# 8 Test di Primalità

Nella costruzione del crittosistema RSA è necessario generare due numeri primi 'casuali'.

Nella pratica si generano interi dispari casuali e si testa la loro primalità attraverso gli algoritmi di **Soloway-Strassen** e **Miller-Rabin**. Entrambi, come vedremo, sono algoritmi Montecarlo randomizzati il cui tempo di esecuzione è polinomiale.

Per comprendere siffatti test è necessario introdurre ulteriori nozioni di Teoria dei Numeri. Ricordiamo i seguenti risultati:

1. Per ogni $p^m$, $p$ primo, $m \in \mathbb{N}$, esiste, a meno di un isomorfismo, un unico campo finito $GF(p^m)$ di ordine $p^m$. (Esso si ottiene come campo di spezzamento del polinomio $X^{p^m} - X \in \mathbb{Z}_p[X]$);
2. Per il **Teorema di Cauchy** $GF(p^m)^*$, l'insieme degli elementi non nulli di $GF(p^m)$, è un gruppo ciclico di ordine $p^m - 1$;
3. Il numero dei generatori di $GF(p^m)^*$ è $\varphi(p^m - 1)$;
4. I sottocampi di $GF(p^m)$ sono tutti e soli i campi $GF(p^i)$ con $i \mid m$.

**Definizione 8.1.** **(Radice $n$-esima dell'unità)**
Un elemento $x$ di $GF(q)^*$, $q = p^m$, si dice **radice $n$-esima dell'unità**, se $x^n = 1$. Se, inoltre, le radici $n$-esime dell'unità sono tutte e sole le potenze di $x$, allora $x$ si dice **radice $n$-esima primitiva dell'unità**.

**Proposizione 8.2.** Valgono i seguenti risultati:

- **(1)** Sia $g$ un generatore di $GF(q)^*$, allora $g^j$ è una radice $n$-esima dell'unità se e solo se $nj \equiv_{q-1} 0$;
- **(2)** Il numero delle radici $n$-esime dell'unità è $gcd(n, q-1)$;
- **(3)** $GF(q)$ ha radici $n$-esime primitive dell'unità se e solo se $n \mid q-1$;
- **(4)** Se $x_0$ è una radice $n$-esima primitiva dell'unità in $GF(q)$, allora $x_0^j$ è una radice $n$-esima primitiva dell'unità se e solo se $gcd(j, n) = 1$.

**Dimostrazione.**

**(1)** Sia $g$ un generatore di $GF(q)^*$. Allora $o(g) = q-1$, e quindi $g^j$ è una radice $n$-esima dell'unità se e solo se $g^{jn} = 1$, cioè $q-1 \mid nj$ e quindi l'asserto **(1)** è dimostrato.

**(2)-(3)** Il numero delle radici $n$-esime dell'unità è uguale al numero degli $j$ compresi tra 1 e $q-1$ tali che $(q-1) \mid nj$. Posto $d = gcd(n, q-1)$, si ha $\frac{q-1}{d} \mid \frac{n}{d} j$ e poiché $gcd\left(\frac{q-1}{d}, \frac{n}{d}\right) = 1$, risulta: $\frac{q-1}{d} \mid j$. Quindi le radici $n$-esime dell'unità sono tutti e soli gli elementi della forma $g^{\frac{q-1}{d}k}$ con $k = 1, \ldots, d$ che sono appunto $d$. Osserviamo inoltre che tali radici sono $n$ se e solo se $d = n$, i.e. se $n \mid q-1$. Pertanto valgono gli asserti **(2)** e **(3)**.

**(4)** Infine, sia $x_0$ radice $n$-esima primitiva dell'unità, allora $\mathcal{R} = \left\{x_0^i : i = 1, \ldots, n\right\}$ rappresenta l'insieme di tutte le radici $n$-esime dell'unità. $\mathcal{R}$ è il sottogruppo di $GF(q)^*$ di ordine $n$. Allora $x_0^j$ è una radice $n$-esima primitiva dell'unità se e solo se $x_0^j$ è un generatore di $\mathcal{R}$ e ciò si verifica se e solo se $gcd(j, n) = 1$. Abbiamo così provato l'asserto **(4)**.

□

Sia $p$ un primo dispari e sia $a \in GF(p)^*$. Allora $a$ è un quadrato in $GF(p)$ se e solo se esiste $b$ in $GF(p)$ tale che $a = b^2$. In tal caso, $a$ ha precisamente due radici quadrate: $\pm b$. Pertanto i quadrati in $GF(p)^*$ possono essere trovati calcolando $b^2 \ mod \ p$ per $b = 1, 2, 3, \ldots, \frac{(p-1)}{2}$ (poiché i restanti interi fino a $p-1$ sono tutti congrui a $-b$ per ciascuno di tali $b$), e precisamente la metà degli elementi in $GF(p)^*$ sono quadrati.

**Definizione 8.3.** **(Residui Quadratici modulo $p$)**
I quadrati in $GF(p)$ sono detti **residui quadratici modulo $p$**. I restanti elementi non nulli sono detti **residui non quadratici**.

**Esempio 8.4.** In $GF(11)$ ci sono 5 residui quadrati che sono: $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 5$ e $5^2 = 3$, e 5 non quadrati che sono: $2, 6, 7, 8, 10$.

Poiché il prodotto di due quadrati in $GF(p)^*$ e l'inverso di un quadrato in $GF(p)^*$ sono ancora dei quadrati, allora l'insieme $Q$ dei quadrati di $GF(p)^*$ è un sottogruppo di $GF(p)^*$.

L'applicazione

$$\alpha : \ GF(p)^* \longrightarrow Q, \quad x \longmapsto x^2$$

è un omomorfismo suriettivo di gruppi e quindi $\frac{GF(p)^*}{ker\alpha} \cong Q$, dove $\ker \alpha$ è il sottogruppo di $GF(p)^*$ costituito dalle radici quadrate di 1. Poiché $\ker \alpha = \{\pm 1\}$, essendo $p$ dispari, si ha $|Q| = \frac{p-1}{2}$.

E' facile verificare che valgono, inoltre, le seguenti proprietà:

1. il prodotto di due quadrati o di due non quadrati è un quadrato in $GF(p)^*$;
2. il prodotto di un quadrato e di un non quadrato è un non quadrato in $GF(p)^*$.

**Proposizione 8.5.** $-1$ è un quadrato in $GF(p)$ se e solo se $p \equiv_4 1$.

**Dimostrazione.** $-1$ è un quadrato in $GF(p)$ se e solo se $x^2 = -1$, i.e. $x^4 = 1$, cioè se e solo se $GF(p)$ ammette radici quarte primitive dell'unità. Per la **Proposizione 8.2 (3)**, ciò si verifica solo se $p \equiv_4 1$.

□

**Definizione 8.6.** **(Simbolo di Legendre)**
Siano $p$ un primo dispari ed $a$ un intero, allora:

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{se } p \mid a \\ 1 & \text{se } a \text{ è un residuo quadratico in } GF(p) \\ -1 & \text{se } a \text{ è un residuo non quadratico in } GF(p) \end{cases}$$

$\left(\frac{a}{p}\right)$ è detto **Simbolo di Legendre**.

**Teorema 8.7.** ***(Teorema di Eulero)***
*Per il Simbolo di Legendre vale la seguente relazione:*

$$\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}}$$

**Dimostrazione.** Se $p$ divide $a$, l'asserto segue banalmente.
Quindi supponiamo $(a,p) = 1$. Per il **Piccolo Teorema di Fermat** segue che $a^{p-1} \equiv_p 1$ e quindi $a^{\frac{p-1}{2}} \equiv_p \pm 1$, essendo $p$ dispari. Sia $g$ un generatore di $GF(p)^*$. Allora esiste un intero $j$ tale che $a \equiv_p g^j$. Pertanto $a^{\frac{p-1}{2}} \equiv_p g^{j\frac{p-1}{2}}$. Osserviamo che $a^{\frac{p-1}{2}} \equiv_p g^{j\frac{p-1}{2}} \equiv_p 1$ se e solo se $p-1$ divide $j\frac{p-1}{2}$. Ciò si verifica se e solo se $j$ è pari e quindi se e solo se $a$ è un residuo quadratico in $GF(p)$, i.e. $\left(\frac{a}{p}\right) = 1$.

□

**Proposizione 8.8.** Il Simbolo di Legendre soddisfa le seguenti proprietà:

**(1)** Se $a_0 \equiv_p a$, allora $\left(\frac{a}{p}\right) = \left(\frac{a_0}{p}\right)$;

**(2)** $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

**(3)** Se $(b,p) = 1$, allora $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$;

**(4)** $\left(\frac{1}{p}\right) = 1$ e $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

**Dimostrazione.**

**(1)** L'asserto **(1)** segue dalla definizione.

**(2)** Dal **Teorema 8.7** si ha

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv_p \left(\frac{ab}{p}\right)$$

e quindi $p$ divide $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right)$. Inoltre $p$ è dispari e poiché

$$\left|\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right)\right| \leq 2,$$

vale l'asserto **(2)**.

**(3)** L'asserto **(3)** segue da **(2)**.

**(4)** Infine, poiché risulta $\left|\left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}}\right| \leq 2$, con $\left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}}$ divisibile per $p$ per il **Teorema 8.7**, vale l'asserto **(4)**.

