

Arithmétique des entiers et des polynômes

Avant propos

Dans ces notes de cours nous allons aborder des notions évoquées dans les points 3.1, 3.5, 3.6 du programme 2009 des épreuves écrites ainsi que des notions des points 1, 2, 7 du programme 2009 spécifique de l'option C.

Références

[CF06] Henri Cohen and Gerhard Frey. *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman & Hall/CRC, 2006.

[Dem97] Michel Demazure. *Cours d'Algèbre — Primalité, Divisibilité, Codes*, volume 1 of *Nouvelle Bibliothèque mathématique*. Cassini, 1997.

[Knu97] Donald E. Knuth. *The Art of Computer Programming, Vol 2*. Addison-Wesley, 1997.

1 Questions de coût (de la vie ?)

Afin de déterminer les **coûts** ou la **complexité** des divers algorithmes que nous allons aborder dans ce cours, il convient tout d'abord de réfléchir à ce qu'est la taille «machine» des quantités que nous allons manipuler. Plus précisément, demandons nous ce qu'est la taille d'un entier ou d'un polynôme. Pour simplifier, on supposera qu'un ordinateur code un entier dans un tableau contenant les chiffres (ou bits ou encore digits) de sa décomposition binaire¹. Quant aux polynômes, ils sont eux aussi codés dans un tableau contenant ses coefficients.

- Question 1.** a. Exprimer la taille nécessaire pour stocker un entier n en fonction de n .
 b. Faire de même pour un polynôme.

- Question 2.** a. A votre avis qu'est-ce qu'un algorithme **polynomial** ou **exponentiel** dans le cadre des entiers ?
 b. Et dans le cadre des polynômes ?

Cela étant, évaluons la complexité des opérations de base entre entiers ou polynômes.

Question 3. Compléter, en justifiant votre réponse, le tableau récapitulatif des complexités suivant :

Opération	Complexité	$a, b \leq n$	Opération	Complexité	$\deg(A), \deg(B) \leq d$
$a + b$			$A + B$		
$a - b$			$A - B$		
$a \times b$			$A \times B$		
a^e			A^e		
$a \div b$			$A \div B$		
$\text{pgcd}(a, b)$			$\text{pgcd}(A, B)$		

Question 4. Avez-vous eu connaissance d'une opération sur les entiers que l'on sait, à ce jour, ni faire efficacement, ni montrer qu'il est impossible de le faire efficacement ?

1. Ce faisant nous nous écartons que très peu de la réalité (cf. §4.3 pour plus de précisions)

2 Anneaux euclidiens

Les anneaux \mathbb{Z} et $K[X]$ partagent la qualité fondamentale d'être **euclidien**. Un anneau A est dit **euclidien** s'il existe une application $\omega : A^* \rightarrow \mathbb{N}$ telle que :

1. pour tous $a, b \in A^*$, si $a \mid b$ alors $\omega(a) \leq \omega(b)$;
2. pour tout $a \in A$ et tout $b \in A^*$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $r \neq 0$ et $\omega(r) < \omega(b)$.

L'anneau des entiers \mathbb{Z} est euclidien avec

Théorème 2.1 (Division Euclidienne) Soient $a, b \in \mathbb{Z}$, avec $b \neq 0$. Il existe un unique couple d'entiers $(q, r) \in \mathbb{Z}^2$ tel que :

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

Quant à l'anneau des polynômes $K[X]$ à coefficients dans un corps K , il est euclidien
Pour simplifier les énoncés, on convient que le degré du polynôme nul vaut $-\infty$ avec la convention supplémentaire $-\infty < d$ pour tous $d \in \mathbb{N}$.

Théorème 2.2 (Division euclidienne polynomiale) Soit A et B deux polynômes de $K[X]$ avec B non nul. Il existe $(Q, R) \in K[X]^2$ unique tel que :

$$A = BQ + R \quad \text{et} \quad \deg(R) < \deg(B).$$

Les entiers q, r (respectivement les polynômes Q, R) des deux énoncés précédents s'appellent le **quotient** et le **reste** de la division euclidienne de a par b (respectivement de A par B).

Question 5. Soient a et b deux entiers écrits en base 2 comptant respectivement α et β digits. Quel est l'ordre de grandeur du nombre d'additions (ou soustractions) que requiert la division de a par b ?

