MathComp - Algèbre Arithmétique

Pierre-Alain Fouque

Université de Rennes 1

Septembre 2020

Agenda

1. Plus grand commun diviseur
2. Algorithme Euclide
3. Nombres premiers
4. Numération en base b
5. Théorème des restes chinois
6. Fonction indicatrice d'Euler
7. Théorème d'Euler
8. Groupes cycliques
9. Le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$ où p est premier impair

Division euclidienne

Proposition (Division euclidienne)

Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. *Il existe un unique* $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ *tq*

$$a = bq + r \text{ et } 0 \leq r < |b|.$$

q, r *est le quotient, reste de la division euclidienne de* a *par* b.

Lemme

Soit H *un sous-groupe de* $\mathbb{Z}$. *Il existe un unique* $n \in \mathbb{N}$ *tq* $H = n\mathbb{Z}$.

Example

Soient a et b des entiers relatifs non tous les deux nuls. L'ensemble $a\mathbb{Z} + b\mathbb{Z} = \{au + bv : u, v \in \mathbb{Z}\}$, est un sous-groupe de $\mathbb{Z}$. Il existe donc un unique entier $d \geq 1$ tq $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Plus grand commun diviseur

Definition

L'entier d s'appelle le plus grand commun diviseur de a et b, ou en abrégé le pgcd de a et b, noté $d = \gcd(a, b)$.

Propriété de Bézout

Il existe des entiers relatifs u et v tq $d = au + bv$.

Lemme

Le pgcd de a et b est l'unique entier naturel satisfaisant :

1. *c'est un diviseur de a et b.*
2. *Il est multiple de tout diviseur commun de a et b.*

Definition

a et b premiers entre eux (a est premier avec b), si $\gcd(a, b) = 1$.

Plus grand commun diviseur

Lemme

a et b sont premiers entre eux ssi $\exists\ (u, v) \in \mathbb{Z}^2$ *tq* $au + bv = 1$.

Corollary

Les entiers $\frac{a}{d}$ *et* $\frac{b}{d}$ *sont premiers entre eux.*

Corollary (Théorème de Gauss.)

Soit c un entier relatif tq a divise bc et a premier avec b. Alors a divise c.

Plus petit commun multiple

Definition

Étant donnés des entiers relatifs a et b non nuls, l'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. L'entier naturel m tel que

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$$

s'appelle le plus petit commun multiple de a et b.

Proposition

$$\gcd(a, b)\,\mathrm{lcm}(a, b) = |ab|.$$

Algorithme Euclide (Calcul du pgcd)

Definition

Construire une suite finie d'entiers naturels $(r_i)_{i\geq 0}$, appelée la suite des restes (associée à a et b), par le procédé suivant : on pose

$$r_0 = a \text{ et } r_1 = b.$$

Soit $r_0, r_1, \cdots, r_i$ où $i \geq 1$. Si $r_i \neq 0$, r_{i+1} est le reste de la division euclidienne de r_{i-1} par r_i. Si $r_i = 0$, le procédé s'arrête et la suite des restes est $r_0, r_1, \cdots, r_{i-1}, r_i$. Il existe un unique entier $n \geq 1$ tq :

$$0 < r_n < r_{n-1} < \ldots < r_1 < r_0 \text{ et } r_{n+1} = 0.$$

Proposition

$$r_n = \gcd(a, b).$$

Calcul Relation de Bézout

Definition

Deux suites d'entiers $(u_i)_{0\leq i\leq n}$ et $(v_i)_{0\leq i\leq n}$ tq

$$u_0 = 1, u_1 = 0 \text{ et } v_0 = 0, v_1 = 1,$$

$u_{i+1} = u_{i-1} - u_i q_i$ et $v_{i+1} = v_{i-1} - v_i q_i$ pour tout $i = 1, \ldots, n-1$,

où q_i est le quotient de la division euclidienne de r_{i-1} par r_i.

