Simbolo di Jacobi

$\forall a, n \qquad n \in \mathbb{N} \quad n$ dispari

Se p è un primo dispari $\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } p \mid a \\ +1 & \text{se } a \in \square_p \\ -1 & \text{se } a \notin \square_p \end{cases}$

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

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ poniamo $\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i}$

per convenzione poniamo $\boxed{\left(\frac{a}{1}\right) = 1}$

- $a = b \bmod n \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

se $a = b \bmod n \Rightarrow a = b + kn \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b+kn}{n}\right) =$

$= \prod \left(\frac{b+kn}{p_i}\right)^{\alpha_i}$ ma $p_i \mid n \Rightarrow$

$\Rightarrow \prod \left(\frac{b}{p_i}\right)^{\alpha_i} \rightarrow$ ok

- $\boxed{\left(\frac{a}{n}\right) = \left(\frac{a \,\%\, n}{n}\right)}$ facili ragionando sulla fattorizzazione
- $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
- $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
- $\boxed{\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}}$ legge di reciprocità quadratica

$\left(\frac{m}{n}\right) \neq 0$

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}} \left(\frac{n}{m}\right)$$ m, u dispari

CALCOLO DI $\left(\frac{m}{n}\right)$

```
function Jacobi(a,m)
    t=1
    a %= m
    while a!=zero(a)
        while (a%2)==zero(a)
            a=a÷2
            (m%8 ∈ [3,5]) && (t*=-1)
        end
        a,m=m,a
        (a%4==3) && (a%4==m%4) && (t*=-1)
        a %= m
    end
    m==1 && return t
    return 0
end
```

$$\left(\frac{73}{13}\right) = \left(\frac{1}{13}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}} = 1 \quad \text{fine.}$$

$$\left(\frac{38}{105}\right) = (-1)^{\frac{104}{2}\cdot\frac{38}{2}} \left(\frac{105}{38}\right) = \left(\frac{105}{38}\right) =$$

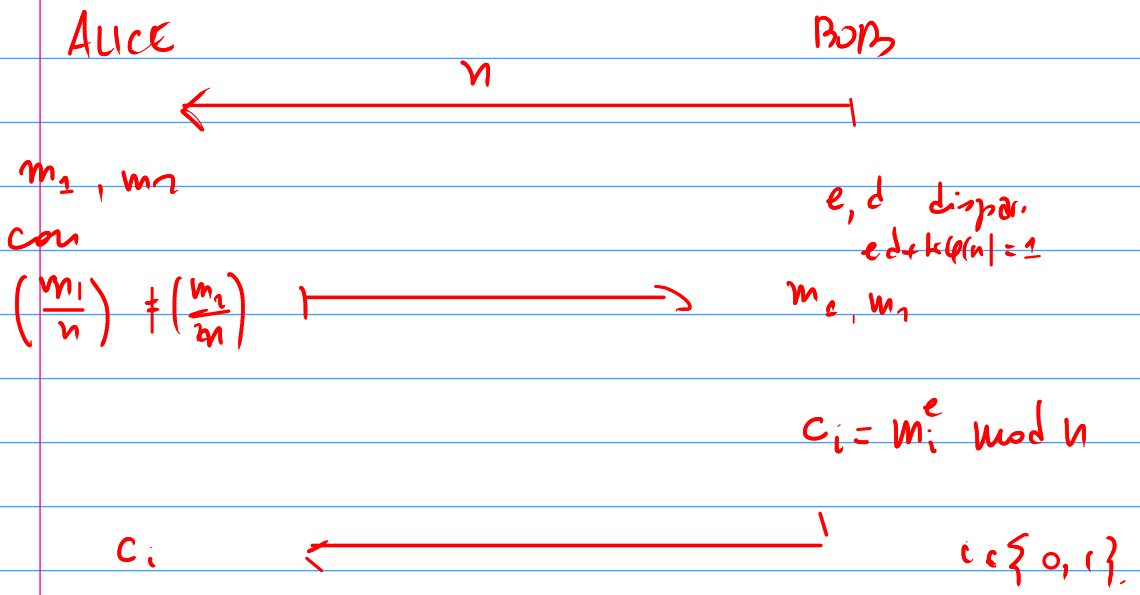
$$= \left(\frac{27}{38}\right) = (-1)^{\frac{26}{2}\cdot\frac{38}{2}} \left(\frac{38}{27}\right) = -\left(\frac{38}{27}\right) =$$

$$= -\left(\frac{12}{27}\right) = -\left(\frac{4}{27}\right)\cdot\left(\frac{3}{27}\right) =$$

$$= 0$$

- $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$
- $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$ $\begin{cases} +1 & \text{se } n \equiv 1 \bmod 4 \\ -1 & \text{se } n \equiv 3 \bmod 4 \end{cases}$

RSA - IND - CPA



$$\left(\frac{c_i}{n}\right) = \left(\frac{m_i}{n}\right)$$

Ricavarsi c_i

ATTACCO IN UNO SCENARIO PARTICOLARE MA IL PROBLEMA VERO É FATTORIZZARE n

→ Servono primi p, q grandi e "casuali".

Come costruire un primo casuale

k intero casuale dispari e "grande"

k (primo?) → sì → k

→ no → proviamo con k+2

primes is in P !

come testare se p é primo

$\forall i$ con $2 \leq i < p$ provare a dividere p per i

se $\exists i$ t.c. $p = ki \Rightarrow$ p non é primo

se non p è primo

in questo caso ($x \exists i$) vale $\Rightarrow$ è una <u>verifica</u> del fatto che p non è primo.

