Numeri primi grandi

Il crivello di Eratostene

N = 30

7.7 = 49 > 30

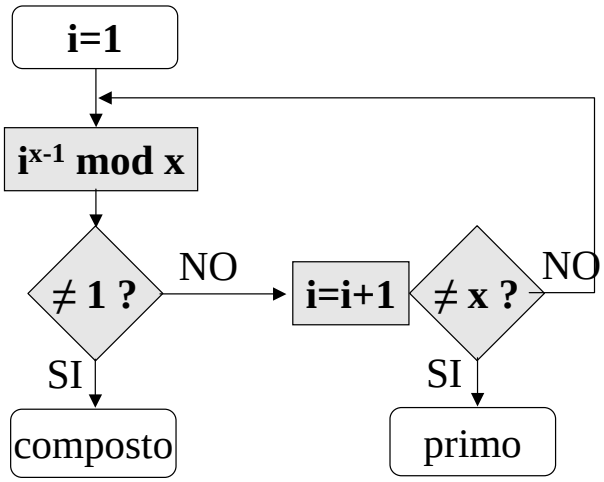
2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13

~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~

~~26~~ ~~27~~ ~~28~~ 29 ~~30~~

$\pi(30) = 10$

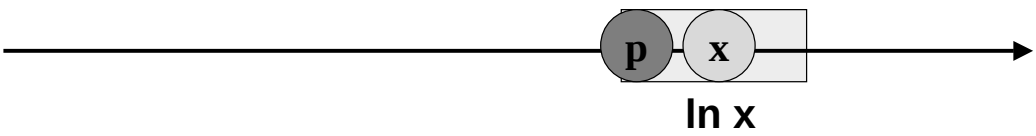
Il test di Fermat



Ricerca di un numero primo grande

π(x): n° di primi nell'intevallo 2÷**x**

T9: $\lim_{x \to \infty} \frac{\pi(x)}{x / \ln x} = 1$



ln x

Teorema di Dirichlet: $\mathbf{p_n \cong n \ln n}$

1. **x** generato a caso
   1.1 If **x** pari then **x = x+1**
2. If (x primo?) = *false*
   then **x = x + 2** and repeat 2.
3. Return **x**

Test di primalità

1. Test **deterministici**: se **n** non lo supera è **composto**, se lo supera è primo
2. Test **probabilistici**: se **n** fallisce il test è composto; se lo supera è **probabilmente primo**

I test deterministici sono computazionalmente più onerosi dei test probabilistici.
2002: algoritmo polinomiale AKS (Indian Institute of Technology)
I test probabilistici sono polinomiali, ma devono essere poi ripetuti più e più volte per far tendere a 1 la probabilità di avere realmente individuato un primo.

Miller-Rabin: dopo t iterazioni superate positivamente la probabilità che n non sia primo è più piccola di $\mathbf{2^{-2t}}$.

Numeri pseudo-primi

Fermat: Dato **n**

1. si sceglie a caso un intero **a**, con **1 <a <n**
2. si calcola $\mathbf{a^{n-1}}$ **mod n**:
   2.1 se il risultato è diverso da 1, allora **n** è composto;
   2.2 se il risultato vale 1, **n** è **pseudo-primo in base a**

Fermat, Eulero, Dirichlet, ecc.

Test di Solovay-Strassen

Test di Miller-Rabin

Test di Miller e Rabin: principi

n (il numero da sottoporre al test) deve essere dispari.
Si pone $\mathbf{n-1 = r.2^s}$ (con **r** dispari, $\mathbf{s \geq 1}$)
Si sceglie a caso un intero **a** e si calcola:

$$\mathbf{a^{n-1} \bmod n = (a^r)^{2^s} \bmod n}$$

n è sicuramente composto se

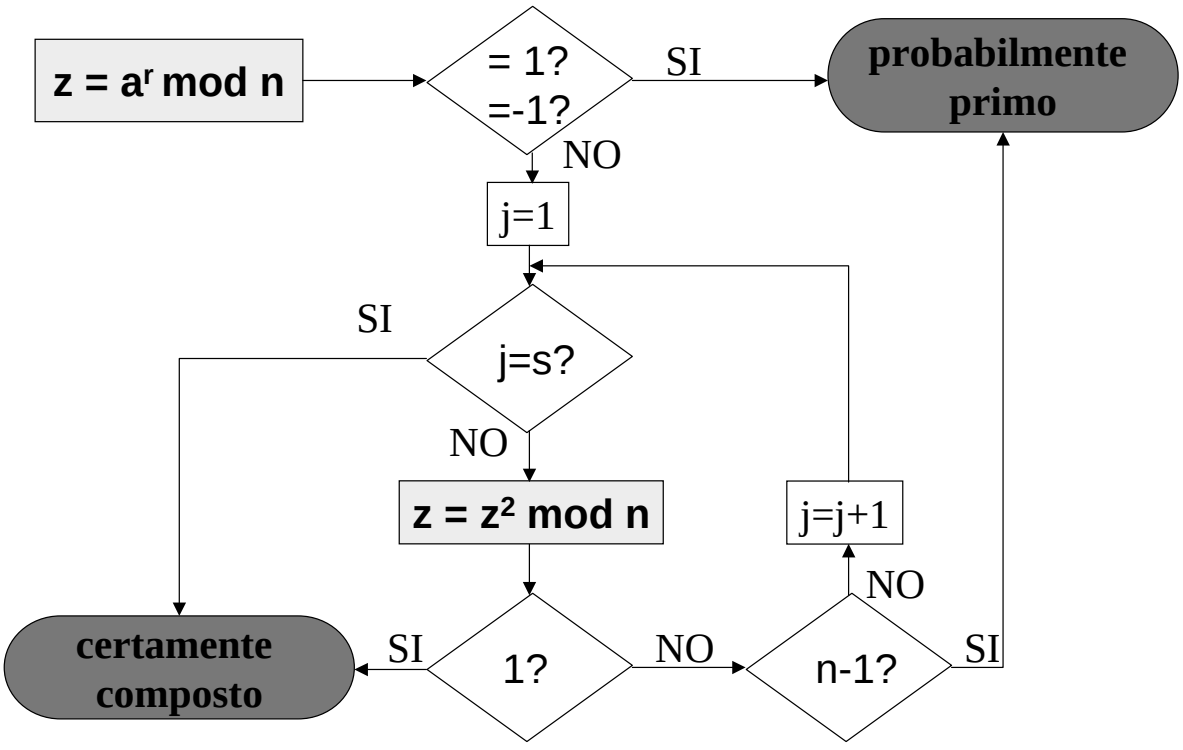
$$\mathbf{a^r \bmod n \neq 1}$$

e se, per ogni j, $0 \leq j \leq s-1$,

$$\mathbf{(a^r)^{2^j} \bmod n \neq -1}$$

[2] pag.138
[9] pag.236

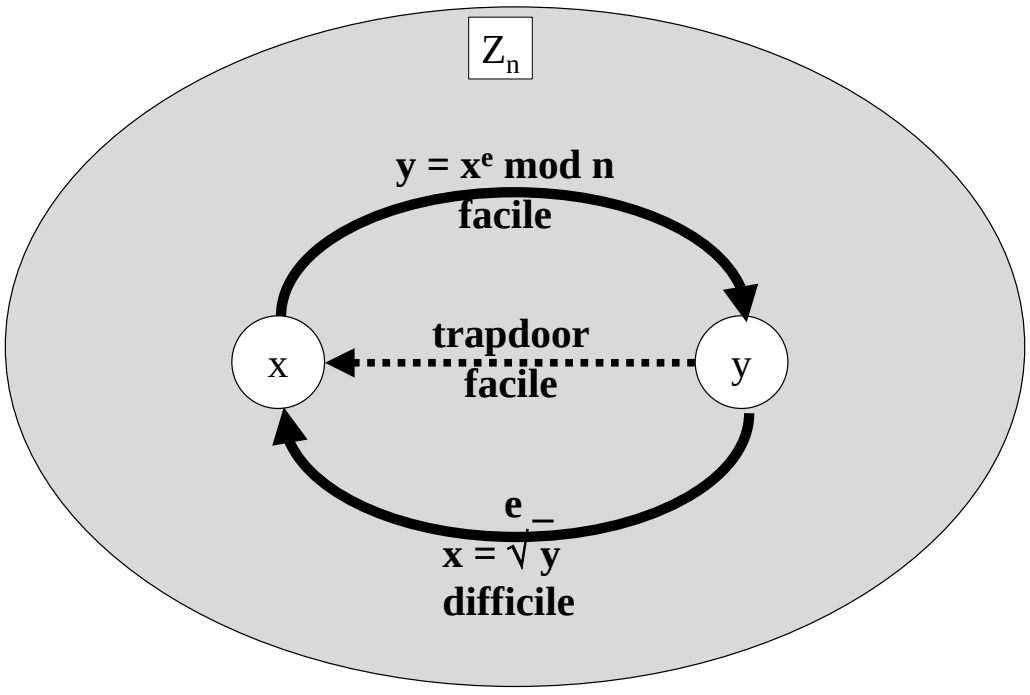
Test di Miller e Rabin



Un numero diverso da 1 con quadrato uguale a 1 è sicuramente composto

RSA

Esponenziazione mod n = p×q e
Radice e-esima



The RSA Algorithm (1978)

Public key: {n,e}
n = p×q con p e q primi
e coprimo con **Φ(n)**

Encryption

- Plaintext: **m < n**
- Ciphertext: **$c = m^e \bmod n$**

Private key: {n,d}
$d = e^{-1} \bmod \Phi(n)$

trapdoor

Decryption

- Ciphertext: **c < n**
- Plaintext: **$m = c^d \bmod n$**

Key Generation

- Select *p,q* — ***p* and *q* both prime**
- Calculate *n* — ***n* = *p* x *q***
- Calculate Φ(*n*) — **$\Phi(n) = (p-1)(q-1)$**
- Select integer *e* — **$\gcd(\Phi(n),e) = 1;\ 1<e<\Phi(n)$**
- Calculate *d* — **$d = e^{-1} \bmod \Phi(n)$**
- Public Key — **k[pub] = {e,n}**
- Private key — **k[priv] = {d,n}**

exp	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2	4
3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9
4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16
5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5	25
6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6	3
7	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7	16
8	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8	31
9	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15
10	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1
11	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22
12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
13	13	4	19	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20	4
14	14	31	5	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1
15	15	27	9	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12
16	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25
17	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32	16	8	4	2	1	17	25
18	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6	9	30	12	18	27
19	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10	25	13	16	7	1	19	31
20	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20	4
21	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12
22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22
23	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1
24	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24	15
25	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31
26	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26	16
27	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3
28	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28	25
29	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29	16
30	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30	9
31	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4
32	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1

Esponenziazione modulo un numero composto da due primi

Esempio: $n = 3 \times 11$

$Z_n = \{1,2,..31,32\}$

$\Phi(33) = 20$

exp	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1
3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12
4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1
5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1
6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12
7	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1
8	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1
9	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12
10	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1
11	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22
12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
13	13	4	19	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1
14	14	31	5	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25
15	15	27	9	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15
16	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1
17	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32	16	8	4	2	1
18	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6	9	30	12
19	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10	25	13	16	7	1
20	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1
21	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12
22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22
23	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1
24	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12
25	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1
26	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1
27	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12
28	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1
29	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1
30	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12
31	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1
32	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1

T10: "se $\mathbf{n = p \times q}$ e $\mathbf{r \equiv s \pmod{\Phi(n)}}$, allora $\mathbf{a^r \equiv a^s \pmod{n}}$ per ogni **a**

Conviene prendere $\mathbf{e \leq \Phi(n)}$

exp	1		3		7		9		11		13		17		19	20
1	1		1		1		1		1		1		1		1	1
2	2		8		29		17		2		8		29		17	1
3	3		27		9		15		3		27		9		15	12
4	4		31		16		25		4		31		16		25	1
5	5		26		14		20		5		26		14		20	1
6	6		18		30		24		6		18		30		24	12
7	7		13		28		19		7		13		28		19	1
8	8		17		2		29		8		17		2		29	1
9	9		3		15		27		9		3		15		27	12
10	10		10		10		10		10		10		10		10	1
11	11		11		11		11		11		11		11		11	22
12	12		12													
13	13		19													
14	14		5													
15	15		9													
16	16		4													
17	17		29													
18	18		24													
19	19		28													
20	20		14													
21	21		21													
22	22		22		22		22		22		22		22		22	22
23	23		23		23		23		23		23		23		23	1
24	24		30		18		6		24		30		18		6	12
25	25		16		31		4		25		16		31		4	1
26	26		20		5		14		26		20		5		14	1
27	27		15		3		9		27		15		3		9	12
28	28		7		19		13		28		7		19		13	1
29	29		2		17		8		29		2		17		8	1
30	30		6		24		18		30		6		24		18	12
31	31		25		4		16		31		25		4		16	1
32	32		32		32		32		32		32		32		32	1

T11:"se $x \in Z^*_{\Phi(n)}$, cioè se **MCD(x, Φ(n))=1,** per ogni $y \in Z_n$

$$y^x \bmod n$$

genera una permutazione di Z_n"

Per la decifrabilità deve essere

$e \in Z^*_{\Phi(n)}$

exp	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2	4
3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9
4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16
5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5	25
6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6	3
7	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7	16
8	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8	31
9	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15
10	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1
11	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22
20	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20	4
21	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12
22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22
23	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1
24	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24	15
25	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31
26	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26	16
27	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3
28	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28	25
29	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29	16
30	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30	9
31	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4
32	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1

T12 (estensione di Eulero del piccolo teorema di Fermat):
"per ogni intero **n, primo** o **composto,** e per ogni $x \in Z^*_n$ si ha

$$x^{\Phi(n)} \equiv 1 \pmod n$$

N.B. **x coprimo** con **n**

exp	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2	4
3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9
4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16
5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5	25
6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6	3
7	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7	16
8	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8	31
9	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15
10	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1
11	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22
22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22
23	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1
24	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24	15
25	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31
26	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26	16
27	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3
28	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28	25
29	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29	16
30	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30	9
31	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4
32	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1

T13 (corollario di T12): "per ogni **n = p × q**, con **p** e **q primi,** e per ogni **x > 0** si ha

$$x^{\Phi(n)+1} \equiv x \pmod{n}$$

e anche, per ogni intero k,

$$x^{k\Phi(n)+1} \equiv x \pmod{n}$$ "

Giustificazione di RSA

Da T13 discende che per **n = p.q** *e per ogni* **0 < m < n** *si ha*:

$$m^{k\Phi(n)+1} \equiv m^{k(p-1)(q-1)+1} \pmod{n} = m$$

In RSA deve essere:

$$m^{e\,d} \equiv m \pmod{n}$$

Ciò è vero se

e d = k(p-1)(q-1)+1

o anche

e d - k(p-1)(q-1) = 1

e quindi

- **MCD (e, Φ(n)) = 1**
- **$d = e^{-1} \bmod \Phi(n)$**

proprietà vere per costruzione

The RSA Algorithm (1998)

$\lambda(n) = mCM(p-1, q-1)$
$= \Phi(n)/MCD(p-1, q-1)$

Public key: {n,e}
n = p.q con p e q primi
e coprimo con **$\lambda(n)$**

Private key: {n,d}
$d = e^{-1}$ mod **$\lambda(n)$**

exp	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	31	29	25	17	1
3	3	9	27	15	12	3	9	27	15	12
4	4	16	31	25	1	4	16	31	25	1
5	5	25	26	31	23	16	14	4	20	1
6	6	3	18	9	21	27	30	15	24	12
7	7	16	13	25	10	4	28	31	19	1
8	8	31	17	4	32	25	2	16	29	1
9	9	15	3	27	12	9	15	3	27	12
10	10	1	10	1	10	1	10	1	10	1
11	11	22	11	22	11	22	11	22	11	22
12	12	12	12	12	12	12	12	12	12	12
13	13	4	19	16	10	31	7	25	28	1
14	14	31	5	4	23	25	20	16	26	1
15	15	27	9	3	12	15	27	9	3	12
16	16	25	4	31	1	16	25	4	31	1
17	17	25	29	31	32	16	8	4	2	1
18	18	27	24	3	21	15	6	9	30	12
19	19	31	28	4	10	25	13	16	7	1
20	20	4	14	16	23	31	26	25	5	1
21	21	12	21	12	21	12	21	12	21	12
22	22	22	22	22	22	22	22	22	22	22
23	23	1	23	1	23	1	23	1	23	1
24	24	15	30	27	21	9	18	3	6	12
25	25	31	16	4	1	25	31	16	4	1
26	26	16	20	25	23	4	5	31	14	1
27	27	3	15	9	12	27	3	15	9	12
28	28	25	7	31	10	16	19	4	13	1
29	29	16	2	25	32	4	17	31	8	1
30	30	9	6	15	21	3	24	27	18	12
31	31	4	25	16	1	31	4	25	16	1
32	32	1	32	1	32	1	32	1	32	1