□

**Lemma 8.9.** *Siano $n \in \mathbb{N}$ e*

$$f(n) = \begin{cases} (-1)^{\frac{n^2-1}{8}} & \text{se } n \text{ è dispari} \\ 0 & \text{se } n \text{ è pari} \end{cases}$$

*allora $f(n_1n_2) = f(n_1)f(n_2)$ per ogni $n_1, n_2 \in \mathbb{N}$.*

**Dimostrazione.** Siano $n_1, n_2 \in \mathbb{N}$. Se almeno uno tra $n_1$ ed $n_2$ è pari, l'asserto segue banalmente. Quindi si supponga che $n_1$ e $n_2$ siano entrambi dispari. Allora

$$\begin{aligned} f(n_1n_2) &= (-1)^{\frac{(n_1n_2)^2-1}{8}} = (-1)^{\frac{n_1^2n_2^2-n_1^2+n_1^2-1}{8}} = (-1)^{\frac{n_1^2(n_2^2-1)+n_1^2-1}{8}} \\ &= (-1)^{\frac{n_1^2-1}{8}}(-1)^{n_1^2\frac{n_2^2-1}{8}} = (-1)^{\frac{n_1^2-1}{8}}(-1)^{\frac{n_2^2-1}{8}} = f(n_1)f(n_2). \end{aligned}$$

□

**Proposizione 8.10.** Sia $p$ un primo dispari. Allora:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{se } p \equiv_8 \pm 1 \\ -1 & \text{se } p \equiv_8 \pm 3 \end{cases}$$

**Dimostrazione.** Poiché $p$ è dispari, allora $8 \mid p^2 - 1$ e $GF(p^2)$ ammette radici ottave primitive dell'unità per la **Proposizione 8.2 (3)**. Sia $\xi$ una di esse. Si definisca

$$H = \sum_{j=0}^{7} f(j)\xi^j,$$

dove $f(j) = (-1)^{\frac{j^2-1}{8}}$ se $j$ è dispari e 0 altrimenti. Allora $H = \xi - \xi^3 - \xi^5 + \xi^7$. Siccome $\xi^4 = -1$, allora risulta $\xi^5 = -\xi$, $\xi^7 = -\xi^3$ e quindi $H = 2(\xi - \xi^3)$ e $H^2 = 4(\xi^2 - 2\xi^4 + \xi^6) = 8$. In particolare, $H \neq 0$. Dal **Teorema 8.7** e dalla **Proposizione 8.8 (3)**, tenendo presente che $p$ è dispari, segue

$$H^p = (H^2)^{\frac{p-1}{2}} H = 8^{\frac{p-1}{2}} H = \left(\frac{8}{p}\right) H = \left(\frac{2}{p}\right) H. \tag{8.1}$$

Per il **Lemma 8.9**, vale che $f(j) = f(p)^2 f(j) = f(p)f(pj)$ e quindi

$$\begin{aligned} H^p &= \sum_{j=0}^{7} f(j)^p \xi^{jp} = \sum_{j=0}^{7} f(j)\xi^{jp} = \sum_{j=0}^{7} f(p)f(pj)\xi^{jp} \\ &= f(p) \sum_{j=0}^{7} f(pj)\xi^{jp}. \end{aligned}$$

L'insieme $\{jp \ : \ j = 0, \ldots, 7\}$ è un sistema completo di residui *mod* 8. Quindi per ogni $j = 0, \ldots, 7$ esiste un unico $j' = 0, \ldots, 7$ t.c. $jp \equiv_8 j'$. Pertanto $jp = j' + 8k$, con $k$ intero. Allora $\xi^{jp} = \xi^{j'}\xi^{8k}$ e quindi $\xi^{jp} = \xi^{j'}$, essendo $\xi$ una radice ottava dell'unità.

Inoltre vale che

$$f(jp) = f(j').$$

Infatti, $j$ e $j'$ appartengono alla stessa classe di parità, quindi $f(jp) = 0 = f(j')$ se $j'$ è pari. Se $j'$ è dispari, vale che

$$\begin{aligned} f(jp) = f(j' + 8k) &= (-1)^{\frac{(j'+8k)^2-1}{8}} = (-1)^{\frac{j'^2+16j'k+64k^2-1}{8}} = \\ &= (-1)^{\frac{j'^2-1}{8}} (-1)^{\frac{16j'k+64k^2}{8}} = f(j'). \end{aligned}$$

Pertanto, si ha che

$$H^p = f(p) \sum_{j=0}^{7} f(pj)\xi^{jp} = f(p) \sum_{j'=0}^{7} f(j')\xi^{j'} = f(p)H = (-1)^{\frac{p^2-1}{8}} H. \tag{8.2}$$

Ora uguagliando (8.1) e (8.2) e tenendo presente che $H \neq 0$, si ottiene l'asserto.

□

**Definizione 8.11.** **(Somma Gaussiana)**
Se $p, q$ sono due primi dispari distinti tali che $\xi \in GF(p^f)$ è una radice $q$-esima primitiva dell'unità, allora

$$G = \sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \xi^j$$

si dice **somma Gaussiana**.

Si noti che i primi della **Definizione 8.11** esistono. Infatti se $f$ è un multiplo di $q-1$, allora $p^f \equiv_q 1$ per il **Piccolo Teorema di Fermat** e quindi le radici $q$–esime primitive dell'unità esistono per la **Proposizione 8.2 (3)**.

**Lemma 8.12.**

$$G^2 = (-1)^{\frac{q-1}{2}} q.$$

**Dimostrazione.** Poiché $\{-k : k = 0, \ldots, q-1\}$ è un sistema completo di residui modulo $q$, vale che per ogni $j = 0, \ldots, q-1$ esiste un unico $k = 0, \ldots, q-1$ tale che $j = -k + \vartheta q$, con $\vartheta \in \mathbb{Z}$. Allora $\left(\frac{j}{q}\right) = \left(\frac{-k}{q}\right)$ per la **Proposizione 8.8 (1)** e $\xi^j = \xi^{-k} \left(\xi^q\right)^\vartheta = \xi^{-k}$ essendo $\xi$ una radice $q$–esima dell'unità. Quindi si ha che:

$$G = \sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \xi^j = \sum_{k=0}^{q-1} \left(\frac{-k}{q}\right) \xi^{-k}.$$

Poiché $\left(\frac{0}{q}\right) = 0$, allora

$$\begin{aligned} G^2 &= \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \xi^j \sum_{k=1}^{q-1} \left(\frac{-k}{q}\right) \xi^{-k} \underset{\text{Prop. } 8(2)}{=} \\ &= \left(\frac{-1}{q}\right) \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \xi^j \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \xi^{-k}. \end{aligned}$$

Per un qualsiasi $j$ fissato, l'insieme $\{jh : h = 0, \ldots, q-1\}$ è ancora un sistema completo di residui modulo $q$. Quindi per ogni $k = 0, \ldots, q-1$ esiste un unico $h \in \{0, \ldots, q-1\}$ tale che $k = jh + aq$, con $a \in \mathbb{Z}$. Allora, ragionando come sopra, valgono $\left(\frac{k}{q}\right) = \left(\frac{jh}{q}\right)$ e $\xi^{-k} = \xi^{-jh}$ e quindi

$$\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \xi^{-k} = \sum_{h=1}^{q-1} \left(\frac{jh}{q}\right) \xi^{-jh}.$$

Quindi

$$\begin{aligned} G^2 &= (-1)^{\frac{q-1}{2}} \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \xi^j \sum_{h=1}^{q-1} \left(\frac{jh}{q}\right) \xi^{-jh} \\ &= (-1)^{\frac{q-1}{2}} \sum_{j=1}^{q-1} \sum_{h=1}^{q-1} \left(\frac{j^2 h}{q}\right) \xi^{j(1-h)} \\ &= (-1)^{\frac{q-1}{2}} \sum_{j=1}^{q-1} \sum_{h=1}^{q-1} \left(\frac{h}{q}\right) \xi^{j(1-h)}. \end{aligned} \tag{8.3}$$

Siccome i quadrati e i non quadrati di $GF(q)^*$ sono in egual numero pari a $\frac{q-1}{2}$, vale che $\sum_{k=1}^{q-1}\left(\frac{k}{q}\right) = 0$ e quindi non si altera la somma (8.3) se si aggiunge il termine relativo a $j = 0$. Pertanto segue che:

$$G^2 = (-1)^{\frac{q-1}{2}} \sum_{j=0}^{q-1}\sum_{k=1}^{q-1}\left(\frac{k}{q}\right)\xi^{j(1-k)} = (-1)^{\frac{q-1}{2}} \sum_{k=1}^{q-1}\left(\frac{k}{q}\right)\sum_{j=0}^{q-1}\xi^{j(1-k)}. \tag{8.4}$$

Se $k \neq 1$, si ha:

$$\sum_{j=0}^{q-1}\xi^{j(1-k)} = (\xi^{q(1-k)} - 1)(\xi^{(1-k)} - 1)^{-1} = 0$$

e in (8.4) resta solo l'addendo relativo a $k = 1$. Così $G^2 = (-1)^{\frac{q-1}{2}}\, q$.