Proposition

$$r_n = au_n + bv_n$$

Theorem (Complexité)

$$n \leq \frac{3}{2\log 2} \log b + 1$$

Complexité

Definition (Suite de Fibonacci)

$$U_0 = 0, U_1 = 1 \text{ et } U_{k+1} = U_k + U_{k-1} \text{ pour } k \geq 1.$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k = \begin{pmatrix} U_{k+1} & U_k \\ U_k & U_{k-1} \end{pmatrix}.$$

Proposition (U_k et U_{k+1} sont premiers entre eux)

$$U_{k+1}U_{k-1} - U_k^2 = (-1)^k$$

Proposition (Lamé, 1845)

$$a \geq dU_{n+2} \text{ et } b \geq dU_{n+1}$$

Nombres premiers

Definition (Nombre premier)

Tout entier $p \geq 2$ dont les seuls diviseurs positifs sont 1 et p.

Lemme

Soit p un entier ≥ 2. Alors, p est premier ssi p n'est pas le produit de deux entiers strictement plus grands que 1.

Corollary (Euclide)

L'ensemble des nombres premiers est infini.

Lemme (Lemme d'Euclide)

Soient a, b entiers naturels et p un nombre premier tq p divise ab. Alors, p divise l'un des entiers a et b.

Théorème fondamental de l'arithmétique

Theorem

Tout entier $n \geq 2$ s'écrit de façon unique sous la forme

$$n = p_1^{n_1} \dots p_r^{n_r},$$

où les n_i sont des entiers naturels non nuls, et les p_i sont des nombres premiers vérifiant $p_{i-1} < p_i$ pour tout $i = 2, \dots, r$, appelée décomposition de n en produit de nombres premiers

Theorem ($\pi(x)$: Nombre de nombres premiers $\leq x$ - $\pi(x) \simeq \frac{x}{\log x}$)

Pour tout nombre réel $x \geq 2$, on a

$$\left(\frac{\log 2}{2}\right)\frac{x}{\log x} \leq \pi(x) \leq (9 \log 2)\frac{x}{\log x}.$$

Numération en base $b \geq 2$

Theorem

Soit x un entier naturel non nul. On peut écrire x de manière unique sous la forme

$$x = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0$$

où $n \in \mathbb{N}$, $a_0, \ldots, a_n \in \mathbb{N}$ tq $0 \leq a_i \leq b-1$ et a_n est non nul.
$x = a_n a_{n-1} \ldots a_1 a_0$: écriture de x en base b et $x = (a_n \cdots a_0)_b$.

Theorem (Exponentiation rapide)

On peut calculer rapidement x^n en $O(\log n)$ multiplications

Théorème des restes chinois

Theorem

Soient m et n des entiers naturels non nuls premiers entre eux.

$$f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

définie pour tout $a \in \mathbb{Z}$

$$f(a) = (a + m\mathbb{Z}, a + n\mathbb{Z}),$$

est un morphisme d'anneaux surjectif, de noyau $mn\mathbb{Z}$.
Les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes.
via l'application $a + mn\mathbb{Z} \mapsto (a + m\mathbb{Z}, a + n\mathbb{Z})$

Fonction indicatrice d'Euler

Definition

Pour tout $n \geq 1$, l'entier $\varphi(n)$ est le nombre d'entiers compris entre 1 et n, et premiers avec n.

$$\varphi(n) = \left\{1 \leq k \leq n : \gcd(k, n) = 1\right\}$$

Lemme

Pour tout nombre premier p et tout entier $r \geq 1$, on a

$$\varphi(p^r) = p^r - p^{r-1}$$

Lemme

Soit $n \geq 1$. Un entier a et $\bar{a}$ sa classe modulo $n\mathbb{Z}$. Alors, $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi $\gcd(a, n) = 1$.

$$(\mathbb{Z}/n\mathbb{Z})^* = \left\{\bar{a} : 1 \leq a \leq n \text{ et } \gcd(a, n) = 1\right\}$$

Fonction indicatrice d'Euler

Corollary (L'ordre de $(\mathbb{Z}/n\mathbb{Z})^*$ est $\varphi(n)$.)

