UN METODO DI FATTORIZZAZIONE

Sia **N** un intero positivo:

$$N = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot x_3^{\alpha_3} \cdot \cdots\cdots \cdot x_k^{\alpha_k} = \prod_{i=1}^{k} x_i^{\alpha_i} \qquad (1)$$

N può essere visto come prodotto di due macrofattori:

$$n_{1j} = x_1^{(\alpha_1-\beta_{1j})} \cdot x_2^{(\alpha_2-\beta_{2j})} \cdot x_3^{(\alpha_3-\beta_{3j})} \cdots\cdots\cdots \cdot x_k^{(\alpha_k-\beta_{kj})} = \prod_{i=1}^{k} x_i^{(\alpha_i-\beta_{ij})}$$

$$n_{2j} = x_1^{\beta_{1j}} \cdot x_2^{\beta_{2j}} \cdot x_3^{\beta_{3j}} \cdots\cdots\cdots \cdot x_k^{\beta_{kj}} = \prod_{i=1}^{k} x_i^{\beta_{ij}} \qquad (2)$$

Con:

$$x_1 < x_2 < x_3 < \ldots\ldots x_k \quad \text{interi}$$
$$0 \le \beta_{ij} \le \alpha_i \quad \text{interi} \qquad (3)$$
$$j \le j_{Max}$$

L'indice $j = 1$ viene attribuito alla K.upla che rende minimo il valore assoluto della differenza tra la prima e la seconda delle (2); si attribuisce poi il valore j = 2 e così via.

La quantità: $\pi_j = n_{1j} \cdot n_{2j} = N \qquad \forall \quad j \le j_{Max}$

Quindi: $$N = n_{1j} \cdot n_{2j} \qquad (4)$$

non è affetto da indice.

Se oltre al prodotto conoscessimo anche la somma S_j di n_{1j} ed n_{2j} potremmo determinare immediatamente n_{1j} ed n_{2j} come soluzioni dell'equazione di secondo grado:

$$z_j^2 - \left(n_{1j} + n_{2j}\right) \cdot z_j + n_{1j} \cdot n_{2j} = 0 \qquad (5)$$

Ovvero: $$z_j^2 - S_j \cdot z_j + N = 0 \qquad (6)$$

Quindi: $$z_j = \left[S_j \pm \left(S_j^2 - 4 \cdot N\right)^{1/2}\right] / 2 \qquad (7)$$

Ed in definitiva**:**

$$n_{1j} = \left[S_j - \left(S_j^2 - 4 \cdot N\right)^{1/2}\right] / 2 \qquad (8)$$

$$n_{2j} = \left\lfloor S_j + \left(S_j^2 - 4 \cdot N\right)^{1/2} \right\rfloor / 2$$

Se n_{1j} ed n_{2j} sono entrambi pari od entrambi dispari , allora S_j è sicuramente pari cioè: $S_j = 2 \cdot h_j \Rightarrow h_j = S_j / 2$ e quindi le (8) diventano:

$$\begin{aligned} n_{1j} &= \left\lfloor h_j - \left(h_j^2 - N\right)^{1/2} \right\rfloor \\ n_{2j} &= \left\lfloor h_j + \left(h_j^2 - N\right)^{1/2} \right\rfloor \end{aligned} \qquad (9)$$

Per quanto diremo in seguito si può verificare il caso in cui le quantità n_{1j} ed n_{2j} siano una pari e l'altra dispari o viceversa,per cui dobbiamo prestare la massima attenzione nell'utilizzare le (8) o le (9).

Poiché conosciamo solo il prodotto $N = n_{1j} \cdot n_{2j}$,per determinare n_{1j} ed n_{2j} dobbiamo operare per tentativi.

Consideriamo allora la (7):

$$z_j = \left\lfloor S_j \pm \left(S_j^2 - 4 \cdot N\right)^{1/2} \right\rfloor / 2 \qquad (10)$$

Determiniamo la quantità: $\sqrt{N}$; se $\left\lfloor \sqrt{N} \right\rfloor = \sqrt{N}$ (Con $\left\lfloor \sqrt{N} \right\rfloor$ indichiamo il massimo intero contenuto in $\sqrt{N}$) ovvero se N è un quadrato perfetto,allora $n_{1j} = n_{2j} = \sqrt{N}$.
Se ciò non avviene, poniamo $s_0 = 2 \cdot \left\lfloor \sqrt{N} \right\rfloor$, $s_1 = 2 \cdot \left\lfloor \sqrt{N} \right\rfloor + 1$ e calcoliamo la quantità: $\gamma_1 = \left(s_1^2 - 4 \cdot N\right)^{1/2}$. Se γ_1 è un quadrato perfetto allora poniamo: $s_1 = S_1$ e:

$$\begin{aligned} n_{11} &= \left\lfloor S_1 - \left(S_1^2 - 4 \cdot N\right)^{1/2} \right\rfloor / 2 \\ n_{21} &= \left\lfloor S_1 + \left(S_1^2 - 4 \cdot N\right)^{1/2} \right\rfloor / 2 \end{aligned} \qquad (11)$$

Se γ_1 non è un quadrato perfetto poniamo: $s_2 = 2 \cdot \sqrt{N} + 2$ e rifacciamo il calcolo fino a quando, per un certo indice m , γ_m non risulti un quadrato perfetto; poniamo allora: $s_m = S_1$

e: $$\gamma_m = \left(s_m^2 - 4 \cdot N\right)^{1/2} = \left(S_1^2 - 4 \cdot N\right)^{1/2} \qquad (12)$$

Possiamo così determinare n_{11} ed n_{21}

Continuando il procedimento,il successivo valore per cui γ_m è un quadrato perfetto ci darà $s_m = S_2$, $\gamma_m = \left(S_2^2 - 4 \cdot N\right)^{1/2}$ e quindi: n_{12} ed n_{22}
Si osservi che il primo valore per cui γ_m è un quadrato perfetto corrisponde alla prima K.upla della (2) :

Vediamo di quantificare le operazioni da eseguire.

$$s_0 = 2 \cdot \left[\sqrt{N}\right] \quad ; \quad s_1 = 2 \cdot \left[\sqrt{N}\right] + 1 = s_0 + 1;$$

$$s_1^2 - 4 \cdot N = \left(s_0 + 1\right)^2 - 4 \cdot N = s_0^2 + 1 + 2 \cdot s_0 - 4 \cdot N = \left(s_0^2 - 4 \cdot N\right) + 2 \cdot s_0 + 1;$$

$$s_2 = 2 \cdot \left[\sqrt{N}\right] + 2 = s_0 + 2;$$

$$s_2^2 - 4 \cdot N = \left(s_0 + 2\right)^2 - 4 \cdot N = s_0^2 + 4 + 4 \cdot s_0 - 4 \cdot N = \left(s_0^2 - 4 \cdot N\right) + 4 \cdot s_0 + 4;$$

$$s_3 = 2 \cdot \left[\sqrt{N}\right] + 3 = s_0 + 3;$$

$$s_3^2 - 4 \cdot N = \left(s_0 + 3\right)^2 - 4 \cdot N = s_0^2 + 9 + 6 \cdot s_0 - 4 \cdot N = \left(s_0^2 - 4 \cdot N\right) + 6 \cdot s_0 + 9;$$

$$s_4 = 2 \cdot \left[\sqrt{N}\right] + 4 = s_0 + 4;$$

$$s_4^2 - 4 \cdot N = \left(s_0 + 4\right)^2 - 4 \cdot N = s_0^2 + 16 + 8 \cdot s_0 - 4 \cdot N = \left(s_0^2 - 4 \cdot N\right) + 8 \cdot s_0 + 16;$$

$$s_5 = 2 \cdot \left[\sqrt{N}\right] + 5 = s_0 + 5;$$

$$s_5^2 - 4 \cdot N = \left(s_0 + 5\right)^2 - 4 \cdot N = s_0^2 + 25 + 10 \cdot s_0 - 4 \cdot N = \left(s_0^2 - 4 \cdot N\right) + 10 \cdot s_0 + 25;$$

E in generale:

$$s_m = s_0 + m \qquad (13)$$

$$s_m^2 - 4 \cdot N = \left(s_0^2 - 4 \cdot N\right) + 2 \cdot m \cdot s_0 + m^2; \qquad (14)$$

Se ci interessiamo solo al caso $J = 1$, bisogna considerare la quantità $s_m = S_1$ che dà luogo ad n_{11} ed n_{21}
In tale circostanza,per semplicità, poniamo:

$$n_{11} = X \quad \text{ed} \quad n_{21} = Y \quad \text{con} \quad X \le Y \qquad (15)$$

Per cui: $$X \cdot Y = N \qquad (16)$$

$$s_m = s_0 + m$$

$$X = \left[s_m - \left(s_m^2 - 4 \cdot N \right)^{1/2} \right] / 2 \qquad (17)$$

$$X = \left\{ (s_0 + m) - \left[(s_0 + m)^2 - 4 \cdot n \right]^{1/2} \right\} / 2 \qquad (18)$$

da cui: $$m = \left(N + X^2 - 2 \cdot \left[\sqrt{N} \right] \cdot X \right) / X \qquad (19)$$

Dalla (19): $$X = \sqrt{N} \Rightarrow m = 0 \qquad (20)$$

Cioè la scomposizione nei due fattori viene immediatamente realizzata con s_0.

Ancora più semplicemente si può scrivere:

$$m = S_1 - s_0 \quad \text{ovvero:} \quad m = S_1 - 2 \cdot \left[\sqrt{N} \right] \qquad (21)$$

Riprendiamo ancora in considerazione il numero $N = X \cdot Y$ di cui,naturalmente, non conosciamo i singoli fattori.

Da quanto sin qui detto appare possibile e conveniente trasformare il numero $N = X \cdot Y$ nel numero $N_1 = X_1 \cdot Y_1$ e da questo ottenere con **" relativa facilità "** i fattori X_1 ed Y_1 tali che:

$$X_1 = \mu \cdot X \cong \sqrt{N_1} \quad \text{e} \quad Y_1 = \lambda \cdot Y \cong \sqrt{N_1} \qquad (22)$$

Con μ e λ composti da **" Fattori noti ".**

A questo punto si ricavano immediatamente X ed Y.

Per realizzare quanto propostoci operiamo come segue.

Moltiplichiamo il numero $N = X \cdot Y$ per l'intero $\vartheta = \eta_1^{\varphi_1} \cdot \eta_2^{\varphi_2} \cdot \eta_3^{\varphi_3} \cdot \cdots \cdot \eta_t^{\varphi_t}$,

con $\eta_1, \eta_2, \eta_3, \ldots\ldots\eta_t$ interi o decimali con un numero finito di decimali dopo la virgola e $\varphi_1, \varphi_2, \varphi_3, \ldots\ldots \varphi_t$ interi.

Allora: $$N_1 = \eta_1^{\varphi_1} \cdot \eta_2^{\varphi_2} \cdot \eta_3^{\varphi_3} \cdots\cdot \eta_t^{\varphi_t} \cdot X \cdot Y \qquad (23)$$

Applicando all'intero N_1 il procedimento analizzato si trova,per un opportuno valore di ϑ, come prima soluzione:

$$X_1 = \eta_1^{\varphi_1 - \omega_1} \cdot \eta_2^{\varphi_2 - \omega_2} \cdot \eta_3^{\varphi_3 - \omega_3} \cdots\cdot \eta_t^{\varphi_t - \omega_t} \cdot X$$

(24)

$$Y_1 = \eta_1^{\omega_1} \cdot \eta_2^{\omega_2} \cdot \eta_3^{\omega_3} \cdot \cdots \cdot \eta_t^{\omega_t} \cdot Y$$

Quindi:

$$\mu = \eta_1^{\varphi_1 - \omega_1} \cdot \eta_2^{\varphi_2 - \omega_2} \cdot \eta_3^{\varphi_3 - \omega_3} \cdot \cdots \cdot \eta_t^{\varphi_t - \omega_t}$$

$$\lambda = \eta_1^{\omega_1} \cdot \eta_2^{\omega_2} \cdot \eta_3^{\omega_3} \cdot \cdots \cdot \eta_t^{\omega_t} \qquad (25)$$

$$\vartheta = \mu \cdot \lambda$$

Col procedimento illustrato bisogna,tuttavia,tenere presente che $N_1 \geq N$ e pertanto se ϑ non è ben strutturato potrebbe essere vanificata ogni convenienza nell'adottare il procedimento medesimo.

Dalla: $m = S_1 - s_0$ osserviamo che: $m_{\max} = S_{1\max} - s_0$ ed essendo:
$S_{1\max} = N_1 + 1$ ed $s_0 = 2 \cdot \left[\sqrt{N_1}\right]$ si ha:

$$m_{\max} = N_1 + 1 - 2 \cdot \sqrt{N_1} \qquad (26)$$

E ancora dalla relazione: $S_1 = X_1 + N / X_1$:

$dS_1 / dX_1 = 1 - N / X_1^2$ da cui: $dS_1 / dX_1 = 0 \quad \Rightarrow \quad X_1 = Y_1 = \sqrt{N_1}$
ed $S_{1\min} = 2 \cdot \sqrt{N}$

$m_{\min} = S_{1\min} - s_0$ ovvero: $m_{\min} = 0$ (27)

Cosa che,del resto, era stata osservata in precedenza.

