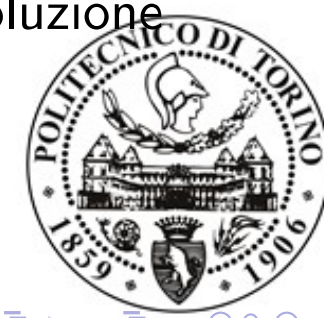
Fattorizzazione

Dato un intero positivo N quali sono i numeri primi che lo compongono ?

Si tratta di un problema di fattorizzazione che può essere ricondotto al problema di ricerca del periodo (ordine). L'algoritmo di fattorizzazione procede in due passi che provano rispettivamente che:

- è possibile ottenere un fattore di N se possiamo trovare una soluzione non banale $x \neq \pm 1 (\mathrm{mod}\, N)$ dell'equazione $x^2 = 1 (\mathrm{mod}\, N)$.
- dato un y scelto casualmente co-primo di N, tale y ha con una certa probabilità un ordine r che è un numero pari e tale che $y^{r/2} \neq \pm 1 (\mathrm{mod}\, N)$. Quindi $x \equiv y^{r/2} (\mathrm{mod}\, N)$ è una soluzione non banale per $x^2 = 1 (\mathrm{mod}\, N)$.



Fattorizzazione

Tutti i passaggi dell'algoritmo possono essere eseguiti in modo efficiente su un computer classico tranne (per quanto noto oggi) una "subroutine" di ricerca ordini utilizzata dall'algoritmo per la quale è stata proposta la routine di ricerca del periodo quantistica della lezione precedente.

Ripetendo la procedura potremmo trovare una fattorizzazione primaria completa di N. L'algoritmo è riassunto di seguito.

Fattorizzazione

Inputs: Un numero N prodotto di numeri primi

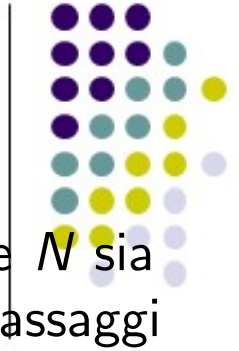
Outputs: Un fattore of N (non banale)

Tempo di esecuzione: $O\left((\log N)^3\right)$. Probabilità di successo $O(1)$

Procedimento:

1. Se N è pari, restituisce il fattore 2
2. Se $N = a^b$ per gli interi $a \geq 1$ e $b \geq 2$, restituire il fattore a.
3. Sceglie in modo casuale x nell'intervallo 1 - $N - 1$, se $\gcd(x, N) > 1$ restituisce il fattore $\gcd(x, N)$
4. Usa la subroutine di *order-finding* per trovare r di x modulo N
5. Se r è pari e $x^{r/2} \neq -1 (\mathrm{mod}\, N)$ allora calcola $\gcd\left(x^{r/2} - 1, N\right)$ e $\gcd\left(x^{r/2} + 1, N\right)$, per verificare che uno di questi è un fattore non triviale, restituisci quel fattore. Altrimenti, riprova.

Fattorizzazione



I passaggi 1 e 2 restituiscono un fattore, oppure assicurano che N sia un numero intero dispari con più di un fattore primo. Questi passaggi possono essere eseguiti utilizzando rispettivamente un numero di operazioni $O(1)$ e $O\left(L^3\right)$.

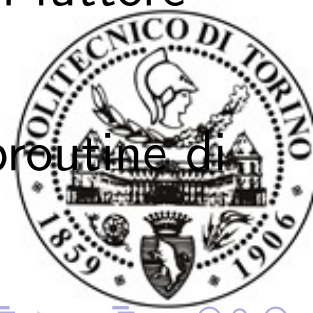
Il passaggio 3 restituisce un fattore o produce un elemento scelto in modo casuale x di $\{0, 1, 2, \ldots, N-1\}$.

Il passaggio 4 chiama la subroutine di ricerca dell'ordine, calcolando l'ordine r di x modulo N.

Il passaggio 5 completa l'algoritmo.

Il teorema 5.3 garantisce che con probabilità almeno pari adun mezzo, r sarà pari e $x^{r/2} \neq -1 (\mathrm{mod}\, N)$, e quindi il Teorema 5.2 garantiscono che $\gcd\left(x^{r/2}-1, N\right)$ o $\gcd\left(x^{r/2}+1, N\right)$ è un fattore non banale di N.

Un esempio che illustra l'uso di questo algoritmo con la subroutine di ricerca dell'ordine quantistico è mostrato nel Riquadro 5.4



Fattorizzazione di $N = 15$.

Prima di tutto scegliamo un numero che non ha fattori in comune con N; supponiamo di scegliere $x = 7$.

Poi calcoliamo l'ordine r di x rispetto a N usando l'algoritmo di order-finding: iniziamo con lo stato $|0\rangle|0\rangle$. Applichiamo la trasformata di Hadamard ai t qubits del primo registro ($t = 11$ garantisce una probabilità di errore ϵ di almeno $1/4$) :

$$\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle|0\rangle = \frac{1}{\sqrt{2^t}} \left[|0\rangle + |1\rangle + |2\rangle + \cdots + \left|2^t - 1\right\rangle\right] |0\rangle \qquad (1)$$

Successivamente si calcoli $f(k) = x^k \bmod N$ lasciando il risultato nel secondo registro:

$$\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle \left|x^k \bmod N\right\rangle \qquad (2)$$

$$= \frac{1}{\sqrt{2^t}} [|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + |6\rangle|4\rangle + \ldots] \qquad (3)$$

Fattorizzazione

Si applichi adesso la trasformata di Fouriere inversa $QFT^\dagger$ al primo registro e lo si misuri.

Si misuri il secondo registro, ottenendo un risultato qualunque tra $7, 4$, or 13. Supponiamo sia stato misurato 4 questo significa che $QFT^\dagger$ sarebbe stata $\sqrt{\frac{4}{2^t}}[|2\rangle + |6\rangle + |10\rangle + |14\rangle + \cdots]$.

Dopo aver applicato $QFT^\dagger$ otteniamo alcuni stati $\sum_\ell \alpha_\ell |\ell\rangle$, con una distribuzione di probabilità mostrata per $2^t = 2048$.