Factorization nr.888

Part I

If N=4*G+3 -> N1=N ; N2=5*N

If N=4*G+1 -> N1=3*N ; N2=3*5*N

If (N1-3) mod 8 == 0 -> N=N1

else if (N2-3) mod 8 == 0 ->N=N2

(N-3)/8-q*(p-A)/8-[4-(A-7)*(A-5)/8]=A*(q+A-4-8)/8

->

N=p*q

if we choose A such that p-A mod 8 = 0 and we choose A of the same size order as q with A<q

we can write it this way

(N-3)/8-Q-[4-(A-7)*(A-5)/8]=A*X

so there are 4 chances to find A and they are

8*h+1 ; 8*h+3 ; 8*h+5 ; 8*h+7

(N-3)/8-p*(q-B)/8-[4-(B-7)*(B-5)/8]=B*(p+B-4-8)/8

->

N=p*q

if we choose B such that q-B mod 8 = 0 and we choose B of the same size order as p with B<p

we can write it this way

(N-3)/8-P-[4-(B-7)*(B-5)/8]=B*Y

so there are 4 chances to find B and they are

8*k+1 ; 8*k+3 ; 8*k+5 ; 8*k+7

f(N,A,B) is O(16)

Example

1763=41*43

220-q*(p-25)/8-[4-(25-7)*(25-5)/8]=25*(q+25-4-8)/8

220-p*(q-27)/8-[4-(27-7)*(27-5)/8]=27*(p+27-4-8)/8

220-Q-[4-(25-7)*(25-5)/8]=25*X

220-P-[4-(27-7)*(27-5)/8]=27*X

Q=25*y+11 X=10-y

P=27*x+1 X=10-x

solve Q=q*(p-25)/8=25*y+11 ,p*q=1763

-> q=67-8*y

solve p*(q-27)/8=27*x+1 ,p*q=1763

-> p=65-8*x

Part II Factorization example

The whole is based on a partial factorization of another number (which we can build ourselves (in the example 451328=8*g))

P=27*x+1 ; p=65-8*x

Q=25*y+11 ; q=67-8*y

K=(65-8*x)^2=64*x^2-1040*x+4225

(27*h-1040)^2-4*64*(4225+h)=D^2

h=1/729*(28208-sqrt(729*D^2+795691264))

795691264=1763*451328

sqrt[729*D^2+795691264]-sqrt[729*D^2]==8*(67-8*y)

replace D

sqrt[729*((27*h-1040)^2-4*64*(4225+h))+795691264]-27*sqrt[(27*h-1040)^2-4*64*(4225+h)]=8*(67-8*y)

28208-729*h-27*sqrt[(27*h-1040)^2-4*64*(4225+h)]=8*(67-8*y)

→ h=4*(64*y^2+55344*y+11964681)/(729*(8*y-67))

64*y^2+55344*y+11964681=729*W

55344+729*a=64*b -> a=16

11964681+729*c=64*d -> c=15

[64/64*y^2+((55344+16*729)/64 mod 729)*y+((11964681+15*729)/64 mod 729)] mod 729 = 0

y^2+318*y+495 mod 729 = 0

apply coppersmith method

-> y=3 → q=43

Alberico Lepore

Contact:

albericolepore@gmail.com