

Lundi : Entiers

Cours de remise à niveau MPRI 2005–2006

David A. Madore
david.madore@ens.fr

19 septembre 2005

Programme du cours

- ▶ Lundi : Entiers (\mathbb{Z})
- ▶ Mardi : Entiers modulaires ($\mathbb{Z}/n\mathbb{Z}$)
- ▶ Mercredi : Polynômes ($k[t]$)
- ▶ Jeudi : Corps finis (\mathbb{F}_q)
- ▶ Vendredi : Extensions de corps (K/k)

9h30 à 12h00 ; salle 0D1 du 19 au 22, 1C1 le 23

Lundi : Entiers

David Madore

Programme du
cours

Table des matières

L'anneau des
entiers

Premiers et
divisibilité

Division
euclidienne

PGCD et PPCM

Bézout et Euclide

Divers

Bibliographie

Table des matières

L'anneau des entiers

Premiers et divisibilité

Division euclidienne

PGCD et PPCM

Bézout et Euclide

Divers

Bibliographie

Lundi : Entiers

David Madore

Programme du
cours

Table des matières

L'anneau des
entiers

Premiers et
divisibilité

Division
euclidienne

PGCD et PPCM

Bézout et Euclide

Divers

Bibliographie

Propriétés de base de \mathbb{Z}

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ est l'ensemble des **entiers (relatifs)**.

\mathbb{Z} est un anneau commutatif

- ▶ $(\mathbb{Z}, 0, +)$ est un groupe abélien.
- ▶ \times est distributif sur $+$.
- ▶ \times est associatif.
- ▶ 1 est élément neutre pour \times .
- ▶ \times est commutatif.

\mathbb{Z} est un anneau intègre : si $ab = 0$ alors $a = 0$ ou $b = 0$.

Les éléments inversibles (ou *unités*) de \mathbb{Z} sont : 1 et -1 .

\mathbb{Z} est l'**anneau universel** (i.e., pour tout anneau A il existe un unique morphisme $\mathbb{Z} \rightarrow A$) : ceci permet de définir dans tout anneau des éléments 0, 1, 2, ..., 42...

Relation d'ordre...

Remarques sur la complexité

$n = O(\log N)$ la taille des entiers considérés.

Addition : algorithme naïf en $O(n)$.

Multiplication :

- ▶ *Algorithme naïf* en $O(n^2)$.
- ▶ *Multiplication de Karatsuba* : utilise récursivement l'identité $(a_1w + a_0)(b_1w + b_0) = a_1b_1w^2 + [(a_1 + a_0)(b_1 + b_0) - a_1b_1 - a_0b_0]w + a_0b_0$ pour une complexité en $O(n^{\frac{\log 3}{\log 2}})$ (soit $O(n^{1.58\dots})$). Facile à implémenter.
- ▶ *Multiplication de Strassen* : par transformée de Fourier rapide, complexité en $O(n \log^2 n)$, difficile à implémenter. Amélioration de Schönhage : $O(n \log n \log \log n)$ — complètement théorique.

Relation de divisibilité : On dit que a est *divisible* par b (notation : $b|a$), ou que b *divise* a , ou que a est un *multiple* de b , lorsqu'il existe un q tel que $a = bq$.

La relation de divisibilité est *réflexive* (pour tout a on a $a|a$) et *transitive* (si $b|a$ et $c|b$ alors $c|a$; on peut donc noter $c|b|a$).

Les entiers 1 et -1 divisent tous les entiers. L'entier 0 est divisible par tous les entiers.

Un **nombre premier** p est un entier (par convention : positif) divisible seulement par 1, -1 , lui-même et son opposé ; mais par convention, 1 et -1 (et 0...) ne sont pas premiers.

Les premiers nombres premiers sont donc : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97...

Il y en a une infinité (Euclide).

Pour tout $x > 1$, il y a toujours un nombre premier p tel que $x \leq p < 2x$ (Čebyšëv : « postulat de Bertrand »).