3 Calcul de pgcd

La théorie de la divisibilité est considérablement simplifiée dans les anneaux euclidiens. Si de plus la division euclidienne est explicite — ce qui est le cas pour \mathbb{Z} et $K[X]$ comme nous venons de le voir —, alors beaucoup de concepts liés à la divisibilité deviennent explicites eux aussi, à commencer par le calcul du pgcd.

3.1 Autour de l'identité de Bezout

La théorie de la divisibilité dans les entiers peut se présenter selon deux points de vue bien différents. Soit on met en avant les nombres premiers et le théorème fondamental de l'arithmétique — *tout nombre entier se décompose d'une unique façon (à l'ordre près) en produit de premiers* —, soit on se base sur l'existence d'identités de Bezout. Cependant, dès lors que l'on est concerné par l'effectivité, aucune hésitation n'est possible : c'est le point de vue de Bezout qu'on l'on suit.

Théorème 3.1 Soient a et b deux entiers. Il existe un diviseur commun d à a et b qui est somme d'un multiple de a et d'un multiple de b , c'est-à-dire de la forme :

$$d = au + bv$$

avec $u, v \in \mathbb{Z}$. De plus cet entier est unique au signe près.

Question 6. Le montrer.

En fait l'entier d du théorème précédent n'est rien d'autre que $\text{pgcd}(a, b)$ le **plus grand commun diviseur entre a et b** (au signe près). Quant aux coefficients u et v , ils s'appellent des **coefficients de Bezout**².

2. Etienne Bézout est né le 31 Mars 1730 à Nemours, France et mort le 27 Septembre 1783 à Basses-Loges, France.

Question 7. a. Donner les autres autres caractérisations du $\text{pgcd}(a, b)$ et montrer qu'elles sont toutes équivalentes.

b. Montrer l'égalité entre les idéaux $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

c. Un entier qui est somme d'un multiple de a et d'un multiple de b est-il forcément égal au $\text{pgcd}(a, b)$? Si non, qu'est-il donc ?

Question 8. En raisonnant avec les coefficients de Bezout, montrer que :

$$\text{pgcd}(a, b) = 1 \quad \implies \quad \text{pgcd}(a^n, b^n) = 1, \quad \forall n \geq 1.$$

Voici maintenant le pendant polynomial de l'énoncé précédent.

Théorème 3.2 Soit A et B deux polynômes de $K[X]$. Il existe un diviseur commun D à A et B de la forme :

$$D = AU + BV,$$

avec $U, V \in K[X]$. De plus ce polynôme est unique à un élément de K^* près.

Tout ce que l'on vient de faire pour deux entiers (ou polynômes) se généralise en considérant r entiers (ou polynômes) avec $r \geq 2$.

Question 9. a. Rappeler ce que cela veut dire pour r entiers a_1, \dots, a_r d'être **premiers entre eux** dans leur ensemble? Et d'être **premiers entre eux deux-à-deux**?

b. Pour $1 \leq i \leq r$, on note Π_i le i -ème coproduit défini par $\Pi_i = \prod_{j \neq i} a_j$. Montrer l'équivalence :

$$a_1, \dots, a_r \text{ sont premiers entre eux deux-à-deux} \iff \Pi_1, \dots, \Pi_r \text{ sont premiers entre eux.}$$

c. Montrer les deux formules :

$$\text{pgcd}(a_1, \dots, a_r) = \text{pgcd}(a_1, \text{pgcd}(a_2, \dots, a_r)) = \text{pgcd}(\text{pgcd}(a_1, a_2), a_3, \dots, a_r),$$

puis vérifier que l'une donne naissance à un algorithme récursif, l'autre à un algorithme itératif, pour le calcul du pgcd de r entiers.

3.2 Algorithme d'Euclide (étendu)

L'algorithme d'Euclide dans sa version «étendue» permet de calculer à la fois le pgcd et des coefficients de Bezout. Il repose sur le lemme suivant :

Lemme 3.3 Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$; si r est le reste de la division Euclidienne de a par b , alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Question 10. Le prouver.

