La fattorizzazione con il metodo di Fermat ottimizzato

Di Cristiano Armellini, cristiano.armellini@alice.it

Secondo la fattorizzazione con il metodo di Fermat ogni numero dispari composto ***n*** può scriversi come differenza di due quadrati ovvero: $n = a^2 - b^2 = (a-b)(a+b) = pq$.

Supponiamo che $a \approx kb$ ovvero $a = kb$ intendendo che ***k, a, b*** sono interi positivi e il simbolo "=" deve essere letto nel senso di "circa". Sostituendo avrò $n = a^2 - b^2 = k^2b^2 - b^2 = b^2(k^2 - 1), k > 1$ quindi $b = \sqrt{\frac{n}{k^2-1}}$. Se chiamo $\bar{b} = \text{int}(b)$ dove ***int*** è la funzione parte intera allora basterà trovare per quale valore intero di $\bar{b} \geq \text{int}(b)$ dà $a = \sqrt{\bar{b}^2 + n}$ ponendo ad ogni ciclo di prova $\bar{b} = \bar{b} + 1$. Osserviamo che $p = a - b < \sqrt{n}, q = a + b > \sqrt{n}$ e questo ci porta a dedurre che $b > \frac{\sqrt{n}}{k+1}, b < \frac{\sqrt{n}}{k-1}$, ovvero in definitiva possiamo scrivere che $\frac{\sqrt{n}}{\sqrt{k^2-1}} < b < \frac{\sqrt{n}}{k-1}$. Se assegniamo ad ogni computer di un rete un differente valore di ***k = 2, 3, 4, 5, ...*** e facciamo girare l'algoritmo su ogni PC in breve tempo possiamo fattorizzare numeri RSA anche di grandi dimensioni.

Nel caso di ***k=1***, basterà considerare $a = \sqrt{b^2 + n}, b = 0,1,2,3..$

Una forma in python molto semplificata può essere:

```
import math;
def factor(n, k):
    b = math.floor(math.sqrt(n/(k*k-1)));
    a = math.sqrt(b*b+n);
    while (a!= math.floor(a)):
        b = b+1;
        a = math.sqrt(b*b+n);
    print(a-b);
    print(a+b);
```

Per non appesantire il codice non è stato messo l'estremo superiore per ***b*** e il doppio ciclo per ***k*** e per ***b*** ma il lettore sulla base dell'algoritmo descritto potrà sviluppare un codice più performante.

Osservazione: se $a = kb$ e facciamo il rapporto $l = q/p=(a+b)/(a-b)=(k+1)/(k-1)$ che per valori di ***k*** crescenti tende sempre a 1 e questo fatto ci è particolarmente utile quando consideriamo problemi RSA dove il rapporto tra il fattore più grande e quello più piccolo è poco più dell'unità.