Le nombre $\pi(x)$ de nombres premiers $\leq x$ est équivalent à $\frac{x}{\ln x}$ lorsque $x \rightarrow +\infty$ (Hadamard & de la Vallée Poussin : « théorème des nombres premiers »).

Lemme de Gauß : pour p premier, si p divise ab alors p divise a ou p divise b .

Décomposition en facteurs premiers

Lundi : Entiers

David Madore

Pour tout entier n non nul, il existe une écriture *unique* (à l'ordre près) de n comme produit d'une *unité* (1 ou -1) et de nombres premiers : en regroupant les facteurs premiers p ,

$$n = u 2^{v_2(n)} 3^{v_3(n)} \dots p^{v_p(n)} \dots$$

Ici, $v_p(n)$ (un entier naturel) est l'exposant de la plus grande puissance de p qui divise n : on l'appelle *valuation p -adique* de n . Presque tous ces nombres sont nuls, ce qui permet de donner un sens au produit infini. Dire que $b|a$ signifie $v_p(b) \leq v_p(a)$ pour tout p .

Quant à u , c'est simplement le signe de n .

Exemple : $145883961 = 3^2 \times 251 \times 64579$

On dit que \mathbb{Z} est un anneau **factoriel**.

Programme du cours

Table des matières

L'anneau des entiers

Premiers et divisibilité

Division euclidienne

PGCD et PPCM

Bézout et Euclide

Divers

Bibliographie

Remarques sur la complexité

Toujours $n = \log N$ la taille des entiers considérés.

Tests de primalité : *polynomiaux*. Un test polynomial *déterministe* est connu depuis seulement récemment (Agrawal-Kayal-Saxena), démontrablement en $O(n^{12})$, sans doute meilleur ($O(n^3)$?). En pratique, des tests probabilistes sont suffisants et plus efficaces (p.e., Miller-Rabin « pratiquement » en $O(n^2)$) éventuellement complétés par des certificats de primalité (p.e., test d'Atkin).

Algorithmes de factorisation : *lents*. Font appel à des résultats difficiles de théorie algébrique et analytique des nombres. La meilleure méthode connue (« méthode du crible général de corps de nombres ») a une complexité « attendue » (et heuristique) en $O(e^{n^{1/3}} (\log n)^{2/3} (cte+o(1)))$ (avec $cte \approx 2$).

On ne pourra donc pas envisager d'utiliser la décomposition en facteurs premiers pour calculer les pgcd.

Normes et valuations p -adiques

Définition : si a/b est un rationnel et p un nombre premier, on pose $v_p(a/b) = v_p(a) - v_p(b)$ (ne dépend pas de la représentation a/b choisie). Par convention, $v_p(0) = +\infty$. On définit $|x|_p = p^{-v_p(x)}$ la **valeur absolue p -adique** de x (entier ou rationnel). La valeur absolue usuelle peut être notée $|x|_\infty$.

Quelques propriétés : (pour $v = p$ premier ou $v = \infty$)

- ▶ $|0|_v = 0$
- ▶ $|xy|_v = |x|_v |y|_v$
- ▶ $|x + y|_v \leq |x|_v + |y|_v$, et si $v = p$ premier on a même $|x + y|_p \leq \max(|x|_p, |y|_p)$ (la valeur absolue est dite *ultramétrique*)

Note : Il existe des complétés \mathbb{Q}_p de \mathbb{Q} par rapport à $|\bullet|_p$ comme \mathbb{R} par rapport à $|\bullet|_\infty$. Intérêt : certains calculs plus faciles dans \mathbb{Q}_2 (« négliger les bits de poids fort »).

Programme du cours

Table des matières

L'anneau des entiers

Premiers et divisibilité

Division euclidienne

PGCD et PPCM

Bézout et Euclide

Divers

Bibliographie

Si a est un entier relatif et b un entier naturel *non nul*, il existe un unique couple (q, r) tel que :

- ▶ q est un entier relatif,
- ▶ r est un entier naturel tel que $0 \leq r < b$, et
- ▶ $a = bq + r$.

On dit que q est le *quotient* et r le *reste* de la **division euclidienne** de a par b . (On appelle aussi a le *dividende* et b le *diviseur*.)

Dire que $r = 0$ signifie exactement que b divise a (la division euclidienne est alors *exacte*).

On dit que \mathbb{Z} est un anneau **euclidien**.

Division euclidienne (suite)

Lundi : Entiers

David Madore

Programme du
cours

Table des matières

L'anneau des
entiers

Premiers et
divisibilité

Division
euclidienne

PGCD et PPCM

Bézout et Euclide

Divers

Bibliographie

Algorithme naïf : (celui de l'école primaire) en $O(n^2)$.

Complexité : en $O(n \log n \log \log n)$ avec
Schönhage-Strassen + méthode de Newton (+ subtilités).
Méthode de Newton : on inverse b (en précision fixe) en
itérant $x \leftarrow 2x - bx^2$.

Souvent implémentée **en matériel**.

MMIX (Knuth) : 60 cycles pour une division entière de 128
bits par 64 bits (contre 1 cycle pour une addition 64 bits).

AMD 64 / Intel EM64T : division entière de 128 bits par 64
bits.

Un **idéal** I d'un anneau commutatif A est un sous-groupe additif de A tel que $AI = I$ (i.e., multiplier un élément de I par un élément quelconque de A donne un élément de I).
Intérêt : si A est un anneau commutatif et I un idéal de A , on peut définir un anneau quotient A/I .

Les idéaux de \mathbb{Z} sont exactement les $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ (ensemble des multiples de n), où n parcourt l'ensemble \mathbb{N} des entiers naturels.

On dit que \mathbb{Z} est un anneau **principal**.

Remarque : euclidien \Rightarrow principal \Rightarrow factoriel

Si m_1, \dots, m_ℓ sont des entiers, on dit qu'un entier c est un **plus grand commun diviseur** (en abrégé : *pgcd*) des m_i lorsque :

- ▶ c divise chaque m_i (i.e, c est un diviseur commun des m_i), et
- ▶ tout entier d qui divise chaque m_i (i.e., tout diviseur commun des m_i) divise aussi c .

En principe, le pgcd des m_i est défini au signe près (si c est un pgcd des m_i alors $-c$ l'est aussi) : en imposant qu'il soit positif il devient unique et on parle alors *du* pgcd des m_i .

Exemple : le pgcd de 6 et 10 est 2 ; le pgcd de 6, 10 et 15 est 1.

Le pgcd *existe* toujours : on peut le définir à partir de la décomposition en facteurs premiers par

$$v_p(\text{pgcd}(m_1, \dots, m_\ell)) = \min(v_p(m_1), \dots, v_p(m_\ell))$$

(pour tout nombre premier p).

En terme d'idéaux : c est un pgcd de m_1, \dots, m_ℓ si et seulement si $c\mathbb{Z} = m_1\mathbb{Z} + \dots + m_\ell\mathbb{Z}$.

Notation : Parfois $m_1 \wedge \dots \wedge m_\ell$, mais cette notation peut être utilisée pour d'autres sortes de bornes inf. Certains textes anglais utilisent (m, m') pour le pgcd de deux entiers. La notation $\text{pgcd}(\dots)$ est évidemment la plus claire.

Quelques propriétés :

- ▶ le pgcd d'un seul entier m est lui-même (et le pgcd de zéro entiers est 0),
- ▶ le pgcd est associatif (par exemple $\text{pgcd}(m_1, m_2, m_3) = \text{pgcd}(\text{pgcd}(m_1, m_2), m_3)$),
- ▶ le produit est distributif sur le pgcd ($\text{pgcd}(cm_1, \dots, cm_\ell) = |c| \text{pgcd}(m_1, \dots, m_\ell)$),
- ▶ on peut toujours effacer des 0 d'un pgcd,
- ▶ dès qu'un des entiers est 1 ou -1 , le pgcd est 1,
- ▶ le pgcd d'une famille infinie se définit sans difficulté.

