Lepore Factorization nr.88

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

So we will have Q=(c1)*y+(c2) and P=(c3)*x+(c4)

bruteforce 8 < X <= 192

bruteforce a > 0

on

a*(c1)*(c3)+(c2)*(c4)*b-x*1763=X

linear combination is

a*Q*P+b*q*p=W

coefficients modulo N

and W=2*N or W=3*N

Example

bruteforce 8 < X <= 192

bruteforce a > 0

on

a*25*27+8*8*b-x*1763=X

for example a=1 and X=84 -> b=1763*n+1010

linear combination is

a*(25*y+11)*(27*x+1)+b*(65-8*x)*(67-8*y)=W

1*(25*y+11)*(27*x+1)+1010*(65-8*x)*(67-8*y)=W

65315*x*y-541063*x-525175*y+4398561=W

coefficients modulo 1763

84*x*y+178*x+199*y+1639=2*1763

84*x*y+178*x+199*y+1639=2*1763
,
(65-8*x)*(67-8*y)=1763

→ x=3; y=3 → p=41 :q=43

Alberico Lepore

Contact:

albericolepore@gmail.com