# Teoria SIQS

Si sceglie “a” come prodotto di “s” primi della factor base che si avvicina alla soglia di a ideale

Si ottengono 2^(s-1) “b” diversi che danno luogo a 2^(s-1) polinomi diversi.

Si calcola il polinomio dove

.

Se l(j) viene moltiplicato per a si ottiene

che modulo N da:

Quindi se l(j) è un numero divisibile rispetto alla factor base si è ottenuta una relazione quadratica del tipo

dove FB è il prodotto con molteplicità di alcuni fattori della factor base.(ricorda che a contiene fattori della factor base quindi l(j)\*a continua a contenere fattori primi della factor base).

Combinando/Moltiplicando tra di loro queste relazioni è possibile ottenere relazioni del tipo

Che è equivalente a

E a quel punto è possibile calcolare

## Quando si trovano sicuramente dei fattori non banali di N?

Se valgono contemporaneamente

1)

2)

3)

Allora i gcd restituiscono uno il fattore p e l’altro il fattore q.

Questo succede perché la prima relazione ci dice che :

Combinando insieme le 3 affermazioni si ottiene che è necessario che un gcd ritorni p e l’altro ritorni q.

## Relazioni semi B\_smooth

Se a(j) non è esprimibile come prodotto di fattori primi della factor base la parte che avanza dalla divisione è chiamata residuo P e se compreso tra B e B^2 la relazione semi B\_smooth trovata può essere memorizzata perché è utile per calcolare delle nuove relazioni B\_smooth.

La relazione che si ottiene è:

Se si ottiene un’altra relazione semi\_B\_smooth con lo stesso residuo è possibile ottenere una relazione B\_smooth:

Moltiplicate tra loro danno:

Che portando i termini al lato corretto danno: