Un Algoritmo, efficace ed efficiente, di FATTORIZZAZIONE (1)

Dato $N = N_1 \times N_2$ (1)
con N_1 ed N_2 interi primi (il discorso è valido per qualunque numero di fattori primi di N),
si calcoli:

$\alpha = [\sqrt{N}] + 1$; (2) ; $\beta = (N - \alpha^2)$; (3)

si avrà: $-\beta > 0$ (4);

Se $-\beta = \delta^2$ (5), con δ intero, allora:

$N_1 = (\alpha - \delta)$ (6) ; $N_2 = (\alpha + \delta)$; (7)

Il numero N è stato fattorizzato

Se $-\beta \neq \delta^2$ (8), con δ intero, si consideri la relazione:

$(\alpha y - \beta) = -\delta_1 \cdot \delta_2$ (9), equivalente alla (1)

Con $\delta_1 = (N_1 - \alpha)$ (10), $\delta_2 = (N_2 - \alpha)$ (11)

$y = (\delta_1 + \delta_2) = (N_1 + N_2 - 2\alpha)$ (12);

È facile osservare che:

$\delta_1 = -(z \cdot y + r)$ (13); $\delta_2 = [(z+1)y + r]$ (14);

con $z \geq 0$ intero ed $r > 0$ intero

Si avrà: $(\alpha \cdot y - \beta) = (z \cdot y + r) \cdot [(z+1)y + r]$ (15):

da cui:

$-\beta \bmod y = (r \bmod y)^2 = r^2 \bmod y$ (16) $\Rightarrow$

$r^2 = m \cdot y - \beta \bmod y$ (17)

con $0 \leq m \leq (y-1)$ (18);

Ponendo $-\beta \bmod y = \mu$ (19) si avrà:

$r^2 = m \cdot y + \mu$ (20); $0 \leq \mu \leq (y-1)$, (21)

Utilizzando i noti teoremi ed alcuni artifici di calcolo, è facile determinare la corrispondenza tra y e μ. Non è superfluo precisare inoltre che già in partenza è possibile circoscrivere i valori effettivi di y riducendone il numero al 20%.

In sostanza, dato un ammissibile valore di y, si calcola il corrispondente valore di μ e si verifica se esiste un r^2 tale che:

$r^2 = m \cdot y + \mu$

In realtà durante il processo di fattorizzazione non è necessario effettuare questo calcolo, in quanto dato un valore di y, la quantità $r^2 = m \cdot y + \mu$ si può calcolare in anticipo e utilizzare per qualunque fattorizzazione.

Per ciascun valore di y bisogna memorizzare la matrice di pagina seguente

y

m \ u	0	1	2						$(y-1)$
0									
1									
2									
				r^2					
$(y-1)$									

Per ogni valore di y si ha un foglio costituito dalla matrice di cui sopra.
Le coppie (m, u) individuano la casella all'interno della matrice.
Per un dato valore di y, la colonna che interessa è quella relativa al valore u.
Se nella colonna esiste almeno un valore r^2 allora si verifica l'eguaglianza.

$$(\alpha \cdot y - \beta) = -\delta_1 \cdot \delta_2 \quad (22)$$

Se l'uguaglianza è valida allora:

$$\begin{cases} N_1 = (\alpha + \delta_1) \\ N_2 = (\alpha + \delta_2) \end{cases} \quad (23)$$

Altrimenti si prosegue fino a verificare l'uguaglianza (23).

È ancora opportuno precisare che nella verifica della (22), alcuni semplici artifici di calcolo possono ridurre notevolmente i tempi di elaborazione.

Per la fattorizzazione di numeri con un elevato numero di cifre conviene utilizzare una procedura mista, impiegando anche la tecnica delle combinazioni semplici di cui si è parlato precedentemente.

Esempio 1 $N = 466.793$;

$\sqrt{N} = 683,2225\ldots \Rightarrow \alpha = 684$; $\beta = (N-\alpha^2) = -1063$;

$684 \cdot y + 1063 = -\delta_1 \cdot \delta_2$; $r^2 = my + \mu$

I valori ammissibili di y hanno l'ultima cifra di 6 o di 8.

$\mu(6) = 1$; $\Rightarrow r^2 = m \times 6 + 1 \Rightarrow$ $m = 0 \to r = 1$; $m = 4 \to r = 5$;

$(684 \times 6 + 1063) = (2 \times 6 + 1)\left[(2+1)6+1\right]$ NON AMMETTONO SOLUZIONI INTERE

$(684 \times 6 + 1063) = (2 \times 6 + 5)\left[(2+1)6+5\right]$

$\mu(8) = 4 \Rightarrow r^2 = m \times 8 + 17$: NON AMMETTE SOLUZIONI

$\mu(16) = 4$; $\Rightarrow r^2 = m \cdot 16 + 4 \Rightarrow$ NON AMMETTE SOLUZIONI

$\mu(18) = 1 \Rightarrow r^2 = m \times 18 + 1 \Rightarrow$ $m = 0 \to r = 1$; $m = 16 \to r = 17$;

$(684 \times 18 + 1) = (2 \times 18 + 1)\left[(2+1)18+1\right]$ NON AMMETTE SOL. INTERE

$(684 \times 18 + 1) = (2 \times 18 + 17)\left[(2+1)18+17\right] \Rightarrow z = 5 \Rightarrow$

$\delta_1 = -107$; $\delta_2 = 125 \Rightarrow y = 18$

$N_1 = 684 - 107 = 577$; $N_2 = 684 + 125 = 809$;

Esempio 2 $N = 9.860.616.223$;

$\sqrt{N} = 99.309,6356.. \Rightarrow \alpha = 99301$;

$\beta = (N - \alpha^2) = -72378$

$99301 \cdot y + 72378 = -\delta_1 \cdot \delta_2$;

$h^2 = m \cdot y + \mu$;

I valori ammissibili di y hanno l'ultima cifra di 2 o di 4;

Operando per valori crescenti di y si trova che per $y = 254$ e per $m = 23$ si ha:

$$78^2 = 23 \times 254 + 242$$

essendo $\mu(254) = 242$;

quindi $h = 78$

dove anche: $99301 \times 254 + 72378 =$

$$= (2 \cdot 254 + 78)[(7+1)254 + 78];$$

Valida per $z = 19$; $\Rightarrow \delta_1 = -4904$; $\delta_2 = 5158 \Rightarrow$

$y = \delta_1 + \delta_2 = 254$;

$N_1 = (\alpha + \delta_1) = 99301 - 4904 = 94397$;

$N_2 = (\alpha + \delta_2) = 99301 + 5158 = 104459$