Lorsque $\text{pgcd}(m_1, \dots, m_\ell) = 1$, on dit que les m_i sont **premiers entre eux** *dans leur ensemble*.

Lorsque $\text{pgcd}(m_i, m_j) = 1$ pour tous $i \neq j$, on dit que les m_i sont premiers entre eux *deux à deux*.

Lemme de Gauß amélioré : Si m et n sont premiers entre eux, être multiple de m et de n équivaut à être multiple de mn .

Dirichlet : La probabilité pour que deux entiers « tirés au hasard » soient premiers entre eux est $\frac{6}{\pi^2}$.

Définition du (ou d'un) **plus petit commun multiple** (*ppcm*) analogue à celle du pgcd : c'est un multiple commun (il est divisible par chacun des m_i) et il divise n'importe quel autre multiple commun.

Exemple : le ppcm de 6 et 10 est 30 ; le ppcm de 6, 10 et 15 est aussi 30.

Avec la décomposition en facteurs premiers :

$$v_p(\text{ppcm}(m_1, \dots, m_\ell)) = \max(v_p(m_1), \dots, v_p(m_\ell))$$

En terme d'idéaux : c est un ppcm de m_1, \dots, m_ℓ si et seulement si $c\mathbb{Z} = m_1\mathbb{Z} \cap \dots \cap m_\ell\mathbb{Z}$.

Remarque : le ppcm d'une famille infinie d'entiers est défini, mais parfois surprenant...

Relations de Bézout

Si a et b sont premiers entre eux (c'est-à-dire $\text{pgcd}(a, b) = 1$), on a $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$, c'est-à-dire qu'il existe des entiers u et v tels que $au + bv = 1$: on appelle cette égalité une **relation de Bézout**¹ entre a et b (ou, bien sûr, entre u et v , ou entre a et v ...).

Réciproquement, l'existence d'une relation de Bézout entre a et b implique que a et b sont premiers entre eux (et alors les coefficients, u et v , sont aussi premiers entre eux).

Exemple : $42 \times 38 - 55 \times 29 = 1$ constitue une relation de Bézout entre 42 et 55. On verra plus loin comment obtenir une relation de Bézout.

Naturellement, ajouter b à u et $-a$ à v donne une nouvelle relation de Bézout entre a et b .

Si $au + bv = \pm 1$ on dit parfois que les rationnels a/b et $-v/u$ (écrits sous forme irréductible) sont *adjacents*.

¹Le nom d'Étienne Bézout (1730–1783) s'écrit avec un accent aigu. 19/28

Soit à calculer le pgcd de deux entiers a et b . **L'algorithme d'Euclide** pour ce faire est le suivant :

- ▶ Initialiser : $(m, n) \leftarrow (|a|, |b|)$.
- ▶ Tant que $n \neq 0$, répéter :
 - ▶ $(m, n) \leftarrow (n, r)$ où r est le reste de la division euclidienne $m = nq + r$ de m par n .
- ▶ Renvoyer m (le pgcd recherché).

Invariant : $\text{pgcd}(m, n) = \text{pgcd}(a, b)$ (constant)

Exemple : soit à calculer le pgcd de $a = 98$ et $b = 77$:

- ▶ $(m, n) = (98, 77)$; division euclidienne $98 = 77 \times 1 + 21$;
- ▶ $(m, n) = (77, 21)$; division euclidienne $77 = 21 \times 3 + 14$;
- ▶ $(m, n) = (21, 14)$; division euclidienne $21 = 14 \times 1 + 7$;
- ▶ $(m, n) = (14, 7)$; division euclidienne $14 = 7 \times 2 + 0$;
- ▶ $(m, n) = (7, 0)$; on renvoie 7.

Calcul des coefficients de Bézout

Lundi : Entiers

David Madore

Algorithme d'Euclide « étendu » : L'idée est de « remonter » les coefficients dans l'algorithme d'Euclide : la dernière division $m = nq + 1$ donne une relation $1 = m - nq$ puis on remplace n (qui est lui-même un reste de division euclidienne) et ainsi de suite jusqu'à trouver une relation entre les entiers a et b de départ.

