Algoritmi randomizzati

> **Note**
>
> Gli algoritmi randomizzati sono algoritmi che effettuano decisioni randomiche durante la loro esecuzione. In pratica un algoritmo randomizzato userà valori generati randomicamente per decidere il cosa fare al prossimo step.

Gli algoritmi randomizzati sono più rapidi dei soliti algoritmi deterministici e anche più facili da implementare. Tutto questo però ha un costo: la risposta può avere la probabilità di essere incorretta.

Applicazione: verificare l'identità di polinomi

Supponiamo di avere due polinomi, $F(x)$ e $G(x)$, dove $F(x)$ è dato come prodotto di fattori e $G(x)$ è dato in forma canonica:

$$[F(x)]: \ (x+1)(x-2)(x+3)(x-4)(x+5)(x-6) \equiv [G(x)]: \ x^6 - 7x^3 + 25$$

Una soluzione banale è quella di portare $F(x)$ in forma canonica e verificare che i coefficienti delle forme canoniche siano uguali. Però questa soluzione ha un problema, ovvero, se notiamo con d il massimo grado del polinomio, allora, per trasformare $F(x)$ nella sua forma canonica impieghiamo $\theta(d^2)$.

Proviamo adesso ad aggiungere un pò di randomness. L'algoritmo ora sceglie un intero r in modo randomico da un intervallo $\{1, \dots, d100\}$, con distribuzione uniforme, ovvero ogni intero ha probabilità equa di essere scelto. Dopodiché l'algortimo computa $F(r)$ e $G(r)$ in tempo $O(d)$, che è decisamente minore rispetto a $\theta(d^2)$. Infine l'algoritmo decide che $F(x) \equiv G(x)$ se $F(r) = G(x)$ oppure $F(x) \not\equiv G(x)$ se $F(r) \neq G(x)$.

Può però succedere che l'algoritmo dia una risposta sbagliata, analizziamo ora i due casi:

- Se $F(x) \equiv G(x)$ allora l'algoritmo ritorna la risposta corretta per ogni r.
- Se $F(x) \equiv G(x)$ e $F(r) \neq G(r)$ allora l'algoritmo ritorna una risposta corretta. Dunque quando l'algoritmo decide che due polinomi sono diversi possiamo essere sicuri che la risposta è sempre corretta.

- Se $F(x) \equiv G(x)$ e $F(r) = G(r)$ allora l' algoritmo ritorna una risposta sbagliata, in altre parole è possibile che l'algortimo decida che due polinomi siano uguali quando in realtà sono divesi. Questo può accadere quando il valore di r corrisponde ad una delle d radici (per il teorema fondamentale dell'algebra, un polinomio di grado d ha al più "d" radici) dell'equazione $F(x) - G(x) = 0$.

Ora però ci resta che analizzare la probabilità di errore dell'algoritmo. Sapendo che $r \in \{1, 2, \ldots, 100d\}$ allora $Pr[err] \leq \frac{d}{100d} \leq \frac{1}{100}$, dunque la probabilità di errore è al piu 1%.