Test di Miller-Rabin

Dato N intero dispari di n cifre,

- troviamo la massima potenza di 2 che divide $N-1$: $N-1 = 2^w z$ con z dispari ($\mathrm{O}(\log N)$)
- scegliamo un testimone $2 \leq y \leq N-1$
- se N è primo vale:
  - $(N, y) = 1$;
  - $y^z \equiv 1 \mod N \vee \exists i \in \{0, \ldots, w-1\} \,.\, y^{2^i z} \mod N = -1$.

Se almeno un predicato è falso, N è composto, altrimenti iterando k volte scegliendo y in modo casuale e indipendente, se i predicati sono sempre veri è possibile affermare che N è primo con probabilità di errore $\left(\frac{1}{4}\right)^k$.

Una buona scelta per k è 30.

Algoritmo

VERIFICA(N, y)

```
1  if not P_1 or not P_2
2        return 1
3  else return 0
```

TESTMR(N, k)

```
1  for i = 1 to k
2        y = RANDOM(2, N − 1)
3        if VERIFICA(N, y) == 1
4              return 0
5  return 1
```

Lemma di Miller-Rabin

Se N è composto, il numero di interi y compresi tra 2 e $N-1$ che soddisfano entrambe le condizioni è minore di $N/4$. La probabilità di scegliere un testimone y che rende veri entrambi i predicati è $< \frac{N/4}{N-2} < \frac{1}{4}$

Complessità

- w e z si trovano con al più n divisioni per 2: $O(n)$;
- P_1: $O(n^3)$ con algoritmo di Euclide;
- P_2: $z \leq \frac{N-1}{2} = \Theta(N)$ (= quando $w = 1$)
  - valutazione di $y^z \mod N$ con QS: $\mathrm{O}(\log^3 z) = \mathrm{O}(n^3)$;
  - polinomiale elevando al quadrato:

    $$y^z \bmod N \to y^{2z} \bmod N \to y^{4z} \bmod N \to \ldots$$

    al più w volte ($0 \leq i \leq w-1$), e $w = \mathrm{O}(n)$.

Quindi il costo complessivo è $O(kn^3)$, che fissato k è polinomiale.