E' necessario precisare che questa trattazione è stata sviluppata in maniera estremamente sintetica senza considerare, fra l'altro, i relativi problemi di complessità computazionale e il dimensionamento di ϑ .
ϑ, ad esempio, potrebbe essere: $\vartheta = \eta!$ (con η di valore opportuno), oppure il prodotto dei primi p numeri primi, ovvero:
$\vartheta = p_p!$ (dove abbiamo usato, analogicamente, il simbolo del fattoriale) o ancora il prodotto dei primi p numeri primi dispari.
Se si considera poi che per fattorizzare un numero con alcune centinaia di cifre potrebbero rendersi necessari molti processori operanti in parallelo,ciascuno con una propria ϑ_φ, si vede come la correlazione fra fra le ϑ_φ e il tipo e la dimensione di ciascuna di esse assuma particolare importanza per la soluzione del problema.
Un'altra questione che qui si vuole evidenziare è quella relativa all'esistenza o meno di una serie "ottima", ovvero di un particolare ϑ che per qualunque valore dei fattori X ed Y di N dia una differenza tra Y_1 ed X_1 tale da rendere vantaggiosa la procedura rispetto a qualsiasi algoritmo alternativo.

E' facile ,comunque,pervenire alla conclusione che,con alta probabilità,almeno uno di ω processori in parallelo effettui la fattorizzazione di un numero dell'ordine di 10^{ω} per $m=1$,cioè al primo passaggio.
In sostanza, per un numero di 100 cifre bastano 100 processori operanti in parallelo e per uno di 1000 cifre ne bastano 1000.

Queste dimostrazioni non vengono qui svolte per non appesantire il discorso oltre misura.

Un risultato,tuttavia,si ritiene utile presentare e precisamente nel caso in cui ϑ sia il prodotto dei primi t numeri primi ed $N = X \cdot Y$, cioè costituito da due soli fattori primi e quindi:

$$N_1 = \vartheta \cdot X \cdot Y = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \cdots \cdot p_t \cdot X \cdot Y \qquad (28)$$

Allora,con semplici passaggi,si ottiene che il numero delle soluzioni totali fornite dalla (11) sono pari a Σ , con Σ così espresso:

Per t dispari:

$$\Sigma = \binom{t+2}{1} + \binom{t+2}{2} + \binom{t+2}{3} + \cdots\cdots + \binom{t+2}{(t+2)/2} + 1 = 2^{(t+1)} \qquad (29)$$

Per t pari:

$$\Sigma = \binom{t+2}{1} + \binom{t+2}{2} + \binom{t+2}{3} + \cdots\cdots + \binom{t+2}{(t+2)/2} / 2 + 1 = 2^{(t+1)} \qquad (30)$$

In definitiva per qualunque valore di t : $\Sigma = 2^{t+1}$ (31)

Il numero delle soluzioni **" utili "** C_u , cioè quelle che contengono la **X** e la **Y** separate sono:

$$C_u = 2^t \qquad (32)$$

Il discorso è facilmente generalizzabile.

E’ il momento di considerare alcuni esempi.

n°1) N = 2183

Poniamo $\vartheta = \mu \cdot \lambda = 3 \cdot 5$;
Allora: $N_1 = 3 \cdot 5 \cdot 2183 = 32745$; $\sqrt{N_1} = 180{,}9558..$; $\left[\sqrt{N_1}\right] = 180$;
Poiché N_1 è dispari possiamo applicare la formula ridotta:

$$z = h \pm \left(h^2 - N_1\right)^{1/2}; \qquad s_0 = \left[\sqrt{N_1}\right];$$

Come abbiamo visto,per t = 2, si hanno $\Sigma = 2^3$ soluzioni:

La prima si trova al primo passaggio. Infatti:

$$h_1 = 180 + 1 = 181;\ \gamma_1^2 = 181^2 - N_1 = 16; \Rightarrow \gamma_1 = \sqrt{16} = 4; \Rightarrow$$
$$z_1 = 181 - 4 = 177; \quad z_2 = 181 + 4 = 185; \Rightarrow$$
$$z_1 = 3 \cdot 59; \qquad z_2 = 5 \cdot 37; \Rightarrow \qquad X_1 = 5 \cdot 37; Y_1 = 3 \cdot 59; \mu = 5; \lambda = 3;$$

La seconda si trova per m = 23, infatti:

$$h_{23} = (180 + 23) = 203; \quad \gamma_{23}^2 = (203)^2 - N_1 = 8464; \gamma_{23} = \sqrt{8464} = 92; \Rightarrow$$
$$X_2 = 111 = 3 \cdot 37; \qquad Y_2 = 295 = 5 \cdot 59;$$

La terza si trova per $m = 127$, infatti:

$$h_{127} = 180 + 127 = 307; \quad \gamma_{127} = \left(307^2 - N_1\right)^{1/2} = 248;$$
$$X_3 = 59; \quad Y_3 = 3 \cdot 5 \cdot 37;$$

La quarta si ha per $m = 281$; infatti:

$$h_{281} = 180 + 281 = 461; \quad \gamma_{281} = \left(281^2 - N_1\right)^{1/2} = 424;$$

$$X_4 = 37; \quad Y_4 = 3 \cdot 5 \cdot 59;$$

La quinta si trova per $m = 919$, infatti:

$$h_{919} = 180 + 919 = 1099; \quad \gamma_{919} = \left(1099^2 - N_1\right)^{1/2} = 1084; \qquad \Rightarrow$$
$$X_5 = 15 = 3 \cdot 5; Y_5 = 2183 = 37 \cdot 59;$$

