

$$200 \cdot 32 = 80^2$$

$$41^2 \cdot 43^2 \equiv 80^2 \pmod{1649}$$

$$[(42-1)(42+1)]^2 \equiv 80^2$$

$$(42^2 - 1)^2 = 80^2$$

$$174^2 \equiv 80^2$$

$$(174 - 80)(174 + 80) \vdots 1649$$

$$34 \cdot 194 \vdots 1649$$

$$17 \cdot 97 \vdots 1649$$

$$1649 = 17 \cdot 97$$

Fern:

$$1. \text{ Den } n = \prod_{i=1}^k p_i^{\alpha_i} \quad a^{p_i} \equiv a \pmod{p_i} \quad \forall p_i, \text{ da } a^n \equiv a \pmod{n}$$

$$\text{Gilt für alle } a^{p_i} \equiv a \pmod{p_i}$$

$$\text{ptim für } n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$\cancel{a^{p_i} \equiv a \pmod{p_i}} \Rightarrow a^{p_i} - a \equiv 0 \pmod{p_i}$$
$$\Rightarrow p_i \mid (a^{p_i} - a)$$

$$a^{p_i} - a \equiv 0 \pmod{p_i}$$

$$a^n \equiv a \pmod{p_i} \Rightarrow a^n - a \equiv 0 \pmod{p_i} \Rightarrow$$

$$\Rightarrow p_i \mid (a^n - a) \quad \left| \begin{array}{l} p_i \mid n \\ \text{d.h. } \varphi(p_i) \neq 1 \end{array} \right. \Rightarrow$$

$\rightarrow a^n \equiv a \pmod{p_i}$

T.C.R.

(Teorema chineză a resturilor)

$p_i^{x_i}$ sunt coprime între

$$1428 \Rightarrow a^n \equiv 1 \pmod{p_i^{x_i}} \quad \forall i \Rightarrow a^n \equiv 1 \pmod{n}$$

2. $a^n \equiv 1 \pmod{n}$ a prime num

$$1428 = 2 \cdot 13 \cdot 19$$

prim prim prim

$$\begin{array}{c|cc} 1428 & 7 \\ \hline 2 & 13 \\ 13 & 19 \\ \hline 1 & \end{array}$$

Korselt's criterion?

Un întreg număr pozitiv n este ~~un~~ număr Carmichael dă și numai dacă n este față patrat și pt toate divizorii primi p de n, este adevărat că $(p-1) | (n-1)$

Din teorema \Rightarrow toate numerele Carmichael sunt impare

în F mCarmichael nu există 2 divizori primi

(Wikipedia)

Ex: $561 = 3 \cdot 11 \cdot 17$

$$2 | 560$$

$$11 | 560$$

$$17 | 560$$

$1428 = 2 \cdot 13 \cdot 19$

$$\begin{array}{r} 1428 \\ -12 \\ \hline 52 \\ -48 \\ \hline 4 \\ -4 \\ \hline 0 \end{array} \quad 1428 : 6 = 288$$

$$1\cancel{2}8 : 12 = 144$$

$$\begin{array}{r} 12 \\ \overline{)52} \\ 48 \\ \hline 48 \\ \hline 0 \end{array}$$

$$1\cancel{2}8 : 18 = 96$$

$$\begin{array}{r} 162 \\ \overline{)108} \\ 108 \\ \hline 0 \end{array}$$

$$10585 = 5 \cdot 29 \cdot \cancel{73}$$

~~$$\begin{array}{r} 10585 \\ 2114 \\ \hline 73 \\ \hline 14 \\ \hline 14 \\ \hline 0 \end{array}$$~~

~~$$\begin{array}{r} 10585 \\ \hline 10585 \end{array}$$~~

$$10584 : 4 = 2646$$

$$\begin{array}{r} 8 \\ \hline 25 \\ 14 \\ \hline 18 \\ 16 \\ \hline 24 \\ 24 \\ \hline 0 \end{array}$$

$$10584 : 28 = 378$$

$$\begin{array}{r} 84 \\ \hline 298 \\ 196 \\ \hline 224 \\ 224 \\ \hline 0 \end{array}$$

$$10584 : 72 = 147$$

$$\begin{array}{r} 72 \\ \hline 338 \\ 28 \\ \hline 504 \\ 504 \\ \hline 0 \end{array}$$

~~$$\cancel{73}$$~~

$$\cancel{75361} = 11 \cdot \cancel{73} \cdot 1431$$

~~$$\begin{array}{r} 75361 \\ 6851 \\ \hline 527 \\ 31 \\ \hline 1 \end{array}$$~~

$$45360 : 10 = 4536$$

$$45360 : 12 = 6280$$

$$\begin{array}{r} 72 \\ \underline{-53} \\ 24 \\ \underline{-96} \\ 0 \\ \underline{0} \\ = \end{array}$$

$$45360 : 16 = 4710$$

$$\begin{array}{r} 64 \\ \underline{113} \\ 112 \\ \underline{-16} \\ 16 \\ \underline{-16} \\ 0 \\ \underline{0} \\ = \end{array}$$

$$45360 : 30 = 2512$$

$$\begin{array}{r} 60 \\ \underline{153} \\ 150 \\ \underline{-30} \\ 30 \\ \underline{-30} \\ 0 \\ \underline{0} \\ = \end{array}$$

3. $2^n - 1$ prim $\Rightarrow n$ este prim

$$\cancel{2^n \not\equiv 1 \pmod{n}}$$

$$\text{Pf } n \text{ compus} \Rightarrow n = a \cdot b$$

~~bie f~~ $2^a - 1 \Rightarrow 2^{ab} - 1 \Rightarrow 2^a - 1$ are divizori diferiti
de 1 primi insupri $\Rightarrow n$ nu este prim

Pf $n = ab$ ~~bie f~~ $a, b \geq 1$ nu este prim

$$2^n - 1 = 2^{ab} - 1$$

$$2^{ab} - 1 = (2^a - 1) \underbrace{(2^{a(b-1)} + 2^{a(b-2)} + \dots + 2^a + 1)}_{(*)}$$

$\Rightarrow 2^{ab} - 1$ nu este prim pt 2 factori > 1

$$2^a - 1 \geq 3$$

$$(*) > 1$$

\Rightarrow contradicție \Rightarrow

$\Rightarrow n$ trebuie să fie prim

4. Dacă sunt 2 numere prime p și q se va scrie

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

$\left(\frac{p}{q}\right)$ simbolul Legendre

$$\text{Dacă } \exists x \text{ astfel că } x^2 \equiv p \pmod{q}$$

p și q sunt impare

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & b \equiv x^2 \pmod{p} \text{ - rest patratic} \\ -1 & b \not\equiv x^2 \pmod{p} \text{ - rest nepatratic} \\ 0 & p/a \end{cases}$$

$$\frac{(p-1)(q-1)}{4} \text{ întreg} \Rightarrow p-1 \text{ și } q-1 \text{ sunt pară} \rightarrow \begin{cases} p-1 \\ q-1 \end{cases} \text{ pară}$$

~~(*)~~

\exists prim impar

$$P \cdot 1, P^{-2}, \dots, P \cdot \left[\frac{q-1}{2} \right] \bmod q$$

Fiecare dintre acestea valori mod q are rest $[1, q-1] \rightarrow$

$$\Rightarrow \left[-\frac{q-1}{2}, -\frac{q-1}{2} \right]$$

Notăm $N(P, q)$ nr de resturi negative

T. Gauss

$$\left(\frac{P}{q} \right) = (-1)^{N(P, q)} \Rightarrow \left(\frac{q}{P} \right) = (-1)^{N(q, P)}$$

$$N(P, q) + N(q, P) = \frac{(P-1)(q-1)}{4} \Rightarrow$$

$$\Rightarrow (-1)^{N(P, q)} = (-1)^{\frac{(P-1)(q-1)}{4}} \cdot (-1)^{N(q, P)} \Rightarrow$$

T. Gauss

$$\left(\frac{P}{q} \right) = (-1)^{N(P, q)} = (-1)^{\frac{(P-1)(q-1)}{4}} \cdot \left(\frac{q}{P} \right)$$

tit
tit

8. Simbolul lui Kronecker $\left(\frac{a}{b} \right)$ este o funcție definită pentru a, b întregi și $b \neq 0$. Acesta are următoarele valori, în funcție de a și b:

1. $\left(\frac{a}{b} \right) = 1$ dacă a este divizibil cu b sau $a=b$

2. $\left(\frac{a}{b} \right) = 0$ dacă $b=0$

3. $\left(\frac{a}{b} \right) = -1$ în alte cazuri

9. #31

$$b=2$$

$$2^{\frac{431-1}{2}} = \left(\frac{2}{431}\right) \pmod{431}$$

$$2^{\frac{430}{2}} = 2^{365} = 2^5 \cdot 2^{43} = 2^5 \cdot 2^{70} \cdot 2^3$$

$$\begin{aligned}2^2 &= 4 \\2^4 &= 16 \\2^8 &= 256 \\2 & \\2^5 &= 32 \\2^3 &= 8 \\2^{10} &= 1024 \\2^4 &= 128 \\2^7 \cdot 2^3 &= 2^{10} = 253\end{aligned}$$

$$32 \cdot 253 = 9344 \pmod{431} \Rightarrow 604$$

$$604 \cdot 253 = 146942 \Rightarrow 40$$

$$2^{365} = 2^{360} \cdot 2^5$$

$$= 2^{10} \cdot 2^{30} \cdot 2^5 \cdot 2^{70} \cdot 2^3$$

~~2^53~~

~~(2^2)~~

$$2^2 = 4$$

$$2^4 = 16$$

$$2^8 = 256$$

$$2^{10} = 1024 = 293$$

$$(2^{10})^{36} = 293^{36}$$

$$(293^2)^{18} = 85849^{18} = 322^{78}$$

$$\Rightarrow (322^2)^9 = 103.684^9 \leq 693^9$$

$$2^{365} \bmod 731 = 389$$

$$\left(\frac{2}{731} \right) = (-1) \cdot \frac{1 \cdot \frac{730}{4}}{\frac{731}{2}} \cdot \left(\frac{731}{2} \right)$$

~~$\frac{730}{4}$~~
 ~~$\frac{731}{2}$~~

$$= (-1)^{\frac{365}{2}} \cdot \left[\frac{731}{2} \right]$$

$$\lambda = 3$$

$$3^{365} \bmod 731 = 233$$

$$\left(\frac{3}{731} \right) = (-1) \cdot \frac{2 \cdot \frac{730}{4}}{\frac{731}{3}} \cdot \left(\frac{731}{3} \right) = \left(\frac{731}{3} \right)$$

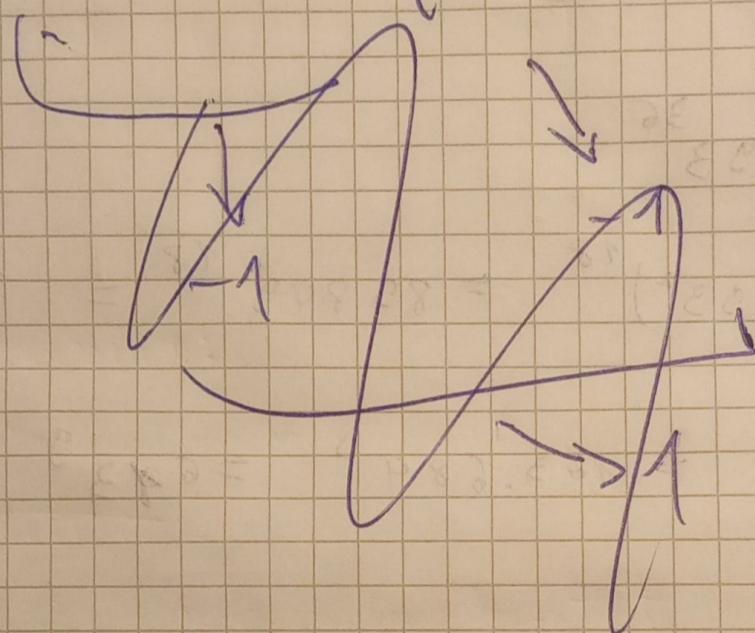
$$b_1 = 2$$

$$b_2 = 3$$

$$b_3 = 5$$

$$\left(\frac{2}{731} \right) = (-1) \cdot \frac{\cancel{730}}{4} \cdot \left(\frac{731}{2} \right) = -1$$

10



$$\left(\frac{3}{731} \right) = \underbrace{(-1)}_{-1} \cdot \frac{2 \cdot \cancel{730}}{4} \cdot \underbrace{\left(\frac{731}{3} \right)}_{-1} = 1$$

$$\left(\frac{5}{731} \right) = \underbrace{(-1)}_{\rightarrow 1} \cdot \frac{4 \cdot \cancel{730}}{4} \cdot \left(\frac{731}{5} \right) \downarrow \underbrace{-1}_{-1} = -1$$

$$2^{365} \pmod{731} = 389$$

$$3^{365} \pmod{731} = 233$$

$$5^{365} \pmod{731} = 632$$

$$389 \equiv -1 \pmod{731} \rightarrow n \text{ complex}$$

$$233 \equiv 1 \pmod{731} \rightarrow n \text{ complex}$$

$$632 \equiv -1 \pmod{731} \rightarrow n \text{ complex}$$

$\Rightarrow n \text{ complex}$

$$24) 10349$$

$$\sqrt{10349} \approx 102$$

$$x = \lceil \sqrt{10349} \rceil = 102$$

$$102^2 = 10404 \geq 10349$$

$$x^2 - n \Rightarrow 102^2 - 10349 = 10404 - 10349 = 55$$

$$55$$

nu este patrat perfect \Rightarrow

nu am gasit factori

$$x = 103 \Leftrightarrow$$

$$x^2 - n \Rightarrow 103^2 - 10349 = 10609 - 10349 = 260$$

260 nu este patrat perfect

$$x = 104 \Rightarrow$$

$$x^2 - n = 104^2 - 10349 = 10816 - 10349 = 467$$

467 nu este patrat perfect

~~t~~ $t = 105$

~~t~~

$$t^2 - n = 105^2 - 10349 = 11025 - 10349 = 676$$

$$n^2 = 676 \Rightarrow n = 26$$

nătrat
perfec

$$10349 = (105-26)(105+26) = 79 \cdot 131$$

71

Impărtirea succesiivă:

Tip: determinist, necondiționat

~~Complexitate~~

Avantaje: Simplu de implementat și oferă rezultat corect.

Dezavantaje: Pentru numere mari, algoritmul poate dura lung datorită numărului mare de impărtiri succesiive.

Fermat:

Tip: probabilistic, necondiționat

Avantaje: Test mai rapid decât algoritm de impărtire succesiivă.

Toate fi utilizat pt numere mari.

Dezavantaje: Are o prob. de eroare, mai ales în cazul numerelor primice.

Miller-Rabin:

Tip: probabilistic, necondiționat

Avantaje: Este mai eficient de către Fermat pt numere mari și are o probabilitate de eroare foarte scăzută.

Dezavantaje: Prob de eroare este foarte mică, nu este 100% sigură.

Lovitură - Uzură

Tip: probabilistic, recondiționat

Avantaje: Eficient și nu morți și are o probă mică de eroare

Deavantaje: Necesită calculul simbolului Jacobian și posibilitatea eroarei.

$$12 \quad f(x) = x^2 + 1 \pmod{n}$$

10909

$$x_0 = 2$$

$$f(x) = x^2 + 1 \pmod{10909}$$

$$x_1 = f(x_0) = (x_0^2 + 1) \pmod{10909} = 2^2 + 1 = 5$$

$$x_2 = f(x_1) = (x_1^2 + 1) = 26$$

$$x_3 = 26^2 + 1 = 677$$

$$x_4 = 677^2 + 1 = 4545$$

~~$x_5 = 6282451$~~

~~$x_6 = 6282$~~

~~$x_7 = 5801$~~

~~$\text{gcd}(677^5, 10909) = \text{gcd}(672, 10909)$~~

~~$\text{gcd}(572, 10909) = \text{gcd}(3, 10909) = 1$~~

$$(x_2 - x_0, n) = (26 - 2, 10909) = (24, 10909) = 1$$

$$(677^2, 10909) = (675, 10909) = 1$$

$$(4545^2, 10909) = (4544, 10909) = 1$$

$$(2451^2, 10909) = 1$$

$$(2134^2, 10909) = (2132, 10909) = 1$$

$$(3967^2, 10909) = (3965, 10909) = 1$$

$$x_8 = 3967^2 + 1 \Rightarrow 9704$$

$$(9704 - 2, 10909) = (9702, 10909) = 1$$

$$x_9 = 9704^2 + 1 \Rightarrow 5988$$

$$(5988 - 2, 10909) = (5986, 10909) = 1$$

$$x_{10} = 5988^2 + 1 \Rightarrow 3540$$

$$(3540 - 2, 10909) = (3538, 10909) = 1$$