p =3, q = 11
n = 33
$\Phi(n) = 20$
$\lambda(n) = 10$

Sicurezza di RSA: radice e-esima, fattorizzazione di n

$$m = \sqrt[e]{c} \bmod n$$

P2: noti **c**, **e**, **n** calcolare **m**

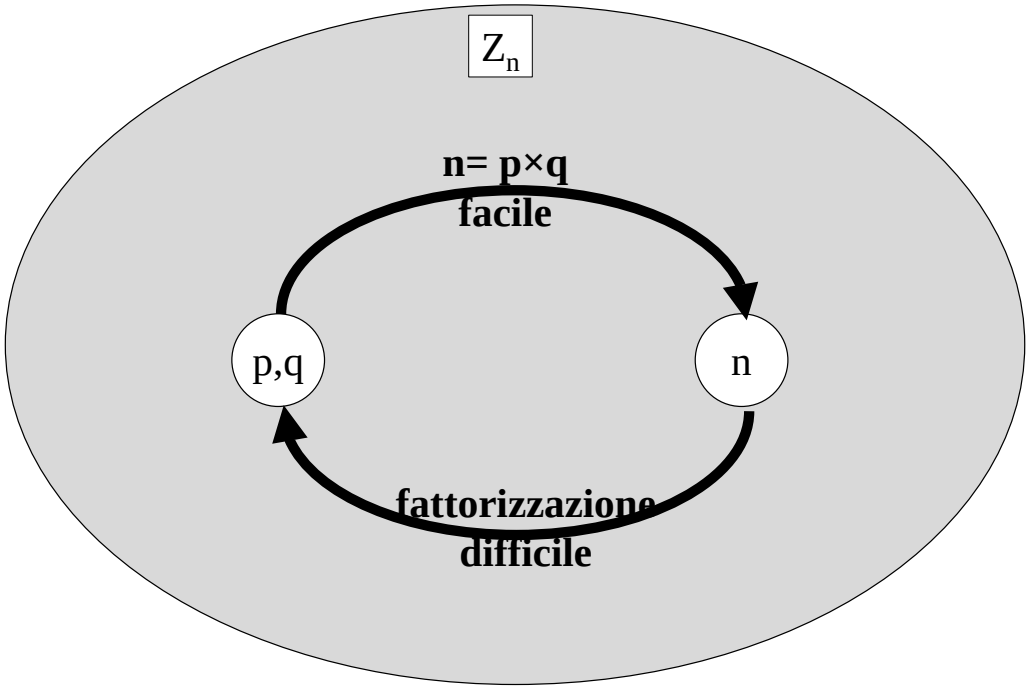
☹

Tempo sub-esponenziale

P2 è facile se si conoscono p e q, che l'utente deve quindi o distruggere, o tenere segreti

Attacco con fattorizzazione

Prodotto di primi e Fattorizzazione



Fattorizzazione di un numero composto

 P3: problema della fattorizzazione - Dato un intero positivo **n**, trovare i numeri primi $\mathbf{p_i}$ ed i coefficienti interi $\mathbf{e_i \geq 1}$ tali che

$$\mathbf{n = p_1^{e1} \times ... \times p_k^{ek}}$$

- Gauss e Fermat: **20** cifre decimali
- 1970: **41** cifre decimali con un main frame
- 1977, Rivest: **125** cifre decimali è un calcolo impossibile
- 1994: **129** cifre decimali in 8 mesi con 1.600 workstations
- 2000 (stima): **150** cifre decimali in un anno con una macchina parallela da 10 milioni di dollari
- 2004 (prev.): **300** cifre decimali (1024 bit)
- 2014 (prev.): **450** cifre decimali (1500 bit)

Algoritmi di fattorizzazione

Trial division:
1. i=1
2. individua p(i): i-esimo primo
3. calcola n/p(i)
se ***resto*** **≠ 0**, i = i+1 e goto 2
altrimenti **I° fattore =** ***quoziente***

I° fattore < sqrt(n)
O(exp (½ (log n)))

. . . . .

General Number Field Sieve:
$\mathbf{O(\exp (\log n)^{1/3} . (\log(\log n))^{2/3})}$

Shamir, 2005
Twinkle

Rivest, 1999
scelta casuale

"p, q *strong primes* : p-1, p+1, q–1, q+1 con grandi fattori primi

"$|p-q| > n^{1/2}$ "

1024 – 2048 bit

Altri attacchi a RSA

•**Cycling attack**: se $(((c^e)^e)^e$ .. = c, allora il risultato precedente è m!

•**Timing attack**

•**Message unconcealed:** $m^e = m$

n = 3 × 11 e=3 Φ(n) = 20 d= 7

m	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
$c=m^3$ mod 33	00	01	08	27	31	26	18	13	17	03	10	11	12	19	05	09	04
c^7 mod 33	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16

m	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$c=m^3$ mod 33	29	24	28	14	21	22	23	30	16	20	15	07	02	06	25	32
c^7 mod 33	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Il calcolo di e

$\gcd(\Phi(n),e) = 1; 1<e<\Phi(n)$

Sia $a \in Z_n$. Condizione necessaria e sufficiente per l'esistenza di a^{-1} (l'inverso moltiplicativo di a) è **MCD(n,a) = 1**

Proprietà del MCD(a,b)

•Esiste ed è unico

•Sia $a \geq b$. Se k|a e k|b allora k|r , con **r = a – q.b**
Segue MCD(a,b) = MCD(b,r)

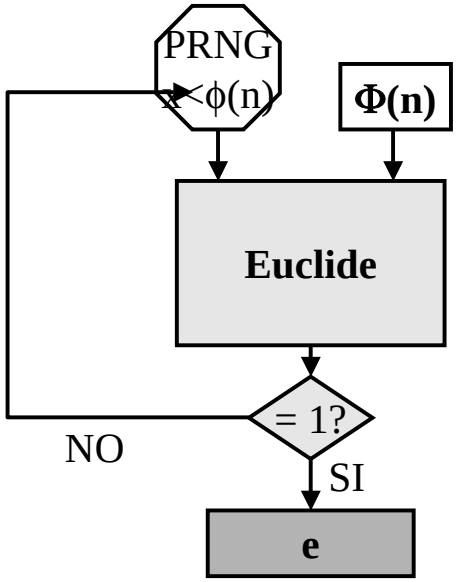
Algoritmo di Euclide

MCD(a,b)
a, b interi positivi;
$a \geq b > 0$
Finché b > 0
    poni r = a mod b
    poni a = b
    poni b = r
Restituisci **a**

$O((\ln n)^2)$

Passo	a	b	r
1	240	42	30
2	42	30	12
3	30	12	6
4	12	6	0
5	**6**	**0**	

$\gcd(\Phi(n),e) = 1;\ 1<e<\Phi(n)$



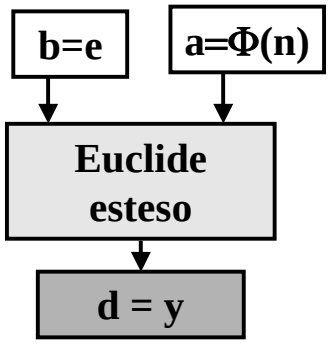
Probabilità [**MCD(x, Φ(n)) =1**]
= Φ(Φ(n)) / Φ(n)

Algoritmo esteso di Euclide

MCD(a,b) = c = x a + y b
a, b interi positivi; $a \geq b > 0$
Poni $x_2 = 1$, $x_1 = 0$, $y_2 = 0$, $y_1 = 1$
Finché b > 0
• calcola $q = \lfloor a/b \rfloor$, $r = a - q.b$
• calcola $x = x_2 - q.x_1$, $y = y_2 - q.y_1$
• poni a= b, b= r,
    $x_2 = x_1$, $x_1 = x$, $y_2 = y_1$, $y_1 = y$
Restituisci **$c = a; x = x_2; y = y_2$**

$O((\ln n)^2)$

$d = e^{-1} \bmod \Phi(n)$
$d\ e + k\ \Phi(n) = 1$

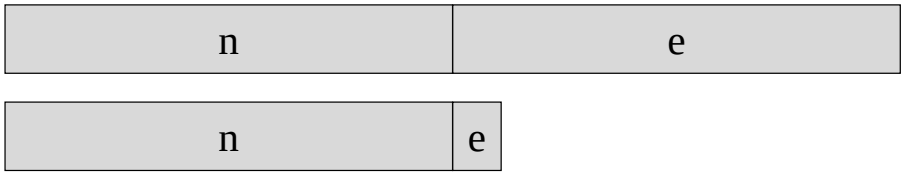


Passo	a	b	x_2	x_1	y_2	y_1	q	r	x	y
1	240	42	1	0	0	1	5	30	1	-5
2	42	30	0	1	1	-5	1	12	-1	6
3	30	12	1	-1	-5	6	2	6	3	-17
4	12	6	-1	3	6	-17	2	0		
5	**6**	**0**		**3**		**-17**				

La scelta di e

N.B. Se il numero binario **e** contiene pochi “uni”
il calcolo di $\mathbf{m^e}$ è più efficiente !

$e = 3$
$e = 2^{16} + 1$
$e = 2^{32} + 1$



T14 (Teorema cinese dei resti): “Se gli interi $\mathbf{n_1, n_2, .., n_k}$ sono a due a due coprimi, allora il sistema di congruenze
$\mathbf{x \equiv a_1 \pmod{n_1}}$,
$\mathbf{x \equiv a_2 \pmod{n_2}}$,
… ,
$\mathbf{x \equiv a_k \pmod{n_k}}$
ha un’unica soluzione modulo $\mathbf{n = n_1 \times n_2 \times \ldots \times n_k}$ **”**.

Conseguenze (nel caso $n_1 = p$, $n_2 = q$ con p,q primi):

- Ogni intero $x < n = p.q$ ha un’unica **rappresentazione modulare**
  $\mathbf{v(x) = (v_1, v_2) = (x \bmod p, x \bmod q)}$
- Somme e moltiplicazioni modulari possono essere fatte vantaggiosamente sulla rappresentazione modulare degli operandi
- Esistono algoritmi facili (Gauss, Garner) per ripristinare la rappresentazione originaria dell’intero

Decifrazione con CRT

1. *Rappresentazione modulare di* **c** :
   v(c) = (c mod p, c mod q)
2. *Calcolo della rappresentazione modulare di* $\mathbf{c^d \bmod n}$:
   $\mathbf{v^d(c) = ((c \bmod p)^d \bmod p, (c \bmod q)^d \bmod q)}$

N.B: numeri di dimensione più piccola (½ log n)

3. *Ripristino della rappresentazione usuale di* **m** (Gauss):

$$\mathbf{m = c^d \bmod n}$$
$$\mathbf{= \{a\times[(c \bmod p)^d \bmod p] + b\times[(c \bmod q)^d \bmod q]\} \bmod n}$$

