Rappels d'arithmétique :

sandra.marcello@epita.fr

Sandra Marcello

11 février 2022

Plan

Nombres premiers

Definition

Un entier $n \in \mathbb{N}$ est dit "premier" s'il posséde exactement deux diviseurs , 1 et lui-méme.
Notons $\mathcal{P}$ l'ensemble des nombres premiers.

Theorem (Théoréme Fondamental)

Soit $n \in \mathbb{N}^*$. Alors n se décompose de faÃ§on unique sous la forme

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

avec $k \in \mathbb{N}^*$, $p_i \in \mathcal{P}$,$\alpha_i \in \mathbb{N}^*$ pour $1 \leq i \leq k$.

PGCD

Definition

Soit a, b deux entiers naturels dont un au moins est non nul.
L'ensemble des entiers de $\mathbb{N}*$ diviseurs communs é a et b admet un plus grand élément noté δ. C'est le Plus Grand Commun Diviseur de a et b.
Notation : $\delta = PGCD(a, b) = a \wedge b$.

Theorem (Théoréme d'Euclide)

Soient a, b deux entiers relatifs non nuls.
Si $a = bq + r$ est la division euclidienne de a par b alors :

$$a \wedge b = b \wedge r.$$

Algorithme d'Euclide

1. Posons $r_0 = a$ et $r_1 = b$
2. Construction d'une suite (r_k) strictement décroissante de "restes" de division euclidienne. Tant que $r_k \neq 0$, réaliser la division euclidienne de r_{k-1} par r_k et nommer r_{k+1} le nouveau reste obtenu.
$$r_k = r_k q_k + r_{k+1}.$$
3. D'aprés le théoréme d'Euclide $r_{k-1} \wedge r_k = r_k \wedge r_{k+1}$. $Or(r_k)$ est une suite d'entiers naturels strictement décroissante donc il existe un rang n tel que $r_n \neq 0$ et $r_{n+1} = 0$.
4. Ainsi $a \wedge b = r_{n-1} \wedge r_n$ et $r_n \mid r_{n-1}$ donc $a \wedge b = r_n$

Application : Implémentation de l'algorithme d'Euclide.

Théoréme de Bezout

Theorem (théoréme de Bezout)

Soient a et b deux entiers relatifs non nuls. Il existe (u, v) entiers relatifs tel que :

$$au + bv = a \wedge b.$$

Utilisation lorsque a et b sont premiers entre eux, alors u est l'inverse modulaire de a idem pour v et b.

Algorithme d'Euclide étendu

Algorithme d'Euclide étendu : Soient a, b deux entiers relatifs non nuls tels que $a \wedge b = \delta$.

1. Appliquer l'algorithme d'Euclide é a et b. Construction des suites (r_n) et (q_n) telles que $r_0 = a$, $r_1 = b$ et $r_n = q_{n+1} r_{n+1} + r_{n+2}$ avec $0 < r_{n+1} < r_n$. Notons $r_{n_0} = \delta$ le dernier terme non nul de la suite (r_n).
2. Chercher des suites (u_n) et (v_n) telles que $r_n = u_n a + v_n b$ pour $1 \leq n \leq n_0$. Les suites suivantes conviennent $u_0 = 1, u_1 = 0$ et $v_0 = 0, v_1 = 1$

$$u_{n+2} = u_n - q_{n+1} u_{n+1}, v_{n+2} = v_n - q_{n+1} v_{n+1}.$$

3. Les coefficients de Bezout sont donc (u_{n_0}) et (v_{n_0}).

Applications de l'algorithme d'Euclide étendu

Inversion modulaire :$x^{-1}[n]$

- $\exists u, n \in \mathbb{Z}$ tel que $xu + nv = x \wedge n = 1$

Anneau $\mathbb{Z}/n\mathbb{Z}$

Theorem

Soit n un entier naturel non nul $(\mathbb{Z}_n, +, .)$ *est un anneau commutatif.*

Notons $\mathbb{Z}_n^*$ l'ensemble des éléments inversibles pour la loi "." de $\mathbb{Z}_n$.

Inversibles de l'anneau $\mathbb{Z}_n$

- Si p est un nombre premier $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.
- Si n n'est pas un nombre premier (th de Bezout) :l'ensemble des inversibles est égal é l'ensemble des éléments de $\mathbb{Z}_n$ premiers avec n.
- Lorsque p est premier l'ensemble des élémenzs inversibles est un corps.

Ordre du groupe des $\mathbb{Z}/n\mathbb{Z}^*$

- Soit $n \in \mathbb{N}$ alors l'ordre du groupe $\mathbb{Z}/n\mathbb{Z}$ est $\phi(n)$ ou ϕ est la fonction d'Euler.

Lemma

Soit $n \in \mathbb{N}$ avec $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ avec p_i premier et $\alpha_i \in \mathbb{N}^*$ pour $1 \leq i \leq k$. Alors,

$$\phi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

Theorem (Lagrange)

Soit G un groupe multiplicatif d'ordre n alors $\forall g \in G$:

$$g^n = 1.$$

Arithmétique modulaire

Theorem (Euler)

Soit $n \in \mathbb{N}$, $\forall a \in (\mathbb{Z}/n\mathbb{Z})^{ast}$ *:*

$$a^{\phi(n)} \equiv 1[n].$$

Definition

Soit $(G, .)$ un groupe multiplicatif d'ordre n. Un élément g de G est dit primitif si $G = (g, g^2, \cdots, g^{n-1}, g^n)$.

Soit p un nombre premier. Dans $(\mathbb{Z}/p\mathbb{Z})^*$ tout élément différent de 1 est primitif.

Théoréme du reste chinois

Question : Soit p et q deux nombres premiers, a, b deux entiers fixés. Trouver $x \in \mathbb{N}$ tel que

$$x \equiv a[p],$$

$$x \equiv b[q].$$

Théoréme du reste chinois

Theorem (Théoréme des restes chinois (CRT))

Soient $p, q \in \mathbb{N}$ *deux nombres premiers, soient* $a, b \in \mathbb{N}$.
$\exists! x \in (\mathbb{Z}/pq\mathbb{Z})$ *tel que :*

$$x \equiv a[p],$$

$$x \equiv b[q].$$

De plus,

$$x = aq\left(q^{-1}[p]\right) + bp\left(p^{-1}[q]\right)[pq].$$

Preuve : utilisation algorithme Euclide étendu.