□

**Teorema 8.13.** ***(Legge di Reciprocità Quadratica)***
*Se $p, q$ sono due primi dispari, allora*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{se } p, q \equiv_4 3, \\ \left(\frac{p}{q}\right) & \text{altrimenti.} \end{cases}$$

**Dimostrazione.** Sia $f$ un qualsiasi intero positivo tale che $q \mid p^f - 1$. Per la nota relativa alla **Definizione 8.11**, tali $f$ esistono. Allora ha senso considerare la somma Gaussiana in $GF(p^f)$

$$G = \sum_{j=0}^{q-1}\left(\frac{j}{q}\right)\xi^j.$$

Dal **Lemma 8.12** e dal **Teorema 8.7**, tenendo presente che le congruenze modulo $p$ sono uguaglianze in $GF(p)$ e quindi in $GF(p^f)$, segue che:

$$G^p = (G^2)^{\frac{p-1}{2}} G = (-1)^{\frac{(p-1)(q-1)}{4}} q^{\frac{p-1}{2}} G = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right) G.$$

D'altra parte

$$\begin{aligned} G^p &= \sum_{j=0}^{q-1}\left(\frac{j}{q}\right)^p \xi^{jp} = \sum_{j=0}^{q-1}\left(\frac{j}{q}\right)\xi^{jp} = \\ &= \sum_{j=0}^{q-1}\left(\frac{p}{q}\right)\left(\frac{jp}{q}\right)\xi^{jp} = \left(\frac{p}{q}\right)\sum_{j=0}^{q-1}\left(\frac{jp}{q}\right)\xi^{jp} \end{aligned}$$

per la **Proposizione 8.8 (2)-(3)**. Poiché l'insieme $\{jp : j = 0, \ldots, q-1\}$ è un sistema completo di residui modulo $q$, allora per ogni $j = 0, \ldots, q-1$ esiste un unico $j' = 0, \ldots, q-1$ tale che valgono $\left(\frac{jp}{q}\right) = \left(\frac{j'}{q}\right)$ e $\xi^{jp} = \xi^{j'}$.

Pertanto si ha $\sum_{j=0}^{q-1}\left(\frac{jp}{q}\right)\xi^{jp} = \sum_{j'=0}^{q-1}\left(\frac{j'}{q}\right)\xi^{j'} = G$ e quindi

$$(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)G = G^p = \left(\frac{p}{q}\right)G. \tag{8.5}$$

Poiché per il **Lemma 8.12** risulta $G \neq 0$, possiamo dividere per $G$ in (8.5) ottenendo così la tesi.

□

**Esempio 8.14.** Dati i primi 7411 e 9283, stabiliamo se 7411 è un residuo quadratico in $GF(9283)$.

Poiché 7411 e 9283 sono entrambi congrui a 3 *mod* 4, allora vale che

$$\left(\frac{7411}{9283}\right) = -\left(\frac{9283}{7411}\right).$$

Risulta:

$$\begin{aligned}\left(\frac{7411}{9283}\right) &= -\left(\frac{9283}{7411}\right) = -\left(\frac{1872}{7411}\right) = -\left(\frac{2^4\cdot 3^2\cdot 13}{7411}\right) = \\ &= -\left(\frac{2^4}{7411}\right)\left(\frac{3^2}{7411}\right)\left(\frac{13}{7411}\right) = -\left(\frac{13}{7411}\right) = \\ &= -\left(\frac{7411}{13}\right) = -\left(\frac{1}{13}\right) = -1\end{aligned}$$

□

**Definizione 8.15.** **(Simbolo di Jacobi)**
Siano $a$ un intero e $n$ un intero positivo dispari. Se $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, $p_i \in \mathbb{P}$ e $\alpha_i \in \mathbb{N}$, allora si definisce **Simbolo di Jacobi** $\left(\frac{a}{n}\right)$ il prodotto dei Simboli di Legendre dei fattori primi di $n$:

$$\left(\frac{a}{n}\right) := \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{\alpha_i}.$$

**Remark 8.16.** Si noti che $\left(\frac{a}{n}\right) = 1$, con $n$ composto, non implica che $a$ è un quadrato modulo $n$. Per esempio $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, mentre non esiste un intero $x$ tale che $x^2 \equiv_{15} 2$. Infatti, $x^2 \equiv_{15} 2$ implica $x^2 \equiv_3 2$, mentre 2 è un non quadrato in $GF(3)$.

**Proposizione 8.17.** Siano $a, b, n$ interi, con $n$ dispari. Valgono le seguenti proprietà:

**(1)** $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$;

**(2)** Se $a \equiv_n b$, allora $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

**Dimostrazione.** Sia $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ con $p_i$ primo.

**(1)** Dalla definizione di Simbolo di Jacobi e dalla **Proposizione 8.8 (2)**, segue:

$$\left(\frac{ab}{n}\right) = \prod_{i=1}^{k}\left(\frac{ab}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{\alpha_i}\left(\frac{b}{p_i}\right)^{\alpha_i} = \left[\prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{\alpha_i}\right]\left[\prod_{i=1}^{k}\left(\frac{b}{p_i}\right)^{\alpha_i}\right] = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

quindi vale l'asserto **(1)**.

**(2)** Se $a \equiv_n b$, allora $a \equiv_{p_i} b$ per ogni primo $i = 1, \cdots, k$, e quindi dalla **Proposizione 8.8(1)** segue che

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{k}\left(\frac{b}{p_i}\right)^{\alpha_i} = \left(\frac{b}{n}\right).$$

Pertanto vale l'asserto **(2)**.

□

**Proposizione 8.18.** Per ogni $n \in \mathbb{N}$, $n$ dispari, vale che:

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

**Dimostrazione.** Se $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, $p_i$ primo, allora dalla **Proposizione 8.10** e dal **Lemma 8.9** segue:

$$\begin{aligned}\left(\frac{2}{n}\right) &= \prod_{i=1}^{k}\left(\frac{2}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{k}\left((-1)^{\frac{p_i^2-1}{8}}\right)^{\alpha_i} = \prod_{i=1}^{k} f(p_i)^{\alpha_i} \\ &= \prod_{i=1}^{k} f(p_i^{\alpha_i}) = f\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = f(n) = (-1)^{\frac{n^2-1}{8}}.\end{aligned}$$

□

**Proposizione 8.19.** Per ogni $n, m \in \mathbb{N}$, $n, m$ dispari, vale che:

$$\left(\frac{m}{n}\right) = (-1)^{\frac{(n-1)(m-1)}{4}} \left(\frac{n}{m}\right).$$

**Dimostrazione.** Supponiamo che $n = \prod_{i=1}^{k} p_i$ e $m = \prod_{j=1}^{h} q_j$, con $p_i, q_j$ primi. Se $(n, m) > 1$, dalla definizione di Simbolo di Jacobi, si ha $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) = 0$.
Se $(n, m) = 1$, allora per la **Proposizione 8.17** si ha

$$\left(\frac{m}{n}\right) = \prod_{j=1}^{h} \left(\frac{q_j}{n}\right) = \prod_{i,j=1}^{k,h} \left(\frac{q_j}{p_i}\right).$$

Ora, applicando $kh$ volte la **Legge di Reciprocità** quadratica si ha:

$$\begin{aligned}
\left(\frac{m}{n}\right) &= \prod_{j=1}^{k} \left(\frac{q_j}{n}\right) = \prod_{i,j=1}^{k,h} \left(\frac{q_j}{p_i}\right) = \prod_{i,j=1}^{k,h} (-1)^{\frac{(p_i-1)(q_j-1)}{4}} \left(\frac{p_i}{q_j}\right) = \\
&= \left(\prod_{i,j=1}^{k,h} (-1)^{\frac{(p_i-1)(q_j-1)}{4}}\right) \prod_{i,j=1}^{k,h} \left(\frac{p_i}{q_j}\right) = \\
&= \left(\prod_{i,j=1}^{k,h} (-1)^{\frac{(p_i-1)(q_j-1)}{4}}\right) \left(\frac{n}{m}\right).
\end{aligned}$$

Notiamo che $(-1)^{\frac{(p_i-1)(q_j-1)}{4}} = -1$ se e solo se $p_i \equiv_4 3$ e $q_j \equiv_4 3$. Ora, se $0 \leq k_0 \leq k$ e $0 \leq h_0 \leq h$ rappresentano il numero dei fattori primi di $n$ ed $m$ rispettivamente, eventualmente ripetuti, congrui a 3 modulo 4, allora $n \equiv_4 3^{k_0}$, $m \equiv_4 3^{h_0}$ e

$$\prod_{i,j=1}^{k,h} (-1)^{\frac{(p_i-1)(q_j-1)}{4}} = (-1)^{k_0 h_0}.$$

Osserviamo che $(-1)^{k_0 h_0} = -1$ se e solo se $k_0$ e $h_0$ sono entrambi dispari. Cioè se $n \equiv_4 3$ e $m \equiv_4 3$ e quindi $(-1)^{\frac{(n-1)(m-1)}{4}} = -1$. Ciò completa la dimostrazione.

□

**Esempio 8.20.** Calcoliamo $\left(\frac{7411}{9283}\right)$ utilizzando il Simbolo di Jacobi.

Per la **Proposizione 8.19** segue che $\left(\frac{7411}{9283}\right) = -\left(\frac{9283}{7411}\right) = -\left(\frac{1872}{7411}\right)$. Osserviamo che, a questo punto, nell'**Esempio 8.14**, era necessario fattorizzare il numero 1872 per poter utilizzare il simbolo di Legendre. In questo caso, invece, possiamo evitare tale fattorizzazione, infatti:

$$\begin{aligned}
-\left(\frac{1872}{7411}\right) &= -\left(\frac{7411}{1872}\right) = -\left(\frac{1795}{1872}\right) = -\left(\frac{1872}{1795}\right) = -\left(\frac{77}{1795}\right) = -\left(\frac{1795}{77}\right) = -\left(\frac{24}{77}\right) = \\
&= -\left(\frac{2^3 \cdot 3}{77}\right) = -\left(\frac{2^3}{77}\right)\left(\frac{3}{77}\right) = -\left(\frac{2}{77}\right)\left(\frac{3}{77}\right) = \left(\frac{3}{77}\right) = \left(\frac{77}{3}\right) = \left(\frac{2}{3}\right) = -1.
\end{aligned}$$

□

## 8.1 Pseudoprimi

**Definizione 8.21.** **(Pseudoprimo)**
Siano $n$ un intero composto dispari e $b$ un intero tale che $gcd(b, n) = 1$. Se

$$b^{n-1} \equiv_n 1,$$

allora $n$ si dice **pseudoprimo** rispetto alla base $b$.

**Esempio 8.22.** L'intero $n = 91 = 7 \cdot 13$ é uno pseudoprimo rispetto alla base $b = 3$ ma non rispetto alla base $b = 2$. Infatti $3^{90} \equiv_{91} 1$ mentre $2^{90} \equiv_{91} 64$.

Si noti che se $b$ é una base per $n$, allora é base per $n$ ogni intero appartenente alla classe di resto modulo $n$ individuata da $b$.

Poiché ogni classe di resto modulo $n$ ha un unico rappresentante compreso tra 0 ed $n - 1$, nel seguito, a meno che non sia esplicitamente detto il contrario, quando parleremo di basi rispetto ad $n$, faremo riferimento esclusivamente a tali residui modulo $n$.

Si noti inoltre che le basi per $n$ sono $\varphi(n)$ e sono tutti e soli gli elementi invertibili in $\mathbb{Z}_n$ rispetto al prodotto (i.e. $\mathcal{U}(\mathbb{Z}_n)$).

**Definizione 8.23.** **(Numero di Carmichael)**
Un intero composto dispari che é pseudoprimo rispetto a tutte le basi, si dice **numero di Carmichael**.

**Proposizione 8.24.** Valgono le seguenti proprietà:

1. Sia $n$ un intero composto dispari, allora $n$ é un numero di Carmichael se e solo se per ogni primo $p$ divisore di $n$ vale che $p^2 \nmid n$ ma $p-1 \mid n-1$.
2. Un numero di Carmichael é prodotto di almeno tre primi distinti e il più piccolo numero di Carmichael é 561.
3. I numeri di Carmichael sono infiniti (Teorema di *Alford, Granville, Pomerance*, 1994).

### 8.1.1 Pseudoprimi di Eulero

**Definizione 8.25.** **(Pseudoprimo di Eulero)**
Siano $n$ un intero composto dispari e $b$ un intero tale che $gcd(n,b) = 1$. Allora $n$ si dice **pseudoprimo di Eulero** rispetto alla base $b$ se vale

$$b^{\frac{n-1}{2}} \equiv_n \left(\frac{b}{n}\right), \tag{8.6}$$

dove $\left(\frac{b}{n}\right)$ è il simbolo di Jacobi.

Si noti che ogni primo dispari soddisfa (8.6) in virtù del **Teorema 8.7**.

**Teorema 8.26.** *Sia $n$ un intero composto dispari e sia $Y$ l'insieme delle basi rispetto alle quali $n$ è uno pseudoprimo di Eulero. Allora*

$$|\mathcal{U}(\mathbb{Z}_n) - Y| \geq \frac{1}{2}\varphi(n).$$

**Dimostrazione.** Sia

$$Y = \left\{ b \in \mathcal{U}(\mathbb{Z}_n) : b^{\frac{n-1}{2}} \equiv_n \left(\frac{b}{n}\right) \right\}.$$

Proviamo che $|\mathcal{U}(\mathbb{Z}_n) - Y| > 0$.

Supponiamo che esista una base $b'$ tale che $(b')^{n-1} \not\equiv_n 1$, allora $(b')^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right)$ e quindi $|\mathcal{U}(\mathbb{Z}_n) - Y| > 0$.

Pertanto supponiamo che $b^{n-1} \equiv_n 1$ rispetto a tutte le basi. Allora vale che $gcd(p, n/p) = 1$ per ogni divisore primo $p$ di $n$. Sia $x$ un non quadrato in $GF(p)^*$. Per il **Teorema Cinese dei Resti** esiste $b_0$ tale che $b_0 \equiv_p x$ e $b_0 \equiv_{n/p} 1$.
Quindi $gcd(b_0, n) = 1$ e $(\frac{b_0}{p}) = -1$, $(\frac{b_0}{n/p}) = 1$. Allora $(\frac{b_0}{n}) = -1$. Se vale che $b_0^{\frac{n-1}{2}} \equiv_n -1$, allora $b_0^{\frac{n-1}{2}} \equiv_{n/p} -1$. Ciò è assurdo poiché $b_0 \equiv_{n/p} 1$ e $b_0^{\frac{n-1}{2}} \equiv_{n/p} 1$.

Quindi $b_0 \in \mathcal{U}(\mathbb{Z}_n) - Y$ e $|\mathcal{U}(\mathbb{Z}_n) - Y| > 0$. Proviamo che $|\mathcal{U}(\mathbb{Z}_n) - Y| \geq |Y|$.

Siano $b \in Y$ e $b_0 \in \mathcal{U}(\mathbb{Z}_n) - Y$. Allora $bb_0 \in Y$ oppure $bb_0 \in U(\mathbb{Z}_n) - Y$. Se $bb_0 \in Y$, allora $(bb_0)^{\frac{n-1}{2}} \equiv_n (\frac{bb_0}{n})$, da cui segue $b^{\frac{n-1}{2}} b_0^{\frac{n-1}{2}} \equiv_n (\frac{b}{n})(\frac{b_0}{n})$.

Pertanto $(\frac{b}{n})b_0^{\frac{n-1}{2}} \equiv_n (\frac{b}{n})(\frac{b_0}{n})$, da cui si ricava $b_0^{\frac{n-1}{2}} \equiv_n (\frac{b_0}{n})$ e quindi $b_0 \in Y$ ma ciò è assurdo. Pertanto $bb_0 \in \mathcal{U}(\mathbb{Z}_n) - Y$ per ogni $b \in Y$. Quindi segue che

$$|\mathcal{U}(\mathbb{Z}_n) - Y| \geq |Yb_0| = |Y|.$$

Ora

$$\varphi(n) = |\mathcal{U}(\mathbb{Z}_n)| = |Y| + |\mathcal{U}(\mathbb{Z}_n) - Y| \leq 2\,|\mathcal{U}(\mathbb{Z}_n) - Y|$$

da cui segue

$$|\mathcal{U}(\mathbb{Z}_n) - Y| \geq \frac{1}{2}\varphi(n).$$

□

**Osservazione 8.27.** La probabilità che un intero composto dispari $n$ sia uno pseudoprimo di Eulero rispetto a $k$ basi distinte è al più $\frac{1}{2^k}$.

**Esempio 8.28.** $n = 561 = 3 \times 11 \times 17$ non è uno pseudoprimo di Eulero.

Infatti, per $p = 17$, siccome $\left(\frac{3}{17}\right) = -1$ si consideri il sistema congruenziale

$$\begin{cases} b \equiv_{17} 3 \\ b \equiv_{33} 1 \end{cases}$$

Utilizzando il **Teorema Cinese dei Resti**, la soluzione compresa tra 0 e 560 è $b = 496$. Allora

$$\left(\frac{496}{561}\right) = \left(\frac{496}{33}\right)\left(\frac{496}{17}\right) = \left(\frac{1}{33}\right)\left(\frac{3}{17}\right) = -1$$

Se 561 fosse uno pseudoprimo di Eulero rispetto alla base $b = 496$, si dovrebbe avere $496^{280} \equiv_{561} -1$ e quindi $496^{280} \equiv_{33} -1$. Ciò è assurdo, perchè $496 \equiv_{33} 1$ implica $496^{280} \equiv_{33} 1$. Pertanto 561 non è uno pseudoprimo di Eulero rispetto alla base $b = 496$.

□

### 8.1.2 Pseudoprimi Forti

**Definizione 8.29.** **(Pseudoprimo Forte)**
Sia $n$ un intero composto dispari, quindi $n = 2^s t + 1$ con $t$ dispari ed $s \geq 1$, e sia $b$ un intero tale che $gcd(b, n) = 1$. Allora $n$ si dice **pseudoprimo forte rispetto alla base** $b$, se

- $b^t \equiv_n 1$, oppure
- esiste $0 \leq r < s$ tale che $b^{2^r t} \equiv_n -1$.

Osserviamo che nella **Definizione 8.29** viene escluso il caso $r = s$. Infatti, se fosse $r = s$, allora $b^{n-1} \equiv_n -1$. Quindi l'ordine di $b$, in quanto invertibile nelle classi di resto modulo $n$, dovrebbe essere $2(n-1)$. D'altra parte, l'ordine di $b$ divide $\varphi(n)$ e $\varphi(n) < 2(n-1)$.