Je vous rappelle brièvement le principe de **l'algorithme d'Euclide**. Il repose sur la remarque suivante : le processus initié dans le lemme 3.3 ne peut être réitéré qu'un nombre fini de fois. On effectue les divisions successives suivantes :

$$(r_0, r_1) \rightarrow (r_1, r_2) \rightarrow (r_2, r_3) \rightarrow \dots \rightarrow (r_n, r_{n+1})$$

où on a posé $r_0 = a$, $r_1 = b$ et noté r_i le reste de la division Euclidienne de r_{i-2} par r_{i-1} . Alors :

$$|b| = |r_1| > r_2 > r_3 > \dots > r_i > \dots \geq 0.$$

Au bout d'un certain nombre de divisions le reste est forcément nul. Notons r_n le dernier reste **non nul**, c'est-à-dire que $r_n \neq 0$ et $r_{n+1} = 0$. D'après le lemme 3.3,

$$\text{pgcd}(a, b) = \text{pgcd}(r_0, r_1) = \text{pgcd}(r_1, r_2) = \text{pgcd}(r_2, r_3) = \dots = \text{pgcd}(r_n, r_{n+1}) = \text{pgcd}(r_n, 0) = r_n,$$

si bien que le dernier reste non nul n'est rien d'autre que $\text{pgcd}(a, b)$.

Question 14. Compléter l'énoncé précédent et donner un algorithme résolvant un tel système de congruences. Indications : pour vous aider, vous pouvez commencer à résoudre les systèmes avec $a = 1$ et $b = 0$, puis $a = 0$ et $b = 1$, puis en déduire les solutions en général.

Question 15. a. Plus généralement, que suffit-il de supposer sur r entiers m_1, \dots, m_r pour qu'étant donnés $a_1, \dots, a_r \in \mathbb{Z}$, le système :

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

admette des solutions (si vous savez répondre pour $r = 3$, vous le saurez pour r quelconque).

b. Donner un algorithme qui résolve ce type de système.

4 Le théorème chinois

4.1 Les divers énoncés

Commençons par donner deux énoncés du théorème chinois.

Théorème 4.1 (Chinois (forme brève)) *Si a et b sont deux entiers premiers entre eux alors les anneaux $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ sont isomorphes.*

Théorème 4.2 (Chinois (forme complète)) *Soient a et b sont deux entiers premiers entre eux et $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Alors les applications :*

$$\begin{array}{ccc} \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} & \qquad \qquad \qquad & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} & \longrightarrow & \mathbb{Z}/ab\mathbb{Z} \\ x \text{ mod } ab & \longmapsto & (\dots\dots\dots, \dots\dots\dots) & & (x \text{ mod } a, y \text{ mod } b) & \longmapsto & \dots\dots\dots \end{array}$$

définissent des isomorphismes d'anneaux réciproques l'un de l'autre.

Question 16. Compléter l'énoncé du théorème précédent.

Question 17. Généraliser ce théorème au cas de r entiers a_1, \dots, a_r .

4.2 Le petit théorème de Fermat

Soit $n = p_1^{e_1} \cdots p_r^{e_r}$ un entier décomposé en premiers. On s'intéresse à $U(\mathbb{Z}/n\mathbb{Z})$ le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Question 18. Au fait à quelle condition sur $x \in \mathbb{Z}$, la classe $x \text{ mod } n$ est-elle inversible dans $\mathbb{Z}/n\mathbb{Z}$? Comment calcule-t-on cet inverse ?

Comme l'isomorphisme du théorème chinois est un isomorphisme $\dots\dots\dots$, il induit un isomorphisme entre les groupes d'inversibles :

$$U(\mathbb{Z}/n\mathbb{Z}) \simeq U(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times U(\mathbb{Z}/p_r^{e_r}\mathbb{Z}).$$

Théorème 4.3 (Petit théorème de Fermat) *Soit n un entier. Pour tout $x \in \mathbb{Z}$ premier à n on a $x^{\varphi(n)} \equiv 1 \pmod{n}$.*

Question 19. C'est un simple résultat de théorie des groupes non ?

En particulier on a le :

Corollaire 4.4 *Si p est premier alors pour tout $x \in \mathbb{Z}$ premier à p on a $\dots\dots\dots$*

Une question assez naturelle vient à l'esprit : la réciproque de l'énoncé précédent est-elle vraie ? La réponse est non.

