2,
se e solo se X_0+j =1+ 2k, per k intero (oppure X_0+j =-1+ 2k, per k intero, che e' la stessa cosa).

poiche' X_0=0 mod 2, sono gli elementi dell'array a(j), con j=1+2m intero dispari:

……. ,a(-5) , a(-3) , a(-1) , a(1) , a(3) , a(5) ,….

setacciamo l'array e dividiamo tutti questi numeri per 2.

l_1^2=4
quali elementi a(j) = (X_0+j)^2-n sono divisibili per per l_1^2=4?

(X_0+j)^2-n=0 mod 4 se e solo se (X_0+j)^2=n mod 4, ossia se e solo se X_0+j e' una radice quadrata di n, modulo 4.
n =1 mod 4, e le radici quadrate di n in Z_4 sono 1 e 3.

quindi X_0+j e' una radice quadrata di n modulo 4 se e solo se X_0+j =1+ 4k, con k in Z oppure X_0+j =3+ 4h, con h in Z.
poiche' X_0=0 mod 4, sono i numeri
a(j), per j=1+4k, con k in Z oppure per j=3+4h, con h in Z.
(in generale sono un sottoinsieme dei precedenti, in questo caso particolare sono gli stessi di prima, perche' n=1 mod 8)

…., a(-10) , a(-7) , a(-3) , a(1) , a(5) , a(9) , a(13),…
….., a(-9), a(-5), a(-1), a(3), a(7), a(11), a(15), ...

Setacciamo l'array dividendo nuovamente questi numeri per 2.

l_1^3=8
quando e' che (X_0+j)^2-n e' divisibile per l_1^3=8?
etc....

arriviamo fino a l_1^8=256
vista l'ampiezza dell'array 2M=50, di numeri a(j) divisibili per l_1^8=256 ne troviamo al massimo 1.

l_2=3
quando e' che (X_0+j)^2-n e' divisibile per l_2=3?
(X_0+j)^2=n mod 3, ossia se e solo se X_0+j e' una radice quadrata di n, modulo 3.
n =1 modulo 3, quindi le radici quadrate di n in Z_3 sono 1 e 2.
quindi X_0+j e' una radice quadrata di n, modulo 3 se e solo se
X_0+j =1+ 3k, con k in Z oppure X_0+j =2+ 3h, con h in Z.
poiche' X_0=1 mod 3, sono i numeri

a(j), per j= 3k, con k in Z oppure a(j), per j=1+3h, con h in Z

….a(-6), a(-3), a(0), a(3), a(6), a(9),….
….a(-5), a(-2), a(1), a(4), a(7), a(10),….

l_2^2=9
etc…….

l_3=7
quando e' che (X_0+j)^2-n e' divisibile per l_3=7?

(X_0+j)^2=n mod 7 se e solo se X_0+j e' una radice quadrata di n, modulo 7.
n =2 modulo 7, e le radici quadrate di n in Z_7 sono 3 e 4.

quindi X_0+j e' una radice quadrata di n, modulo 7 se e solo se
X_0+j =3+ 7k, con k in Z oppure X_0+j =4+ 7h, con h in Z.
poiche' X_0=5 mod 7, sono i numeri

a(j), per j= 5+ 7k, con k in Z oppure a(j), per j= 6+7h, con h in Z

….a(-9), a(-2), a(5), a(12), a(19)
….a(-8), a(-1), a(6), a(13), a(20)

l_3^2=49
quando e' che (X_0+j)^2-n e' divisibile per l_3^2=49?
(X_0+j)^2=n mod 49, ossia se e solo se X_0+j e' una radice quadrata di n, modulo 49.
n =16 modulo 49, e le radici quadrate di n in Z_49 sono 4 e 45.
quindi X_0+j e' una radice quadrata di n, modulo 49 se e solo se
X_0+j =4+ 49k, con k in Z oppure X_0+j =45+ 49h, con h in Z.
poiche' X_0=19 mod 49, sono i numeri

a(j), per j= 34+49k, con k in Z oppure a(j), per j=26+49h, con h in Z

a(-15)
a(-23)

l_3^3=343
etc…. a(-23)