Ad esempio, sia $n = 65 = 2^6 + 1$.

- Consideriamo $b = 8$. Poiché $gcd(8, 65) = 1$ e $8^2 \equiv_{65} -1$, allora 65 è uno pseudoprimo forte rispetto alla base $b = 8$.
- Se invece consideriamo $b = 14$, osserviamo che, poiché $14^2 \equiv_{65} 1$, allora $14^{2^r} \equiv_{65} 1$ per $1 \leq r < 6$. Pertanto 65 non è uno pseudoprimo forte rispetto alla base $b = 14$.

**Lemma 8.30.** *Sia $n = 2^s t + 1$, $t$ dispari, $s \geq 1$, uno pseudoprimo forte rispetto alla base $b$. Sia $p = 2^{s'} t' + 1$, $t'$ dispari, $s' \geq 1$, un divisore primo di $n$. Se $b^{\frac{n-1}{2}} \equiv_n -1$, allora vale che:*

(1) $s' \geq s$;

(2) $\left(\frac{b}{p}\right) = \begin{cases} -1 \text{ se } s = s' \\ 1 \text{ se } s < s' \end{cases}$

**Dimostrazione.**

(1) Poiché $b^{\frac{n-1}{2}} = b^{2^{s-1}t} \equiv_n -1$ e $t'$ è dispari, si ha $(b^{2^{s-1}t})^{t'} \equiv_n -1$. Pertanto $(b^{2^{s-1}t'})^t \equiv_n -1$. Siccome $p \mid n$, risulta

$$(b^{2^{s-1}t'})^t \equiv_p -1. \tag{8.7}$$

Supponiamo che $s' < s$. Allora

$$\left(b^{2^{s-1}t'}\right)^t = \left(b^{2^{s+s'-s'-1}t'}\right)^t = \left(b^{2^{s'-1}t'}\right)^{2^{s-s'}t}. \tag{8.8}$$

Poiché $b^{2^{s'-1}t'} = b^{\frac{p-1}{2}}$ e $b^{\frac{p-1}{2}} \equiv_p \left(\frac{b}{p}\right)$ per il **Teorema 8.7**, allora $b^{2^{s'-1}t'} \equiv_p \pm 1$. Ne segue che $\left(b^{2^{s'-1}t'}\right)^{2^{s-s'}t} \equiv_p 1$. Quindi, per (8.8), risulta $\left(b^{2^{s-1}t'}\right)^t \equiv_p 1$ ma ciò contraddice (8.7). Pertanto si ha $s' \geq s$.

(2) Se $s' = s$, segue che $b^{2^{s-1}t'} \equiv_p \left(\frac{b}{p}\right)$ per il **Teorema 8.7**. Allora $\left(b^{2^{s-1}t'}\right)^t \equiv_p \left(\frac{b}{p}\right)^t$ e quindi, da (8.7) risulta $\left(\frac{b}{p}\right)^t \equiv_p -1$ da cui segue, in modo banale, che $\left(\frac{b}{p}\right) = -1$, essendo $t$ dispari. Ora supponiamo che $s' > s$. Poiché

$$\left(b^{2^{s'-1}t'}\right)^t = \left(b^{2^{s'+s-s-1}t'}\right)^t = \left(\left(b^{2^{s-1}t'}\right)^t\right)^{2^{s'-s}},$$

da (8.7) segue che $\left(b^{2^{s'-1}t'}\right)^t \equiv_p 1$ cioè $\left(b^{\frac{p-1}{2}}\right)^t \equiv_p 1$. Ora, dal **Teorema 8.7** si ha che $\left(\frac{b}{p}\right)^t \equiv_p 1$ e quindi $\left(\frac{b}{p}\right) = 1$, essendo $t$ dispari.

□

Procedendo in modo analogo al **Lemma 8.30**, si prova il seguente Lemma:

**Lemma 8.31.** *Sia $n = 2^s t + 1$, $t$ dispari, $s \geq 1$, uno pseudoprimo forte rispetto alla base $b$. Sia $p = 2^{s'} t' + 1$, $t'$ dispari, $s' \geq 1$, un divisore primo di $n$. Se esiste $0 \leq r < s - 1$ tale che $b^{2^r t} \equiv_n -1$, allora vale che:*

(1) $s' \geq r$;

(2) $\left(\frac{b}{p}\right) = \begin{cases} -1 & \text{se } r = s' \\ 1 & \text{se } r < s' \end{cases}$

**Proposizione 8.32.** Se $n$ è uno pseudoprimo forte rispetto alla base $b$, allora $n$ è uno pseudoprimo di Eulero rispetto a $b$.

**Dimostrazione.** Sia $n = 2^s t + 1$, $t$ dispari, $s \geq 1$, uno pseudoprimo forte rispetto alla base $b$. Analizziamo le tre seguenti (esaustive) possibiltà:

(1) $b^t \equiv_n 1$;
(2) $b^{2^{s-1}t} \equiv_n -1$ (i.e. $r = s - 1$);
(3) Esiste $0 \leq r < s - 1$ tale che $b^{2^r t} \equiv_n -1$.

(1) Supponiamo che valga (1), allora

$$b^{\frac{n-1}{2}} \equiv_n 1$$

poiché $t$ divide $\frac{n-1}{2}$. D'altra parte,

$$\left(\frac{b}{n}\right)^t = \left(\frac{b^t}{n}\right) = 1$$

per la **Proposizione 8.17 (1)-(2)**. Pertanto, essendo $t$ dispari, $\left(\frac{b}{n}\right) = 1$, e quindi

$$b^{\frac{n-1}{2}} \equiv_n \left(\frac{b}{n}\right),$$

cioè $n$ è uno pseudoprimo di Eulero rispetto a $b$. Quindi, nel caso (1), la tesi è provata.

(2) Ora supponiamo che valga (2). Allora

$$b^{\frac{n-1}{2}} \equiv_n -1.$$

Sia $n = \prod_{p|n} p$. Per il **Lemma 8.30 (1)**, vale che $p = 2^{s'}t' + 1$, $t'$ dispari, $s' \geq s \geq 1$. Per il **Lemma 8.30 (2)**, si ha che

$$\left(\frac{b}{n}\right) = \prod_{p|n}\left(\frac{b}{p}\right) = (-1)^k,$$

dove $k$ è il numero, con ripetizione, dei divisori primi di $n$ per cui valga $s' = s$. Essendo $b^{\frac{n-1}{2}} \equiv_n -1$, per provare l'asserto in questo caso è sufficiente provare che $\left(\frac{b}{n}\right) = -1$, cioè che $k$ è dispari. Se $p = 2^{s'}t'+1$, $t'$ dispari, $s' \geq 1$, è un generico primo divisore di $n$, si ha che:

- Se $s' > s$, allora $p \equiv_{2^{s+1}} 1$;
- Se $s' = s$, allora

$$p = 2^s t' + 1 = 2^s(2h' + 1) + 1 = 2^{s+1}h' + 2^s + 1$$

e quindi $p \equiv_{2^{s+1}} 2^s + 1$.

Ora $n = 2^s t + 1 = 2^s(2h + 1) + 1 = 2^{s+1}h + 2^s + 1$, e quindi

$$n \equiv_{2^{s+1}} 2^s + 1. \tag{8.9}$$

D'altra parte, essendo $n = \prod_{p|n} p$ si ha che

$$n \equiv_{2^{s+1}} (2^s + 1)^k. \tag{8.10}$$

Da (8.9) e (8.10) segue che

$$(2^s + 1)^k \equiv_{2^{s+1}} 2^s + 1. \tag{8.11}$$

Poiché

$$(2^s + 1)^k = \sum_{i=0}^{k}\binom{k}{i}2^{si} \equiv_{2^{s+1}} \binom{k}{0} + \binom{k}{1}2^s,$$

segue che

$$(2^s + 1)^k \equiv_{2^{s+1}} 1 + k2^s.$$

Allora per (8.11) vale

$$1 + 2^s k \equiv_{2^{s+1}} 1 + 2^s.$$

Quindi $2^{s+1}$ divide $2^s(k-1)$. Pertanto $k$ è dispari, e quindi, anche nel caso (2) vale la tesi.

(3) Infine supponiamo che valga (3), allora

$$b^{\frac{n-1}{2}} \equiv_n 1.$$

Sia $n = \prod_{p|n} p$. Allora $n \equiv_{2^{r+1}} 1$. Per il **Lemma 8.31 (1)**, vale che se $p = 2^{s'}t' + 1$, $t'$ dispari, $s' \geq 1$, è un generico primo divisore di $n$, allora risulta $s' \geq r$. Inoltre, dal **Lemma 8.31 (2)** segue che

$$\left(\frac{b}{n}\right) = \prod_{p|n}\left(\frac{b}{p}\right) = (-1)^\theta,$$

dove $\theta$ è il numero, con ripetizione, dei divisori primi di $n$ per cui valga $s' = r$. Essendo $b^{\frac{n-1}{2}} \equiv_n 1$, per provare l'asserto in questo caso, è sufficiente provare che $\left(\frac{b}{n}\right) = 1$, cioè basta provare che $\theta$ è pari. Ragionando in modo analogo al caso precedente si ottiene $p \equiv_{2^{r+1}} 1$ o $p \equiv_{2^{r+1}} 1+2^r$ a seconda che il corrispondente $s'$ sia maggiore o uguale ad $r$, rispettivamente. Quindi $n = \prod_{p|n} p$ è congruente sia a 1 che a $(1+2^r)^\theta$ modulo $2^{r+1}$ e pertanto $(1+2^r)^\theta \equiv_{2^{r+1}} 1$. Siccome $(1+2^r)^\theta \equiv_{2^{r+1}} 1 + 2^r\theta$, allora $1 + 2^r\theta \equiv_{2^{r+1}} 1$ e quindi $\theta$ è pari. Pertanto, l'asserto è dimostrato.