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Corollary

Soient m et n des entiers naturels non nuls premiers entre eux. On a

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Theorem

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Lemme

$$n = \sum_{d|n} \varphi(d)$$

Théorème d'Euler

Theorem (Euler, 1760)

Soit n un entier naturel non nul. Pour tout entier a premier avec n,

$$a^{\varphi(n)} = 1 \bmod n$$

Proposition

Soit G un groupe abélien fini d'ordre n, d'élément neutre e.

Pour tout $x \in G$, on a $x^n = e$.

Corollary (Petit théorème de Fermat)

Soit p un nombre premier. Pour tout entier a non divisible par p,

$$a^{p-1} = 1 \bmod p$$

En particulier, pour tout entier a, on a $a^p = a \bmod p$

Groupes cycliques

Definition

Soit G un groupe fini d'ordre n, de neutre e. G est cyclique s'il existe un élément d'ordre n, appelé un générateur de G. Un groupe cyclique est abélien. Si x est un générateur, $G = \{e, x, \ldots, x^{n-1}\}$

Theorem

Soit G un groupe cyclique d'ordre n.
1) Tout sous-groupe de G est cyclique.
2) Pour tout diviseur $d \geq 1$ de n, l'ensemble

$$H_d = \{a \in G : a^d = e\}$$

est un sous-groupe de G d'ordre d.
3) $d \mapsto H_d$ est une bijection entre l'ensemble des diviseurs de n et l'ensemble des sous-groupes de G. En particulier, pour tout diviseur d de n, H_d est l'unique sous-groupe d'ordre d de G.

Groupes cycliques

Corollary

Soit G un groupe cyclique d'ordre n. Pour tout entier $k \geq 1$, $\{a \in G : a^k = e\}$ est un sous-groupe de G d'ordre $\gcd(k, n)$.

Theorem

Soient G un groupe cyclique d'ordre n et x un générateur de G.
1) L'ensemble des générateurs de G est

$$\{x^k : 1 \leq k \leq n \text{ et } \gcd(k, n) = 1\}.$$

En particulier, G possède exactement $\varphi(n)$ générateurs.
2) Pour tout diviseur d de n, il y a exactement $\varphi(d)$ éléments d'ordre d dans G.

Lemme

Soient H et K des groupes cycliques. Le groupe produit $H \times K$ est cyclique ssi les ordres de H et K sont premiers entre eux.

Le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$ où p est premier impair

Lemme (Caractérisation d'un groupe cyclique)

G groupe fini d'ordre m, de neutre e. Si pour tout diviseur d de m, le cardinal de $\{x \in G : x^d = e\}$ est au plus d, alors G est cyclique.

Proposition

Pour tout nombre premier p, $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.

Theorem

Soient p un nombre premier impair et $n \geq 1$. $(\mathbb{Z}/p^n\mathbb{Z})^*$ est cyclique d'ordre $p^{n-1}(p-1)$. Soit a tq $a + p\mathbb{Z}$ est un géné. de $(\mathbb{Z}/p\mathbb{Z})^*$.

1. *Si $a^{p-1} \neq 1 \bmod p^2$, $a + p^n\mathbb{Z}$ est un générateur de $(\mathbb{Z}/p^n\mathbb{Z})^*$.*
2. *Si $a = 1 \bmod p^2$, $(a+p) + p^n\mathbb{Z}$ est un générateur $(\mathbb{Z}/p^n\mathbb{Z})^*$.*

Theorem (Gauss, 1801)

Les entiers $m \geq 1$ tq $(\mathbb{Z}/m\mathbb{Z})^*$ groupe cyclique sont 1, 2, 4, et ceux de la forme p^r et $2p^r$ où p est un nombre premier impair.