En mémoire constante, cela donne :

Soit à calculer une relation de Bézout entre deux entiers a et b (premiers entre eux) :

- ▶ $(m, n, u, v, u', v') \leftarrow (|a|, |b|, \text{signe}(a), 0, 0, \text{signe}(b))$.
- ▶ Tant que $n \neq 0$, répéter :
 - ▶ Division euclidienne de m par n : soit $m = nq + r$.
 - ▶ $(m, n, u, v, u', v') \leftarrow (n, r, u', v', u - qu', v - qv')$.
- ▶ Vérifier $m = 1$ (le pgcd est bien 1).
- ▶ Les coefficients recherchés sont u et v (on a $au + bv = 1$).

Invariants : $au + bv = m$ et $au' + bv' = n$.

Programme du cours

Table des matières

L'anneau des entiers

Premiers et divisibilité

Division euclidienne

PGCD et PPCM

Bézout et Euclide

Divers

Bibliographie

Lien avec les fractions continuées

Lundi : Entiers

David Madore

Programme du
cours

Table des matières

L'anneau des
entiers

Premiers et
divisibilité

Division
euclidienne

PGCD et PPCM

Bézout et Euclide

Divers

Bibliographie

Les $-v'/u'$, où (u', v') sont les variables utilisées dans l'algorithme précédent, sont exactement les *réduites* du développement en fraction continuée de a/b .

Exemple : si $(a, b) = (14, 11)$, le développement de $14/11$ en fraction continuée est :

$$\frac{14}{11} = 1 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2}}}$$

les coefficients 1, 3, 1, 2 sont les quotients successifs des divisions euclidiennes, et les réduites sont $\frac{1}{1}, \frac{4}{3}, \frac{5}{4}, \frac{14}{11}$.

L'arbre de Stern-Brocot

Lundi : Entiers

David Madore

Programme du cours

Table des matières

L'anneau des entiers

Premiers et divisibilité

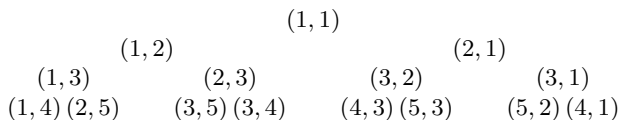
Division euclidienne

PGCD et PPCM

Bézout et Euclide

Divers

Bibliographie



L'**arbre de Stern-Brocot** est un arbre binaire étiqueté, de racine $(1, 1)$, dont chaque nœud porte l'étiquette $(u + u', v + v')$, où (u, v) est son ancêtre le plus immédiatement à gauche (ou $(0, 1)$ s'il n'y en a pas) et (u', v') son ancêtre le plus immédiatement à droite (ou $(1, 0)$).

Propriété : Chaque couple (a, b) d'entiers naturels non nuls avec $\text{pgcd}(a, b) = 1$ apparaît exactement une fois dans l'arbre, et l'ancêtre de (a, b) est un (c, d) tel que a/b et c/d soient adjacents, i.e., $ad - bc = \pm 1$ (d'où une relation de Bézout), le signe étant $+$ si le fils est à droite et $-$ s'il est à gauche.

On peut voir l'arbre comme un arbre des rationnels (strictement positifs), chacun apparaissant exactement une fois (sous forme irréductible) et chaque branche correspondant à un irrationnel (positif). Un *parcours* dans l'arbre donne la décomposition en fraction continue (chaque changement de direction est une réduite).

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_n + F_{n+1}$$

Exercice : Montrer que F_n et F_{n+1} sont premiers entre eux pour tout $n \in \mathbb{N}$, et expliciter une relation de Bézout entre eux. Combien d'étapes faut-il exécuter dans l'algorithme d'Euclide « étendu » pour arriver à cette relation ? Où se trouvent les couples (F_n, F_{n+1}) dans l'arbre de Stern-Brocot ? En introduisant le *nombre d'or* $\phi = \frac{1}{2}(1 + \sqrt{5})$, donner une valeur exacte de F_n et la limite de F_{n+1}/F_n . Quel est le développement en fraction continuée de ϕ ?