□

**Remark 8.33.** In generale non vale il viceversa della Proposizione precedente, come si può notare dal seguente esempio.

**Esempio 8.34.** Consideriamo $n = 561 = 3 \cdot 11 \cdot 17$ e $b = 2$. Risulta che $n$ è uno pseudoprimo di Eulero ma non uno pseudoprimo forte rispetto alla base $b = 2$.

- Vale che $2^2 \equiv_3 1$ e per il **Piccolo Teorema di Fermat** $2^{10} \equiv_{11} 1$. Inoltre, siccome $17 = 2^4 + 1$, si ha che $2^8 \equiv_{17} 1$. Pertanto $2^{40} \equiv_{561} 1$ e quindi $2^{280} \equiv_{561} 1$, dove $280 = \frac{n-1}{2}$. Per la **Proposizione 8.18** vale che $\left(\frac{2}{561}\right) = 1$ e quindi $2^{280} \equiv_{561} \left(\frac{2}{561}\right)$. Pertanto 561 è uno pseudoprimo di Eulero rispetto alla base $b = 2$.
- Vale che $561 = 2^4 \cdot 35 + 1$. Se $2^{35} \equiv_{561} 1$ allora $2^5 \equiv_{561} 1$, poiché $2^{40} \equiv_{561} 1$, ma ciò è impossibile. Se $2^{70} \equiv_{561} -1$, allora $2^{30} \equiv_{561} -1$ e quindi $2^{10} \equiv_{561} -1$. Ciò è assurdo perchè 3 non divide $2^{10} + 1$. Allo stesso modo si prova che $2^{140}, 2^{280} \not\equiv_{561} -1$. Pertanto 561 non è uno pseudoprimo forte rispetto alla base $b = 2$.

□

Tuttavia, se $n \equiv_4 3$, vale anche il viceversa della **Proposizione 8.32** come risulta dalla seguente Proposizione:

**Proposizione 8.35.** Se $n \equiv_4 3$, allora $n$ è uno pseudoprimo forte rispetto alla base $b$ se e solo se $n$ è uno pseudoprimo di Eulero rispetto a $b$.

**Dimostrazione.** Per la **Proposizione 8.32** è sufficiente provare che se $n$ è uno pseudoprimo di Eulero rispetto alla base $b$, allora $n$ è uno pseudoprimo forte rispetto alla base $b$. Siccome $n \equiv_4 3$, allora $n = 2t + 1$ con $t$ dispari e quindi $b^t \equiv_n \left(\frac{b}{n}\right)$, i.e. $b^t \equiv_n \pm 1$.

□

**Lemma 8.36.** *Sia $(G,\cdot)$ un gruppo ciclico di ordine $m$, allora il numero degli elementi $x$ in $G$ tali che $x^k = 1$ è $d = gcd(m,k)$.*

**Dimostrazione.** Sia $x$ in $G$ tale che $x^k = 1$. Allora esiste un unico $0 \le j \le m-1$ tale che $x = g^j$, dove $g$ è un fissato generatore di $G$. Pertanto $g^{jk} = 1$ e quindi $m \mid jk$. Segue che $\frac{m}{d} \mid j$, dove $d = gcd(m,k)$. Allora il numero delle soluzioni di $x^k = 1$ è uguale al numero dei multipli di $\frac{m}{d}$ minori o uguali a $m$, che è appunto $d$.

□

**Lemma 8.37.** *Siano $n = 2^s t + 1$, $t$ dispari, un intero dispari e $p = 2^{s'} t' + 1$, $t'$ dispari, un divisore primo di $n$. Allora il numero delle soluzioni dell'equazione $x^{2^r t} = -1$ in $GF(p)$ è 0 oppure $2^r(t,t')$ a seconda che $r \ge s'$ oppure $r < s'$, rispettivamente.*

**Dimostrazione.** Il numero delle soluzioni di $x^{2^r t} = -1$ è uguale al numero delle soluzioni di $x^{2^{r+1} t} = 1$ che non siano anche soluzioni di $x^{2^r t} = 1$.
Per il **Lemma 8.36**, il numero delle soluzioni è

$$(2^{r+1}t, 2^{s'}t') - (2^r t, 2^{s'}t') = (t', t)(2^{\max(r+1,s')} - 2^{\max(r,s')})$$

che è quindi 0 oppure $2^r(t,t')$ a seconda che sia $r \ge s'$ oppure $r < s'$, rispettivamente.

□

**Teorema 8.38.** *Sia $n$ un intero composto dispari e sia $Y$ l'insieme delle basi rispetto alle quali $n$ è uno pseudoprimo forte. Allora*

$$|\mathcal{U}(\mathbb{Z}_n) - Y| \ge \frac{3}{4}\varphi(n).$$

**Dimostrazione.** Sia $\chi$ il rapporto tra il numero delle basi rispetto alle quali $n$ è uno pseudoprimo forte e il numero totale delle basi. Per provare la tesi è sufficiente provare che $\chi \le \frac{1}{4}$. Si distinguono i seguenti casi:

(1) Esiste un primo $p$ tale che $p^2 \mid n$;
(2) $n = pq$, con $p, q$ primi distinti;
(3) $n = p_1 \cdots p_k$, $k > 2$, con $p_1, ..., p_k$ primi a due a due distinti.

**Supponiamo che si verifichi il caso (1).**
Allora $n$ non è di Carmichael per la **Proposizione 8.24 (1)**. Sia quindi $b$ una base tale che $b^{n-1} \equiv_n 1$. Allora $b^{n-1} \equiv_{p^2} 1$. Poiché $\mathcal{U}\left(\mathbb{Z}_{p^2}\right)$ è ciclico di ordine $p(p-1)$, allora il numero delle basi comprese tra 0 e $p^2$ tali che $b^{n-1} \equiv_{p^2} 1$ è $(p(p-1), n-1)$.

Poiché $p$ non divide $n-1$, allora
$$(p(p-1), n-1) = (p-1, n-1) \leq p-1.$$
Procedendo in modo analogo, si ha che il numero delle basi comprese tra $p^2(h-1)$ e $p^2h$ per $h = 1, \ldots, n/p^2$ con $h$ fissato, è minore o uguale di $p-1$. Pertanto il numero delle basi $b$ comprese tra 0 ed $n$ tali che $b^{n-1} \equiv_{p^2} 1$ è minore o uguale a $\frac{n}{p^2}(p-1)$. Inoltre, il numero degli interi compresi tra 0 ed $n$ che non sono divisibili per $p^2$ è $n - \frac{n}{p^2}$, i.e. $\frac{n}{p^2}(p^2-1)$. Sia $X_1$ l'insieme delle basi $b$ rispetto alle quali $n$ è uno pseudoprimo forte. Osserviamo che $|X_1|$ può essere maggiorata dal numero delle basi rispetto alle quali $n$ è uno pseudoprimo. Tale numero, a sua volta, è minore o uguale del numero delle basi $b$ tali che $b^{n-1} \equiv_{p^2} 1$.
Chiaramente $|X_1| \leq \frac{n}{p^2}(p-1)$. D'altra parte, $|X_2|$ cioè il numero totale delle basi $b$ è minore o uguale al numero totale degli interi $b$ compresi tra 0 ed $n$ che non siano divisibili per $p^2$. Quindi $|X_2| \leq \frac{n}{p^2}(p-1)$. Pertanto segue che:
$$\chi = \frac{|X_1|}{|X_2|} \leq \frac{\frac{n}{p^2}(p-1)}{\frac{n}{p^2}(p^2-1)} = \frac{1}{p+1} \leq \frac{1}{4},$$
essendo $p$ un primo che divide un intero composto dispari. Quindi vale la tesi.