La sesta si trova per $m = 3097$,infatti:

$$h_{3097} = 3097 + 180 = 3297; \quad \gamma_{3097} = \left(3277^2 - N_1\right)^{1/2} = 3272; \quad \Rightarrow$$
$$X_6 = 5; \qquad Y_6 = 3 \cdot 37 \cdot 59;$$

La settima si ha per: $m = 5279$, infatti:

$h_{5279} = 180 + 5279 = 5459; \quad \gamma_{5279} = \left(5459^2 - N_1\right)^{1/2} = 5456; \quad \Rightarrow$
$X_7 = 3; \quad Y_7 = 5 \cdot 37 \cdot 59;$

L'ottava si ha per m = 16193, infatti:

$h_{16193} = 180 + 16193 = 16373; \quad \gamma_{16373} = \left(16373^2 - N_1\right)^{1/2} = 16372;$

$X_8 = 1; \qquad Y_8 = 3 \cdot 5 \cdot 37 \cdot 59;$

Naturalmente ,in questo caso, i valori di m utili sono $C_u = 2^2$: m = 1; m = 23 ; m = 127; m =281; in quanto per tali valori i fattori primi di N risultano separati.

n°2) N =11147; $\vartheta = 2$; $N_1 = 2 \cdot 11147 = 22294;$

I macrofattori di N_1 sono sicuramente uno pari e l'altro dispari o viceversa per cui dobbiamo usare la formula completa.

$\sqrt{N_1} = 149{,}3118..; \qquad s_0 = 2 \cdot \left[\sqrt{N_1}\right] = 2 \cdot 149;$
$s_1 = 2 \cdot 149 + 1; \quad \gamma_1 = (2 \cdot 149 + 1)^2 - 4 \cdot 22294 = 225; \quad \sqrt{\gamma_1} = 15;$

$z = (299 \pm 15)/2; \quad X_1 = 142 = 2 \cdot 71; \quad Y_1 = 157; \Rightarrow \quad X = 71; Y = 157;$

n° 3) N = 3234846615; $\sqrt{N} = 56875{,}7120; \qquad \left[\sqrt{N}\right] = 56875;$

$\gamma_1 = \left(56876^2 - N\right)^{1/2} = 181;$

$X = 56876 - 181 = 56695; \qquad Y = 56876 - - + 181 = 57057;$

Scomponendo con lo stesso procedimento si ottiene:

$X = 5 \cdot 17 \cdot 23 \cdot 29; \qquad Y = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 19;$

Andando avanti,per m = 253,si trova la seconda soluzione; per m = 333 la terza;
per m = 577 la quarta,e così via.

n° 4) $N = 2722331;$

$\sqrt{N} = 1649{,}9488; \qquad \left[\sqrt{N}\right] = 1649; \quad \gamma_1 = \left(1650^2 - N\right) = 13;$

$X = 1650 - 13 = 1637; \qquad Y = 1650 + 13 = 1663;$

n° 5) N = 721949; $\vartheta = 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7;$ $N_1 = 3638622960;$

$\sqrt{N_1} = 60320{,}99933...;$ $h_0 = \left[\sqrt{N_1}\right] = 60320;$ $h_1 = h_0 + 1 = 60321;$

$\gamma_1 = \left(h_1^2 - N_1\right)^{1/2} = 9;$

$X_1 = 60321 - 9 = 60312 = 2^2\cdot 3\cdot 7\cdot 359;$ $Y_1 = 60321 + 9 = 60330 = 2\cdot 3\cdot 5\cdot 2011;$

$X = 359;$ $Y = 2011;$

n° 6) N = 1051877; $\vartheta = 2\cdot 3\cdot 4;$ $N_1 = \vartheta\cdot N = 25245048;$

$\left[\sqrt{N_1}\right] = 5024;$ $s_0 = 2\cdot\left[\sqrt{N_1}\right] = 10048;$ $s_1 = s_0 + 1 = 10049;$

$\gamma_1 = \left(s_1^2 - 4\cdot N_1\right)^{1/2} = 47;$

$X_1 = (10049 - 47)/2 = 5001 = 3\cdot 1667;$ $Y_1 = (10049 + 47)/2 = 5048 = 2^3\cdot 631;$ $\Rightarrow$

$X = 631;$ $Y = 1667;$

n° 7) N = 11466979; $\vartheta = 2\cdot 3\cdot 4\cdot 5\cdot 6;$ $N_1 = \vartheta\cdot N = 8256224880;$