Montrer que la complexité de l'algorithme d'Euclide étendu (dans le pire cas) est linéaire avec une constante $\frac{1}{\log \phi}$ (entre $n = \log N$ et le nombre de divisions euclidiennes).

Programme du cours

Table des matières

L'anneau des entiers

Premiers et divisibilité

Division euclidienne

PGCD et PPCM

Bézout et Euclide

Divers

Bibliographie

Exercice : En utilisant les propriétés suivantes :

- ▶ $\text{pgcd}(2a, 2b) = 2 \text{pgcd}(a, b)$ (cas de deux nombres pairs)
- ▶ $\text{pgcd}(2a, 2b + 1) = \text{pgcd}(a, 2b + 1)$ (pair et impair)
- ▶ $\text{pgcd}(a, b) = \text{pgcd}(b, a - b)$ (comme algo. Euclide)
- ▶ Si a et b sont impairs, $a - b$ est pair et $|a - b| < \max(a, b)$.

décrire un algorithme de calcul de PGCD qui n'utilise pas d'opération de division entière (en réalité, l'algorithme de division « naïf » est caché dedans).

(La complexité de cet algorithme est comparable à celle de l'algorithme d'Euclide.)

Cas d'une puissance de 2

Lundi : Entiers

David Madore

Programme du
cours

Table des matières

L'anneau des
entiers

Premiers et
divisibilité

Division
euclidienne

PGCD et PPCM

Bézout et Euclide

Divers

Bibliographie

Si $a = 2^\ell$ est une puissance de 2 (et b impair, donc premier avec a), on peut calculer une relation de Bézout $au + bv = 1$ de façon simple et efficace sur ordinateur par la **méthode de Newton** : il suffit d'itérer $x \leftarrow 2x - bx^2$, à partir de $x = 1$, en effectuant des calculs modulo $a = 2^\ell$. Ceci converge en $O(\log \ell)$ itérations vers un v tel que recherché (i.e., $bv - 1$ divisible par 2^ℓ).





Explication : Il s'agit de la méthode de Newton appliquée dans \mathbb{Q}_2 , c'est-à-dire qu'il y a convergence de x vers $1/b$ en norme 2-adique.

Exemple : Avec $a = 2^{32}$ et $b = 1729$, on trouve $1 \mapsto 4294965569 \mapsto 3433138497 \mapsto 4255222081 \mapsto 4255222081$ donc on a bien $1729 \times 4255222081 \equiv 1 \pmod{2^{32}}$.

Les entiers relatifs ne sont pas le seul anneau arithmétique à être euclidien : il existe une propriété de division euclidienne par exemple dans $\mathbb{Z}[i] = \{m + in : (m, n) \in \mathbb{Z}^2\}$ (ensemble des entiers gaussiens). Précisément : si $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$, alors il existe $q, r \in \mathbb{Z}[i]$ tels que $a = bq + r$ et $|r|^2 < |b|^2$.

Exercice : Montrer cette propriété, en prenant pour q l'entier gaussien le plus proche (dans le plan complexe) de $a/b \in \mathbb{C}$. Calculer le pgcd de $3 + i$ et $28 + 14i$ dans $\mathbb{Z}[i]$. (*Attention :* $\mathbb{Z}[i]$ a quatre unités (éléments inversibles) : lesquelles ?)

Très courte bibliographie

-  H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer (GTM 138).
-  R. L. Graham, D. E. Knuth & O. Patashnik, *Concrete Mathematics, A Foundation for Computer Science*, 2d ed., Addison-Wesley.
-  D. E. Knuth, *The Art of Computer Programming* (3rd ed.), Addison-Wesley.
-  J. von zur Gathen & J. Gerhard, *Modern Computer Algebra* (2d ed.), Cambridge.

Lundi : Entiers

David Madore

Programme du
cours

Table des matières

L'anneau des
entiers

Premiers et
divisibilité

Division
euclidienne

PGCD et PPCM

Bézout et Euclide

Divers

Bibliographie