**Supponiamo che si verifichi il caso (2).**
Quindi, $n = pq$, con $p, q$ primi distinti, dove $p = 2^{s'}t' + 1$ e $q = 2^{s''}t'' + 1$, con $s', s'' \geq 1$ e $t', t''$ dispari. Senza perdere di generalità, possiamo supporre che $s'' \geq s'$. Sia $n = 2^s t + 1$, $t$ dispari, $s \geq 1$, uno pseudoprimo forte rispetto ad una base $b$. Dalla **Definizione 8.29** segue che o $b^t \equiv_n 1$ oppure esiste $0 \leq r < s$ tale che $b^{2^r t} \equiv_n -1$.
Supponiamo che $b^t \equiv_n 1$. Allora $b^t \equiv_p 1$ e $b^t \equiv_q 1$. Dal **Lemma 8.36**, segue che il numero dei $0 < b < p$ e dei $0 < b < q$ per cui si verifica questa possibilità è $(t', t)$ e $(t'', t)$, rispettivamente. Quindi il numero dei $0 < b < n$ per cui valga $b^t \equiv_n 1$ è $(t', t)(t'', t) \leq t't''$.
Se invece esiste $0 \leq r < s$ tale che $b^{2^r t} \equiv_n -1$, allora $b^{2^r t} \equiv_p -1$ e $b^{2^r t} \equiv_q -1$. Sia $n_{p,r}$ il numero delle soluzioni comprese tra 0 e $p$ dell'equazione congruenziale $b^{2^r t} \equiv_p -1$. Allora, dal **Lemma 8.37**, segue che $n_{p,r} = 2^r(t, t')$ oppure $n_{p,r} = 0$ a seconda che $r < s'$ o $r \geq s'$, rispettivamente ($s' = \min(s', s'')$). Definendo in modo analogo $n_{q,r}$, si ha che $n_{q,r} = 2^r(t, t'')$ oppure $n_{q,r} = 0$ a seconda che $r < s'$ o $r \geq s'$, rispettivamente. Quindi il numero dei $b$ tali che $b^{2^r t} \equiv_n -1$ è $n_{p,r} \cdot n_{q,r} \leq 2^r(t, t')2^r(t, t'') = 4^r t't''$. Siccome $\varphi(n) = (p-1)(q-1) = 2^{s'+s''}t't''$, allora vale che
$$\begin{aligned} \chi &\leq \frac{t't'' + \sum_{r=0}^{s-1} n_{p,r}n_{q,r}}{2^{s'+s''}t't''} = \frac{t't'' + \sum_{r=0}^{s'-1} n_{p,r}n_{q,r}}{2^{s'+s''}t't''} \leq \frac{t't'' + \sum_{r=0}^{s'-1} 4^r t't''}{2^{s'+s''}t't''} \\ &= \frac{1}{2^{s'+s''}}\left(1 + \sum_{r=0}^{s'-1} 4^r\right) = \frac{1}{2^{s'+s''}}\left(1 + \frac{4^{s'}-1}{4-1}\right) \end{aligned} \tag{8.12}$$
Se $s'' > s'$, allora (1) implica
$$\chi < \frac{1}{2^{2s'+1}}\left(\frac{3 + 2^{2s'} - 1}{3}\right) = \frac{1}{2^{2s'}3} + \frac{1}{6} \leq \frac{1}{12} + \frac{1}{6} = \frac{1}{4}.$$
Quindi, in questo sottocaso, vale l'asserto.

Consideriamo il caso in cui $s'' = s'$. Proviamo che $(t,t') < t'$ oppure che $(t,t'') < t''$. Supponiamo per assurdo che $(t,t') = t'$ e $(t,t'') = t''$. Allora $t' \mid t$ e $t'' \mid t$. Dal fatto che $t'$ divide $t$, segue che $t' \mid n-1$ e quindi $t' \mid q-1$, essendo $n-1 = p(q-1)+p-1$ e $t'$ un divisore di $p-1$. Allora $t' \mid t''$, siccome $q-1 = 2^{s''}t''$. Analogamente, si prova che $t'' \mid t'$ e quindi si ha che $t' = t''$. Pertanto, essendo $s' = s''$, segue che $p = q$ ma ciò è assurdo.
Pertanto si ha che $(t,t') \leq \frac{1}{3}t'$ oppure $(t,t'') \leq \frac{1}{3}t''$. Allora $(t,t')(t,t'') \leq \frac{1}{3}tt'$ e quindi segue che:

$$\begin{aligned}\chi &\leq \frac{\frac{1}{3}t't'' + \sum_{r=0}^{s-1} 4^r (t,t')(t,t'')}{2^{2s'}t't''} = \frac{\frac{1}{3}t't'' + \frac{1}{3}\sum_{r=0}^{s'-1} 4^r t't''}{2^{2s'}t't''} \\ &= \frac{\frac{1}{3} + \frac{1}{3}\sum_{r=0}^{s'-1} 4^r}{2^{2s'}} = \frac{1}{2^{2s'}3}\left(1 + \frac{2^{2s'}-1}{2^2-1}\right) = \frac{1}{2^{2s'}3^2}\left(2^{2s'}+2\right) \\ &= \frac{1}{9} + \frac{1}{18} < \frac{1}{4}.\end{aligned}$$

Ciò completa la dimostrazione nel caso (2).

**Supponiamo che si verifichi il caso (3).**
Quindi, $n = p_1 \cdot \ldots \cdot p_k$, $k > 2$, con $p_1, ..., p_k$ primi a due a due distinti. Chiaramente $p_i = 2^{s_i}t_i + 1$, con $s_i, t_i \geq 1$, $t_i$ dispari. Possiamo assumere senza perdere di generalità che $s_1 = \min(s_1, ..., s_k)$. Sia $n = 2^s t + 1$, $t$ dispari, $s \geq 1$, uno pseudoprimo forte rispetto ad una base $b$. Dalla **Definizione 8.29** segue che o $b^t \equiv_n 1$ oppure esiste $0 \leq r < s$ tale che $b^{2^r t} \equiv_n -1$.
Supponiamo che $b^t \equiv_n 1$, allora $b^t \equiv_{p_i} 1$ per ogni $i = 1, \ldots, k$. Dalla **Proposizione 8.2 (2)**, segue che il numero dei $b$ compresi tra 0 ed $n$ per cui $b^t \equiv_n 1$ è uguale al $\prod_{i=1}^k (t_i, t) \leq \prod_{i=1}^k t_i$.
Se invece esiste un $0 \leq r < s$ per cui $b^{2^r t} \equiv_n -1$, allora $b^{2^r t} \equiv_{p_i} -1$ per ogni $i$. Sia $n_{p_i,r}$ il numero delle soluzioni comprese tra 0 e $p_i$ dell'equazione congruenziale $b^{2^r t} \equiv_{p_i} -1$. Allora, dal **Lemma 8.37**, segue che $n_{p_i,r} = 2^r(t_i, t)$ oppure $n_{p_i,r} = 0$ a seconda che $r < s_1$ o $r \geq s_1$, rispettivamente.
Quindi il numero dei $b$ tali che $b^{2^r t} \equiv_n -1$ è $\prod_{i=1}^k n_{p_i,r} \leq \prod_{i=1}^k 2^r (t_i, t) \leq 2^{rk} \prod_{i=1}^k t_i$.
Siccome

$$\varphi(n) = \prod_{i=1}^k \varphi(p_i) = \prod_{i=1}^k (p_i - 1) = \prod_{i=1}^k 2^{s_i} t_i = 2^{s_1+\ldots+s_k} \prod_{i=1}^k t_i,$$

quindi

$$\begin{aligned}\chi &\leq \frac{\prod_{i=1}^k t_i + \prod_{r=0}^{s-1} 2^{rk} \prod_{i=1}^k t_i}{2^{s_1+\ldots+s_k} \prod_{i=1}^k t_i} = \frac{\prod_{i=1}^k t_i + \prod_{r=0}^{s_1-1} 2^{rk} \prod_{i=1}^k t_i}{2^{s_1+\ldots+s_k} \prod_{i=1}^k t_i} \\ &= \frac{1}{2^{s_1+\cdots+s_k}}\left(1 + \sum_{r=0}^{s_1-1} 2^{kr}\right) \leq \frac{1}{2^{ks_1}}\left(1 + \frac{2^{ks_1}-1}{2^k-1}\right) \\ &= \frac{1}{2^{ks_1}}\left(\frac{2^k-2}{2^k-1} + \frac{2^{ks_1}}{2^k-1}\right) = \frac{1}{2^{ks_1}} \cdot \frac{2^k-2}{2^k-1} + \frac{1}{2^k-1} \\ &\leq \frac{1}{2^k} \cdot \frac{2^k-2}{2^k-1} + \frac{1}{2^k-1} = 2^{1-k} \leq \frac{1}{4},\end{aligned}$$

essendo $k > 2$. Ciò completa la dimostrazione.

□

**Remark 8.39.** La probabilità che un intero composto dispari $n$ sia uno pseudoprimo forte rispetto a $k$ basi distinte è al più $\frac{1}{4^k}$.

## 8.2 Test di Primalità

In questa sezione vederemo i Testi di primalità di **Solovay-Strassen** e **Miller-Rabin** che si basano sulle definizioni di Pseudoprimi di Eulero e Pseudoprimi forti, rispettivamente.

**Figura 8.1:** Robert Martin Solovay (1938), Volker Strassen (1936), Gary Miller e Michael Oser Rabin (1931)

Gli algoritmi hanno le seguenti caratteristiche

- **Vantaggio:** Questi algoritmi sono computazionalmente efficienti, ovvero un intero $n$ è testato in un tempo $O(\log^3 n)$.
- **Svantaggio:** Gli algoritmi forniscono come output che $n$ è un numero primo, quando in realtà non lo è. Tuttavia, la probabilià di commettere un errore può essere ridotta sotto una fissata soglia eseguendo l'algoritmo un certo numero di volte.

Una domanda importante è quanti interi casuali bisogna testare prima di trovarne uno che sia primo.

Siano $N$ un intero positivo e $\pi(N) = |\{p \leq N : p \text{ primo}\}|$. Il **Teorema dei numeri Primi** asserisce che $\pi(N) \simeq N/\ln N$. Quindi la probabilià che un intero $p \leq N$ sia primo è $1/\ln N$. Se $p$ è di circa 512 bit, allora la suddetta probabilità è $1/\ln 2^{512} \simeq 1/355$. Pertanto, in media, si trova un numero primo ogni 355 interi casuali.

