Introduzione all'algoritmo di Fattorizzazione.

n intero

$\alpha = [\sqrt{n}] + 1$; $\beta = (n - \alpha^2)$;

$x = \frac{y}{2} \pm \sqrt{\frac{y^2}{4} + \alpha y - \beta}$

Se per un valore di y, la quantità $D = \frac{y^2}{4} + \alpha y - \beta = z^2$, allora:

$x = \frac{y}{2} \pm z = \begin{cases} x_1 = \frac{y}{2} - z \\ x_2 = \frac{y}{2} + z \end{cases}$

$M_1 = (\alpha + x_1)$; $M_2 = (\alpha + x_2)$

se fisso ad un prefissato valore di y non si verifica che $D = z^2$, allora:

$\sqrt[4]{n}$

$(q^i - 1) = \sqrt[4]{\mu}$

i

$\downarrow$

i

$\frac{3^i - 1}{2}$

$\downarrow$

Si considerino i primi J numeri primi con $J \leq i$

Si determinino le $(2^J - 1)$ combinazioni semplici che danno luogo a $(3^J - 1)$ combinazioni generate.

Si moltiplichi di volta in volta u per ciascuna combinazione semplice. e si calcoli α, β:

$\downarrow$

$$x = \frac{y}{2} \pm \sqrt{\frac{y}{6}^2 + \alpha y - \beta}$$

Se per $y \geq 0 \Rightarrow \frac{y^2}{6} + \alpha y - \beta = \tau^2$, si determinino N_1 di u_1 col procedimento precedente e poi μ_1 col μ_2

Il valore massimo di y dipende da quanto J è minore di J.

Proseguendo in questo modo si determinerà certamente la soluzione.