$\left[\sqrt{N_1}\right] = 90863; h_1 = 90864; \gamma_1 = \left(90864^2 - N_1\right)^{1/2} = 204;$

$X_1 = 90864 - 204 = 90660 = 2^2\cdot 3\cdot 5\cdot 1511;$

$\Rightarrow$

$Y_1 = 90864 + 204 = 91068 = 2^2\cdot 3\cdot 7589;$

$X = 1511;$ $Y = 7589;$

n° 8) $N = 11618759;$ $\vartheta = 2\cdot 3\cdot 4\cdot 5\cdot 6;$ $N_1 = \vartheta\cdot N = 8365506480;$

$\left[\sqrt{N_1}\right] = 91463; h_1 = 91464; \gamma_1 = \left(91464^2 - N_1\right)^{1/2} = 396;$

$X_1 = 91464 - 396 = 91068 = 2^2\cdot 3\cdot 7589;$

$\Rightarrow$

$Y_1 = 91464 + 396 = 91860 = 2^2\cdot 3\cdot 5\cdot 1531;$

$X = 1531;$ $Y = 7589;$

n° 9) N = 660743; $\vartheta = 2\cdot 3\cdot 4\cdot 5\cdot 6;$ $N_1 = \vartheta\cdot N = 475734960;$ $\sqrt{N_1} = 21811{,}3493..;$

$\left[\sqrt{N_1}\right] = 21812; \quad \gamma_{12} = \left(21823^2 - N_1\right)^{1/2} = 713;$

$X_1 = 21823 - 713 = 21110 = 2 \cdot 5 \cdot 2111; \quad Y_1 = 21823 + 713 = 22536 = 2^3 \cdot 3^2 \cdot 313;$

$X = 313; \quad Y = 2111;$

n° 10) N = 8027323; $\vartheta = 3 \cdot 5 \cdot 7 \cdot 11; \quad N_1 = \vartheta \cdot N = 9271558065;$

$\left[\sqrt{N_1}\right] = 96288; \quad h_1 = 96289; \quad \left(96289^2 - N_1\right)^{1/2} = 116;$

$X_1 = 96289 - 116 = 96173 = 7 \cdot 11 \cdot 1249; \quad Y_1 = 96289 + 116 = 96405 = 3 \cdot 5 \cdot 6427;$

$X = 1249; \quad Y = 6427;$

n° 11) N = 259283; $\vartheta = 3 \cdot 5 \cdot 7 \cdot 9; \quad N_1 = \vartheta \cdot N = 245022435;$

$\left[\sqrt{N_1}\right] = 15653; h_1 = 15654; \gamma_1 = \left(15654^2 - N_1\right)^{1/2} = 159;$

$X_1 = 15654 - 159 = 15495 = 3 \cdot 5 \cdot 1033; Y_1 = 15654 + 159 = 15813 = 7 \cdot 9 \cdot 251;$

$X = 251; \quad Y = 1033;$

n° 12) N = 686471; $\vartheta = 3^4 \cdot 5; \quad N_1 = \vartheta \cdot N = 278020755; \quad \left[\sqrt{N_1}\right] = 16673;$

$h_1 = 16674; \quad \gamma_1 = \left(16674^2 - N_1\right)^{1/2} = 39:$

$X_1 = 16674 - 39 = 16635 = 3 \cdot 5 \cdot 1109; \quad Y_1 = 16674 + 39 = 16713 = 3^3 \cdot 719;$

$X = 619; \quad Y = 1109;$

n° 13) N = 7776481; $\vartheta = 5 \cdot 7; \quad N_1 = \vartheta \cdot N = 272176835;$

$\left[\sqrt{N_1}\right] = 16497; \quad h_1 = 16498; \quad \gamma_{21} = \left(16498^2 - N_1\right)^{1/2} = 817;$

$X_1 = 16518 - 817 = 15701 = 7 \cdot 2243; \quad Y_1 = 16518 + 817 = 17335 = 5 \cdot 3467;$

$X = 2243; \quad Y = 3467;$

n° 14) N = 7776481; $\vartheta = 7 \cdot 11;$ $N_1 = \vartheta \cdot N = 598789037;$

$\left[\sqrt{N_1}\right] = 24470;$ $h_1 = 24471;$ $\gamma_1 = \left(24471^2 - N_1\right)^{1/2} = 202;$

$X_1 = 24471 - 202 = 24269 = 7 \cdot 3467;$ $Y_1 = 24471 + 202 = 26673 = 11 \cdot 2243;$

$X = 2243;$ $Y = 3467;$

n° 15) N = 718889; $\vartheta = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6;$ $N_1 = \vartheta \cdot N = 517600080;$