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

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 = -2^5 * 7 * 17 mod n
1043^2 = -2^3 * 3^2 * 13^2 mod n
1033^2 = -2^5 * 3 * 7^3 mod n
1025^2 = -2^4 * 3^2 * 7^3 mod n
1049^2 = 2^7 * 3 mod n
1061^2 = 2^3 * 3^3 * 7 * 17 mod n
1063^2 = 2^8 * 3^2 * 13 mod n

Adesso cerchiamo esponenti epsilon_1,…., epsilon_7 in {0,1} in modo che il prodotto delle relazioni

(1047^2)^epsilon_1 * (1043^2) ^epsilon_2 * …… * (1063^2)^epsilon_7=

(-2^5 * 7 * 17)^epsilon_1 * (-2^3 * 3^2 * 13^2)^epsilon_2* ….*(2^8 * 3^2 * 13)^epsilon_7=

(-1)^(epsilon_1+epsilon_2+epsilon_3 +epsilon_4) *
* 2^(5epsilon_1+3epsilon_2+5epsilon_3 +4epsilon_4+7epsilon_6+3epsilon_6+8epsilon_7) *
……. ……

=(-1)^E_1 * 2^E_2 * 3^E_3… * 17^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_7.

epsilon_1+epsilon_2+epsilon_3+ epsilon_4 =0 mod 2
5epsilon_1+3epsilon_2+5epsilon_3 +4epsilon_4+7epsilon_5+3epsilon_6+8epsilon_7 =0 mod 2
2epsilon_2+ epsilon_3 +2epsilon_4+ epsilon_5+3epsilon_6+2epsilon_7 =0 mod 2
epsilon_1+ +3epsilon_3 +3epsilon_4+ + epsilon_6 =0 mod 2
2epsilon_2+ epsilon_7 =0 mod 2
epsilon_1+ + epsilon_6 =0 mod 2

le colonne di questa matrice contengono il segno e gli esponenti dei primi della factor base
nelle relazioni ottenute:

	a(-1)	a(-5)	a(-15)	a(-23)	a(1)	a(13)	a(15)
+/-	1	1	1	1	0	0	0
2	5	3	5	4	7	3	8
3	0	2	1	2	1	3	2
7	1	0	3	3	0	1	0
13	0	2	0	0	0	0	1
17	1	0	0	0	0	1	0

modulo 2:

+/-	1	1	1	1	0	0	0
2	1	1	1	0	1	1	0
3	0	0	1	0	1	1	0
7	1	0	1	1	0	1	0
13	0	0	0	0	0	0	1
17	1	0	0	0	0	1	0

la matrice cosi' ottenuta e' la matrice dei coefficienti di un sistema lineare omogeneo 6x7.
quindi un sistema il cui spazio delle soluzioni ha dimensione almeno uno.

Risolvendo con l'eliminazione di Gauss su Z_2:
lo spazio delle soluzioni ha dimensione due (cioè' contiene due vettori indipendenti):

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

Il primo vettore corrisponde al prodotto fra terza, quarta e quinta relazione, e determina la relazione quadratica:

(1033 * 1025 * 1049)^2 = 2^16 * 3^4 * 7^6 modulo n

a=1033 * 1025 * 1049
b=2^8*3^2*7^3

gcd(a-b,n) = gcd(1033 * 1025 * 1049 - 2^8* 3^2 * 7^3, 1100017) = 1100017
gcd(a+b,n) = gcd(1033 * 1025 * 1049 + 2^8* 3^2 * 7^3, 1100017) = 1

FALLIMENTO !!!

Il secondo vettore corrisponde al prodotto fra prima, seconda, terza, quarta e sesta relazione, e determina la relazione quadratica:

(1047 * 1043 * 1033 * 1025 * 1061)^2 = 2^20 * 3^8 * 7^8 * 13^2 * 17^2 modulo n

a=1047 * 1043 * 1033 * 1025 * 1061
b=2^10 * 3^4 * 7^4 * 13 * 17

gcd(1047 * 1043 * 1033 * 1025 * 1061 - 2^10 * 3^4 * 7^4 * 13 * 17, 1100017) = 547

SUCCESSO !!!

Infatti 1100017 = 547 * 2011