Arithmétique pour la crypto

1 Complexité

$T(n) = O(f(n)) \iff \exists c > 0,\ T(n) < c\, f(n)$

$O(1) < O(\log n) < O(n) < O(n \log n)$
$< O(n^2) < O(n^3) < O(2^n) < O(n!)$

IMBRIQUÉES $\times$ SUCCESSIVES $+$

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \qquad \sum_{i=1}^{n} (2i+1) = n^2 + 2n$$

$$\sum_{i=1}^{n^2} i = \frac{n^2(n^2+1)}{2} = O(n^4)$$

$t \leftarrow 2t$ jusqu'à $m \ \Rightarrow\ \log_2 m$ tours

`if` $n < 100\ B$ `else` $n \times C \ \Rightarrow\ T = T_A + n\, T_C$

chiffres(k bits) $= \lfloor k \log_{10} 2 \rfloor + 1 \qquad \log_{10} 2 \approx 0{,}301$

$t = \dfrac{\text{nb d'opérations}}{10^9 \text{ op/s}} \qquad 1 \text{ an} \approx 3{,}15 \times 10^7 \text{ s}$

$+\ O(n) \quad \times\ O(n^2) \quad \text{pgcd}\ O(n^3) \quad \text{primalité}\ O(n^6)$

factorisation $O\left(e^{\left(\frac{64}{3} k (\ln k)^2\right)^{1/3}}\right)$

Shor $O\big((\ln N)^3\big), \quad \ln N = k \ln 2$

$P \subset NP$

2 Division · PGCD · PPCM

$a = bq + r, \qquad 0 \le r < |b|$

$d \mid a,\ d \mid b \ \Rightarrow\ d \mid \alpha a + \beta b$

$\text{pgcd}(a, b) = \text{pgcd}(b, r)$

$\text{ppcm}(a, b) \times \text{pgcd}(a, b) = |ab|$

$\text{pgcd}(ac, bc) = c \cdot \text{pgcd}(a, b)$

$d = \text{pgcd}(a, b) \iff a = da',\ b = db',\ \text{pgcd}(a', b') = 1$

$\text{pgcd} = \prod p_i^{\min(\alpha_i, \beta_i)} \qquad \text{ppcm} = \prod p_i^{\max(\alpha_i, \beta_i)}$

n premier ? diviseurs $\le \sqrt{n} \qquad \pi(n) \sim \dfrac{n}{\ln n}$

3 Bézout · Euclide étendu

$\text{pgcd}(a, b) = 1 \iff \exists u, v :\ au + bv = 1$

$\text{pgcd}(a, b) = d \ \Rightarrow\ \exists u, v :\ au + bv = d$

$$u = 1,\ u' = 0,\ v = 0,\ v' = 1$$
$$a \leftarrow b, \quad b \leftarrow r$$
$$u \leftarrow u', \quad u' \leftarrow u - q\,u'$$
$$v \leftarrow v', \quad v' \leftarrow v - q\,v'$$

$b = 0 :\ (d, u, v) = (a, u, v)$

$r = 0 :\ (d, u, v) = (b, u', v')$

4 Gauss · Diophantiennes

$a \mid bc,\ \text{pgcd}(a, b) = 1 \ \Rightarrow\ a \mid c$

$a \mid n,\ b \mid n,\ \text{pgcd}(a, b) = 1 \ \Rightarrow\ ab \mid n$

p premier, $p \mid bc \ \Rightarrow\ p \mid b$ ou $p \mid c$

$ax + by = c, \quad d = \text{pgcd}(a, b)$

$d \nmid c \ \Rightarrow\ S = \varnothing$

$a'x + b'y = c' \quad \left(a' = \frac{a}{d},\ b' = \frac{b}{d},\ c' = \frac{c}{d}\right)$

$a'u + b'v = 1 \ \Rightarrow\ (x_0, y_0) = (c'u,\ c'v)$

$$x = x_0 + b'k, \qquad y = y_0 - a'k, \qquad k \in \mathbb{Z}$$

$ax - by = c :\quad x = x_0 + bk,\ \ y = y_0 + ak$

5 Congruences · Inverse mod n

$a \equiv b\ [n] \iff n \mid a - b \iff a = b + kn$

$a \equiv u,\ b \equiv v\ [n] \ \Rightarrow\ a + b \equiv u + v$

$ab \equiv uv, \qquad a^k \equiv u^k$

$10 \equiv 1\ [3], [9] \qquad 10 \equiv -1\ [11]$

$$a^{-1}\ [n] \text{ existe} \iff \text{pgcd}(a, n) = 1$$

$au + nv = 1 \ \Rightarrow\ a^{-1} \equiv u\ (+n \text{ si } u < 0)$

$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ (p premier)

$ax + b \equiv y\ [n] \ \Rightarrow\ x \equiv a^{-1}(y - b)\ [n]$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \equiv (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\ [n]$$

$y = x + k \quad y = ax + b \quad Y = MX\ [n]$

6 Restes chinois

$\text{pgcd}(m_i, m_j) = 1,\ \ i \neq j$

$x \equiv a\ [m],\ x \equiv a\ [n] \iff x \equiv a\ [mn]$

$x \equiv a\,n\,u + b\,m\,v\ \ [mn], \quad u = n^{-1}\ [m],\ v = m^{-1}\ [n]$

$$x \equiv \sum_{i=1}^{k} a_i M_i y_i\ \ [M]$$
$$M = m_1 \cdots m_k, \quad M_i = \frac{M}{m_i}, \quad y_i = M_i^{-1}\ [m_i]$$

$x = x_0 + Mk,\ k \in \mathbb{Z}$