In realtà, la probabiltà è raddoppiata poichè tali primi sono numeri dispari. Quindi la probabilià è di circa 2/355. Pertanto, la genesi dei numeri primi per la costruzione dell'RSA è fattibile.

**Definizione 8.40.** **(Problema Decisionale)**
Un **problema decisionale** è una domanda a cui deve essere risposto con un 'sì' o un 'no'.

**Definizione 8.41.** **(Algoritmo Montecarlo)**
Un **Algoritmo Montecarlo Orientato verso il si con probabilità di errore** $\varepsilon$ è un algoritmo randomizzato utilizzato per un problema decisionale in cui la risposta 'si' è corretta, mentre la risposta 'no' può essere non corretta con probabilità al più $\varepsilon$.

Si consideri il seguente problema decisionale

**Problema 8.42.** **(Interi Composti)**

**Istanza:** Un intero positivo $n \geq 2$
**Domanda:** $n$ è un intero composto?

Vediamo ora il Test di Primalià di **Soloway-Strassen**:

**Algoritmo 8.43.** **(Soloway-Strassen ($n$))**

Si scelga un intero $a$ compreso tra 1 e $n-1$
$x \longleftarrow \left(\frac{a}{n}\right)$
**if** $x = 0$
**then return** ( "$n$ è un intero composto" )
$y \longleftarrow a^{(n-1)/2} \ mod \ n$
**if** $x \equiv y \ mod \ n$
**then return** ( "$n$ è primo")
**else return** ( "$n$ è un intero composto" )

**Teorema 8.44.** *Il Test di Primalità di Soloway-Strassen è un algoritmo Montecarlo orientato verso il si con probabilità di errore al più* $1/2$.

**Dimostrazione.** Dall'analisi dell'**Algoritmo 8.43** segue immediatamente che l'output "$n$ è un intero composto" è sempre corretta, mentre segue dal **Teorema 8.26** che la probabilità che l'output "$n$ è primo" sia scorretto è minore o uguale a $1/2$.

□

**Teorema 8.45.** *Il Test di Primalità di Soloway-Strassen ha complessità* $O(\log^3 n)$.

**Dimostrazione.** Il calcolo del simbolo di Jacobi consiste di riduzioni modulari e la fattorizzazione rispetto alle potenze di 2. Siccome ogni intero è rappresentato in binario, la la fattorizzazione rispetto alle potenze di 2 consiste nel determinare il numero degli 0 finali. Quindi il calcolo del simbolo di Jacobi si riduce al numero di riduzioni modulari. Siccome ogni riduzione modulare ha cmplessità $O(\log^2 n)$ e il numero delle riduzioni è al più pari al numero delle cifre di $n$, vale che il simbolo di Jacobi ha complessità $O(\log^3 n)$. D'altra parte, $a^{(n-1)/2} \ mod \ n$ ha complessità $O(\log^3 n)$. Pertanto, il Test di Primalità di Soloway-Strassen ha complessità $O(\log^3 n)$.

□

**Remark 8.46.** Un'analisi più precisa mostra che in realtà il Test di Primalità di Soloway-Strassen ha complessità $O(\log^2 n)$.

Supponiamo di aver generato un intero causale dispari $n$ e vogliamo testarne la sua primalità attraverso l'**Algoritmo di Soloway-Strassen**. Dopo averlo testato $m$ volte, quale è la confidenza che $n$ sia primo? Saremmo tentati, sulla base del **Teorema 8.26** che avendolo superato $m$ volte la probabilià che $n$ sia primo è $1 - 1/2^m$.

Nella realtà deve essere fatta una più precisa analisi come segue. Si considerino i seguenti eventi

$E_1$ : un intero causale dispari $n$ di fissata grandezza è composto.

$E_2$ : l'**Algoritmo 8.43** fornisce in output "$n$ è primo" $m$ volte in successione.

Dal **Teorema 8.26** segue che $\boldsymbol{P}[E_2/E_1] \leq 1/2^m$. Noi invece siamo interessati a $\boldsymbol{P}[E_1/E_2]$. Dal **Teorema di Bayes** segue che

$$\boldsymbol{P}[E_1/E_2] = \frac{\boldsymbol{P}[E_2/E_1]\boldsymbol{P}[E_1]}{\boldsymbol{P}[E_2]} = \frac{\boldsymbol{P}[E_2/E_1]\boldsymbol{P}[E_1]}{\boldsymbol{P}[E_2/E_1]\boldsymbol{P}[E_1] + \boldsymbol{P}[E_2/E_1^c]\boldsymbol{P}[E_1^c]}.$$

Dal **Teorema dei Numeri Primi** segue che se $N \leq n \leq 2N$, il numero dei primi (dispari) compresi tra $N$ e $2N$ è approssimativamente a

$$\frac{2N}{\ln 2N} - \frac{N}{\ln N} \simeq \frac{N}{\ln N} \simeq \frac{n}{\ln n}.$$

Siccome il numero degli interi dispari tra $N$ è $2N$ è $N/2 \simeq n/2$, allora

$$\boldsymbol{P}[E_1^c] \simeq \frac{n}{\ln n} / \frac{n}{2} = \frac{2}{\ln n}.$$

Inoltre, dal **Teorema di Eulero (Teorema 8.7)** segue che $\boldsymbol{P}[E_2/E_1^c] = 1$.

Quindi

$$\begin{aligned}
\boldsymbol{P}[E_1/E_2] &= \frac{\boldsymbol{P}[E_2/E_1]\left(1-\frac{2}{\ln n}\right)}{\boldsymbol{P}[E_2/E_1]\left(1-\frac{2}{\ln n}\right)+\frac{2}{\ln n}} \\
&= \frac{\boldsymbol{P}[E_2/E_1](\ln n-2)}{\boldsymbol{P}[E_2/E_1](\ln n-2)+2} \\
&\leq \frac{2^{-m}(\ln n-2)}{2^{-m}(\ln n-2)+2} \\
&= \frac{\ln n-2}{(\ln n-2)+2^{m+1}}.
\end{aligned}$$

Nella seguente tabella sono tabulate le funzioni $2^{-m}$ e $\frac{\ln n-2}{(\ln n-2)+2^{m+1}}$.

| $m$ | $2^{-m}$ | bound sulla probabilità di errore |
|---|---|---|
| 1 | 0.500 | 0.989 |
| 2 | 0.200 | 0.978 |
| 5 | $0.312 \times 10^{-1}$ | 0.847 |
| 10 | $0.977 \times 10^{-3}$ | 0.147 |
| 20 | $0.954 \times 10^{-6}$ | $0.168 \times 10^{-3}$ |
| 30 | $0.931 \times 10^{-9}$ | $0.164 \times 10^{-6}$ |
| 50 | $0.888 \times 10^{-15}$ | $0.157 \times 10^{-12}$ |
| 100 | $0.789 \times 10^{-30}$ | $0.139 \times 10^{-27}$ |

I primi utilizzati per la costruzione del crittosistema RSA devono essere di circa 512 cifre binarie. Sia $n$ un intero candidato ad essere uno dei due primi per la costruzione del crittosistema RSA. Quindi sia $n \simeq 2^{512} \simeq e^{355}$ un intero da testare, allora

$$\frac{\ln n-2}{(\ln n-2)+2^{m+1}} \simeq \frac{353}{353+2^{m+1}}$$

per $50 \leq m \leq 100$ la probabilità di commettere un errore è veramente piccola.

**Algoritmo 8.47.** **(Miller-Rabin ($n$))**
Si scriva $n$ come $2^k m$ con $m$ dispari
Si scelga un intero casuale $a$ compreso tra 1 e $n-1$
$b \longleftarrow a^m \ mod\ n$
**if** $b \equiv 1 \ mod\ n$
**then return** ("$n$ è primo")
**for** $i \longleftarrow 0$ **to** $k-1$
**do** { **if** $b \equiv -1 \ mod\ n$ **then return** ("$n$ è primo") **else** $b \longleftarrow b^2 \ mod\ n$
**return** ("$n$ è composto")

**Teorema 8.48.** *Il Test di Primalità di Miller-Rabin è un algoritmo Montecarlo orientato verso il si con probabilità di errore al più* $1/4$ *e complessità* $O(\log^3 n)$.

**Dimostrazione.** Dall'analisi dell'**Algoritmo 8.47** segue immediatamente che l'output "$n$ è un intero composto" è sempre corretto, mentre segue dal **Teorema 8.38** che la probabilità che l'output "$n$ è primo" sia scorretto è minore o uguale a $1/4$. Infine, è facile vedere che la complessità è $O(\log^3 n)$.

□

Procedendo in modo analogo all'algoritmo di **Soloway-Strassen** vale

$E_1$ : un intero causale dispari $n$ di fissata grandezza è composto.

$E_2$ : l'**Algoritmo 8.47** fornisce in output "$n$ è primo" $m$ volte in successione.

Segue che

$$\begin{aligned} \boldsymbol{P}[E_2/E_1] &\leq 1/2^{2m}. \\ \boldsymbol{P}[E_1/E_2] &\leq \frac{\ln n - 2}{(\ln n - 2) + 2^{2m+1}}. \end{aligned}$$