$\left[\sqrt{N_1}\right] = 22750;$ $h_1 = 22751;$ $\gamma_1 = \left(22751^2 - N_1\right)^{1/2} = 89;$

$X_1 = 22751 - 89 = 22662 = 2 \cdot 3^2 \cdot 1259;$ $Y_1 = 22751 + 89 = 22840 = 2^3 \cdot 5 \cdot 571;$

$X = 571;$ $Y = 1259;$

n° 16) N = 13522441; $\vartheta = 2 \cdot 3 \cdot 4 \cdot 5;$ $N_1 = \vartheta \cdot N = 9736157520;$

$\left[\sqrt{N_1}\right] = 98671;$ $\gamma_{50} = \left(98721^2 - N_1\right)^{1/2} = 3111;$

$X_1 = 98721 - 3111 = 95610 = 2 \cdot 3 \cdot 5 \cdot 3187;$ $Y_1 = 98721 + 3111 = 101832 = 2^3 \cdot 3 \cdot 4243;$

$X = 3187;$ $Y = 4243;$

n° 17) N = 17698727; $\vartheta = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6;$ $N_1 = \vartheta \cdot N = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 17698727;$

$s_0 = 2 \cdot \left[\sqrt{N_1}\right] = 225770;$ m = 1; $s_1 = 225771;$ $\gamma_1 = \left(225771^2 - 4 \cdot N_1\right) = 459;$

$X_1 = \left(225771 - \gamma_1\right)/2 = 112656 = 2^4 \cdot 3 \cdot 2347;$ $Y_1 = \left(225771 + \gamma_1\right)/2 = 113115 = 3 \cdot 5 \cdot 7541;$

$X = 2347;$ $Y = 7541;$

Procediamo ora alla fattorizzazione di N con il valore di $\vartheta = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7;$

N = 17698727; $\vartheta = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7;$ $N_1 = \vartheta \cdot N = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 17698727;$

$s_0 = 2 \cdot \left[\sqrt{N_1}\right] = 597332;$ m = 30; $s_{30} = 597362;$ $\gamma_{30} = \left(597362^2 - 4 \cdot N_1\right)^{1/2} = 5918;$

$X_1 = \left(597362 - 5918\right)/2 = 295722 = 2 \cdot 3^2 \cdot 7 \cdot 2317;$

$\Rightarrow$

$Y_1 = \left(597362 + 5918\right)/2 = 301640 = 2^3 \cdot 5 \cdot 7541;$

$X = 2347;$ $Y = 7541;$

Si osservi come in questo caso,aumentando il valore di ϑ il valore di m cresce .

Procediamo ancora alla fattorizzazine di N con il valore di $\vartheta = 3^2 \cdot 5 \cdot 7 \cdot 11;$

In tal caso si ha:

N = 17698727; $\quad \vartheta = 3^2 \cdot 5 \cdot 7 \cdot 11; \quad N_1 = \vartheta \cdot N = 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17698727;$

$\left\lfloor \sqrt{N_1} \right\rfloor = 247641; \quad m = 3; \quad \gamma_3 = \left(247644^2 - N_1\right)^{1/2} = 1209;$

$X_1 = (247644 - 1209) = 246435 = 3 \cdot 5 \cdot 7 \cdot 2347;$

$\Rightarrow$

$Y_1 = (247644 + 1209) = 248853 = 3 \cdot 11 \cdot 7541;$

$X = 2347; \qquad Y = 7541;$

n° 18) N = 18832594345392671; $\quad \vartheta = 2 \cdot 3 \cdot 4 \cdot 5; \quad N_1 = \vartheta \cdot N;$

$\left\lfloor \sqrt{N_1} \right\rfloor = 1503300143; \quad s_0 = 2 \cdot \left\lfloor \sqrt{N_1} \right\rfloor = 3006600286; \quad s_1 = 3006600287;$

$\gamma_1 = \left(s_1^2 - 4 \cdot N_1\right) = 17; \quad m = 1;$

$X_1 = (s_1 - \gamma_1)/2 = 1503300135; \quad X_1 = (s_1 + \gamma_1)/2 = 1503300152;$

$X = X_1 / 3 \cdot 5 = 100220009; \quad Y = Y_1 / 2 \cdot 4 = 187912519;$

n° 19) Consideriamo ora un caso che risolveremo in tre modi diversi.