$\rightarrow$ semplificazione: Verifico $\forall i$ con $2 \le i \le \lfloor \sqrt{p} \rfloor$

perché se $p = ik$ allora $\min\{i,k\} \le \lfloor \sqrt{p} \rfloor$

$\rightarrow$ <u>oss.</u> p è primo $\iff$ $(p-1)! \equiv -1 \bmod p$

<u>DIM</u> se $p = \alpha\beta$ con $1 < \alpha, \beta < p \Rightarrow$

α e β compaiono nel fattoriale di $(p-1)$

se $\alpha \neq \beta \Rightarrow p \mid p-1 \Rightarrow (p-1)! \bmod p = 0$

se $\alpha = \beta \Rightarrow p = \alpha^2$ ma allora α e 2α compaiono in $(p-1)!$ e dunque $\alpha^2 \mid (p-1)!$ e $(p-1)! \bmod p = 0$

Supponiamo adesso p primo $\Rightarrow (p-1)! \bmod p =$

$$= \prod_{x \in \mathbb{F}_p^*} x = 1 \cdot (-1) \underbrace{\prod x_i x_i^{-1}}_{=1} = -1$$

elementi che sono reciproci di se stessi

$\square$

$p = 7$ $\quad (p-1)! = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = -1 \bmod 7$

$3 \cdot 5 \bmod 7 = 1 \bmod 7$

$-1 \bmod 7$

$2 \cdot 4 \bmod 7 = 8 \bmod 7 = 1$

$p = 6$ $\quad 5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \bmod 6 = 0$

6

$p=8$ $\quad 8! = 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 \cdot 7\cdot 8 = 0 \quad 8 \mid 8!$

$3\times 6 = 18$

$p=11$ $\quad 10! = 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10 \equiv -1 \bmod 11$

$+1$ $\quad 1$ $\quad 1$ $\quad -1$

problema: non si conosce un metodo veloce per calcolare $(p-1)! \bmod p$

ALTRI TEST

$$|\mathbb{F}_p^*| = p-1$$

Sia $a \in \mathbb{F}_p^* \Rightarrow a^{p-1} \equiv 1 \bmod p$

per ogni intero $1 \leq a < p$

p è primo $\Leftrightarrow \boxed{a^{p-1} \equiv 1} \bmod p$ (Fermat).

Se p non è primo $\Rightarrow \exists\ 1 \leq a < p$ con $MCD(a,p) \neq 1$, questo elemento non è invertibile $\Rightarrow a^{p-1} \neq 1 \Rightarrow$ esso è un testimone del fatto che p non è primo

IDEA: prendere a "a caso". Vedere se $a^{p-1} \equiv 1 \bmod p$ e se va sempre bene convincersi che p è primo

NON FUNZIONA $\rightarrow \exists$ dei cosiddetti pseudo-primi (di Fermat)

per cui $\forall\, 1 \le a < p-1$ con $MCD(a,p)=1$
si ha $a^{p-1} \equiv 1 \bmod p$.

→ Gli unici testimoni della non primalità di p sono proprio quegli a tali che $MCD(a,p)$ fornisce una fattorizzazione di n.

Il più piccolo pseudoprimo di Fermat è $561 = 3 \cdot 11 \cdot 17$

Solovay-Strassen

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p$$

ci chiediamo se $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n$

a testimone che n non è primo $\iff$

$$a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \bmod n$$

Questi sono i possibili testimoni "mendaci"
cioè gli a per cui

$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$ anche se n non è primo

→ Fermat: $\varphi(n) \approx n$

→ Eulero-Jacobi → sono circa $\frac{\varphi(n)}{2}$

(dopo $\frac{\varphi(n)}{2}+1$ test abbiamo una dim. di primalità)

In generale dopo k iterazioni la prob. che un numero n non sia primo è $\approx \frac{1}{2^k}$.

Miller - Rabin

n intero è una pseudo-prima forte in base a se vale una di queste 2 relazioni $n = 2^s d + 1$

$$\begin{cases} a^d \equiv 1 \bmod n & \text{oppure} \\ \exists r \text{ tale che } a^{2^r d} \equiv -1 \bmod n & 0 \le r < s \end{cases}$$

si vede che per ogni primo questa condizione vale.

→ ci sono al più $\frac{1}{2}\varphi(n)$ testimoni mendaci

Se vale l'ipotesi di Riemann Generalizzata, allora il numero dei testimoni mendaci è al più $O(\log(n)^2)$

```
function SolvayStrassen(n)
    n==2 && return true
    n>2 && (n%2==zero(n)) && return false
    W=(n+3)÷2
    for a in 2:W
        if (powermod(a,(n-1)÷2,n)!=(n+Jacobi(a,n))%n)
            print("Witness=",a,"\n")
            return false
        end
    end
    return true
end
```

```
function SPprime(n,a)
    t,s = n-1,0
    while (t%2==0)
        s += 1
        t >>= 1
    end
    b=powermod(a,t,n)
    ((b==1) | (b==n-1)) && return true
    for j in 1:s-1
        b=powermod(b,2,n)
        b==n-1 && return true
    end
    false
end
```

```
function Miller(n)
    W = Integer(min(round(2*log(n)^2),n-1))
    for a in 2:W
        SPprime(n,a) || return false
    end
    true
end
```

```
function NextPrime(n)
    (n<=2)    && return 2
    (n%2==0)  && return NextPrime(n+1)
    Miller(n) && return n
    NextPrime(n+2)
end
```