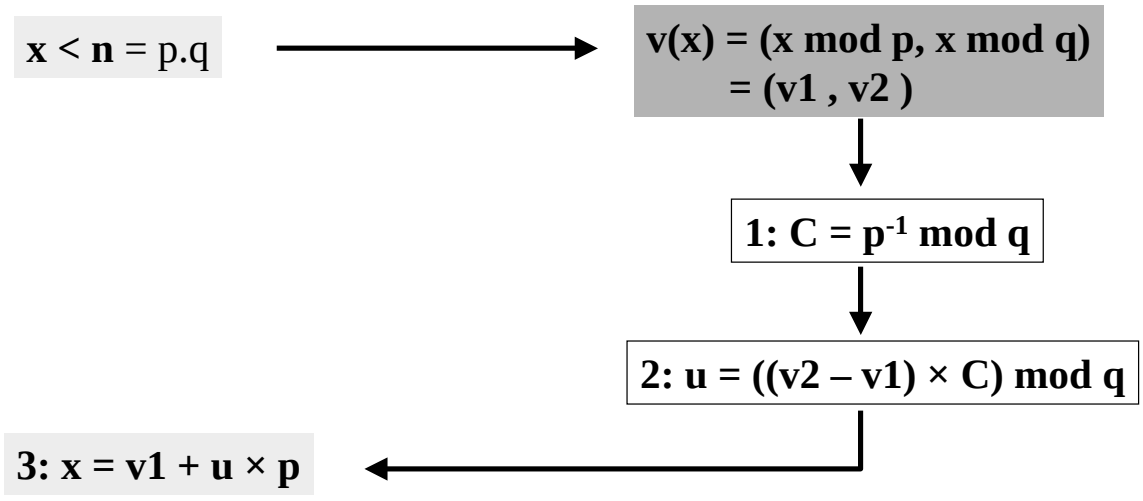
Per **T14** **a, b** devono soddisfare le congruenze

$\mathbf{a \equiv 1 \pmod p}$ $\qquad$ $\mathbf{b \equiv 0 \pmod p}$

$\mathbf{a \equiv 0 \pmod q}$ $\qquad$ $\mathbf{b \equiv 1 \pmod q}$

Circa quattro volte più veloce
Ancora più efficiente se n è il prodotto di più di due primi (PKCS#1)

Algoritmo e Formula di Garner



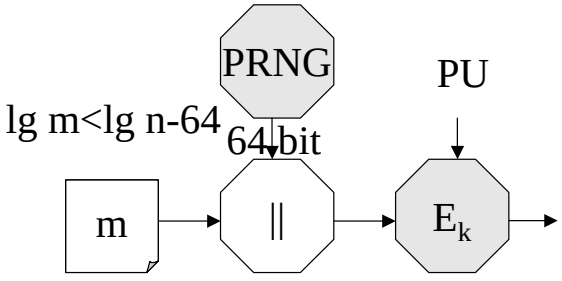
Efficienza di RSA

- **x < n**
- **x^e mod n $\rightarrow$ e con solo due "uni"**
- **x^d mod n $\rightarrow$ CRT**

Randomizzazione di RSA

RSA esegue una sostituzione semplice di blocchi ed è deterministico:
1- **m** identici generano **c** identici
2 - per certi **m** si ha **c = m**

Standard PKCS#1



Altri problemi difficili

P4: problema del fusto - Dato un insieme di **n** interi positivi

$$\{a_1, a_2, .., a_n\}$$

ed un intero positivo **s** determinare se esiste o meno un sottoinsieme di a_j la cui somma è **s**.
Cifrario di Merkle-Hellman, Cifrario di Chor-Rivest

P5: problema della radice quadrata modulare - Dato un **n** composto ed un elemento $a \in Q_n$ (insieme dei residui quadratici modulo n) trovare la sua radice quadrata modulo n, cioè
un intero $x \in Z^*_n$ tale che $x^2 \equiv a \pmod n$.
Cifrario di Rabin

P6: problema della residuosità quadratica - Dato un **n** composto e dispari ed un elemento $a \in J_p$ (insieme degli interi con simbolo di Jacobi = 1) determinare se **a** è o meno un residuo quadratico modulo **n**.
Cifrario di Goldwasser-Micali

Logaritmo discreto su curva ellittica

P7: problema del logaritmo discreto su una curva ellittica - Data la curva ellittica formata da punti le cui coordinate x,y soddisfano l'equazione

$$y^2 = x^3 + ax + b \mod p$$, con p primo,

e dati due suoi punti **P**, **Q** tali che $Q = n \times P$,

determinare **n**.

Complessità degli attuali algoritmi di rottura
$O(\exp(\frac{1}{2}(\log p)))$
160-180 bit

ECC(Ellipltical Curve Cryptography)
Certicom.com