N = 7956937;

1°) $\vartheta = 1; \quad N_1 = \vartheta \cdot N = N; \quad \left\lfloor \sqrt{N} \right\rfloor = 2820; \quad m = 4018;$

$\gamma_{4018} = 3864;$ X = 1487; Y = 5351;

2°) $\vartheta = 2 \cdot 3 \cdot 4 \cdot 5; \quad N_1 = \vartheta \cdot N = 954832440;$

$\left\lfloor \sqrt{N_1} \right\rfloor = 30900; \quad 2 \cdot \left\lfloor \sqrt{N_1} \right\rfloor = 61800; \quad m = 46; \quad \gamma_{46} = 2366;$

$X_1 = 29740; \quad Y_1 = 32106; \quad X = 1487; \quad Y = 5351;$

3°) $\vartheta = 2 \cdot 3 \cdot 4 \cdot 5{,}4 = 129.6000; \quad N_1 = \vartheta \cdot N = 1031219035{,}2000$

Abbiamo usato anche numeri decimali;

$\sqrt{N_1} = 32112{,}5993..; \quad 2 \cdot \sqrt{N_1} = 64225{,}1986..;$

Poiché abbiamo una sola cifra decimale dobbiamo considerare la quantità:

$\left[2 \cdot \sqrt{N_1}\right] = 64225{,}1000;$

E incrementare questo valori di un decimo alla volta.

$s_1 = 64225{,}2000; \quad \gamma_1 = 13{,}2000;$

$X_1 = 32106; Y_1 = 32119{,}2000; X = 32119.2000 / 4 \cdot 5{,}4 = 1487; Y = 32106 / 6 = 5351;$

n° 20) N = 2077; $\vartheta = 2{,}16 \quad N_1 = \vartheta \cdot N = 4486{,}32; \quad \sqrt{N_1} = 66{,}9800; \quad s_0 = 2 \cdot \sqrt{N_1} = 133{,}96;$

$z = (133{,}96 \pm 0{,}04)/2; \quad X_1 = 66{,}96; Y_1 = 67; X = 66{,}96 / 2{,}16 = 31; Y = 67;$

n° 21) N = 969853; $\vartheta = 1{,}02 \cdot 1{,}1 \cdot 1{,}2 \cdot 3; \quad N_1 = \vartheta \cdot N; \quad s_0 = 3958{,}3;$

$s_2 = 3958{,}50; \quad \gamma_2 = 1{,}14;$

$z = (3958{,}50 \pm 1{,}14)/2; \quad X_1 = 1978{,}68; Y_1 = 1979{,}82;$

$X = 1979{,}82 / 1.02 \cdot 3 = 647; \quad Y = 1978{,}68 / 1{,}1 \cdot 1{,}2 = 1499;$

n° 22) N = 5422773 ; $\vartheta = 5 \cdot 10 \cdot 11; \quad N_1 = \vartheta \cdot N = 2982525150; \quad \left[\sqrt{N_1}\right] = 54612;$

$s_0 = 2 \cdot \left[\sqrt{N_1}\right] = 109224; \quad s_1 = 109225; \quad \gamma_1 = \sqrt{109225^2 - 4 \cdot N_1} = 5;$

$X_1 = (109225 - 5)/2 = 54610; \quad Y_1 = (109225 + 5)/2 = 54615;$

$X = 54615 / 5 \cdot 11 = 993; \quad Y = 54610 / 10 = 5461;$

Con valori decimali avremmo:

N = 5422773 ; $\vartheta = 5 \cdot 1{,}1; \quad N_1 = \vartheta \cdot N = 29825251{,}50; \quad \left[\sqrt{N_1}\right] = 5461{,}2;$

$s_0 = 2 \cdot \left[\sqrt{N_1}\right] = 10922{,}4; \quad s_1 = 10922{,}5; \quad \gamma = 0{,}5;$

$X_1 = (10922{,}5 - 0{,}5)/2 = 5461; \quad Y_1 = (10922{,}5 + 0{,}5)/2 = 5461{,}5;$

$X = 5461{,}5 / 5 \cdot 1{,}1 = 993; \quad Y = 5461;$

n° 23) N = 1774821; $\vartheta = 1{,}005 \cdot 1{,}01 \cdot 1{,}05 \cdot 3 \cdot 10 \cdot 11$; $N_1 = \vartheta \cdot N$;

$s_0 = 2 \cdot \sqrt{N_1} = 49969{,}22$; $s_1 = 49969{,}23$; $\gamma_1 = \sqrt{s_1^2 - 4 \cdot N_1} = 22{,}74$;

$X_1 = (49969{,}23 - 22{,}74)/2 = 24973{,}245$; $Y_1 = (49969{,}23 + 22{,}74)/2 = 24995{,}985$;

$X = (24973{,}245)/(3 \cdot 11 \cdot 1{,}005) = 753$; $Y = (24995{,}985)/(10 \cdot 1{,}05 \cdot 1{,}01) = 2357$;

Autore : ***Prof. Santo Giovanni Torrisi***
Contact: ***sgtorrisi@virgilio.it***
Dirigente del Liceo Scientifico " C. Caminiti " di S.Teresa di Riva (ME).