Proposition 4.5 Soit $n \geq 1$ un entier. Alors sont équivalentes :

1. l'entier n est sans facteur carré et pour tout premier p divisant n , on a $p - 1$ qui divise $n - 1$;
2. pour tout x premier à n , on a $x^{n-1} \equiv 1 \pmod{n}$.

Question 20. Le montrer.

Les entiers composés qui satisfont cette proposition s'appellent les **nombre de Carmichael** (cf. [Dem97, §3.3.1]). Ils sont en nombre infini et joueront les trouble-fêtes dans les critères de primalité issus du petit théorème de Fermat.

4.3 Codage des grands entiers

Dans un cours ultérieur, il sera question du codage de grands entiers et plus généralement des nombres réels ou complexes sur un ordinateur. Nous allons aborder ici une alternative au codage le plus courant pour les entiers reposant sur le théorème chinois (cf. l'ouvrage de Knuth [Knu97, §4.3.2] pour plus de détails). L'idée est assez simple : afin de coder les entiers $\leq M$, on choisit r petits entiers m_1, \dots, m_r de telle sorte que $m_1 \cdots m_r > M$. Chaque entier de $x \in [0..M]$ est alors codé par le r -uplet (x_1, \dots, x_r) où on a posé $x_i = x \pmod{m_i}$.

Question 21. a. Parmi toutes les opérations élémentaires déjà évoquées, quelles sont celles qui s'adaptent très bien à cette nouvelle représentation et quelles sont celles qui, au contraire, ne s'en accommodent pas.

b. Est-il facile de comparer deux entiers écrits sous cette forme ?

Pour comprendre le gain en terme d'efficacité que peut apporter cette méthode, il faut revenir sur la représentation des entiers en machine. Tout d'abord une machine «pense» binaire, c'est-à-dire qu'elle ne manie que des 0 et des 1, les fameux *bits*. En fait, la plus petite unité de mémoire est en général le *byte* qui n'est rien d'autre qu'une suite de huit bits. Ensuite le processeur est capable de manipuler en même temps plusieurs bytes au moyen d'un registre. La taille de ce registre, aussi appelé *mot machine*, est une des caractéristiques les plus importantes de l'ordinateur. Ainsi, un *ordinateur 32 bits* (respectivement *64 bits*) est connu pour savoir manier des mots de taille 32 (respectivement 64). Toutes les opérations élémentaires sur les entiers codés sur un seul mot ("single precision integers" in english) sont optimisées au maximum tant et si bien que l'on peut choisir ces opérations comme unité de mesure (et non plus l'opération bit-à-bit) en ne distinguant même pas l'addition de la multiplication. Je renvoie à la lecture des ouvrages de Knuth [Knu97, §4.2] ou Cohen et Frey [CF06, chapter 10] pour un exposé complet sur la question.

Question 22. Sur un ordinateur 32 bits, quel ordre de grandeur est-il judicieux de choisir pour les moduli m_i ?

Question 23. Que deviennent les complexités des opérations élémentaires $+$ et \times avec ce nouveau codage.

Question 24. a. Montrer que tout entier $x < m_1 \cdots m_r$ s'écrit sous la forme :

$$y_1 + m_1 y_2 + m_1 m_2 y_3 + \cdots + m_1 \cdots m_{r-1} y_r, \quad 0 \leq y_i < m_i, \forall i.$$

b. Montrer que l'on peut calculer les y_i à partir des x_i sans jamais manipuler d'entiers occupant plus de deux mots.

c. Quelle opération supplémentaire nous permet la manipulation des y_i ?

4.4 Résolution des systèmes linéaires à coefficients rationnels

Dans le même esprit que la section précédente, via le théorème chinois, on peut résoudre un système linéaire du type $MX = V$ avec $M \in M_{m,n}(\mathbb{Z})$ et $V \in \mathbb{Z}^m$. L'idée est la suivante : on résout ce système modulo plusieurs premiers p_1, \dots, p_r et on remonte à \mathbb{Z} grâce au théorème chinois.

Question 25. a. Si $m = n$ et si $\det(M) \neq 0$ donner un algorithme qui résolve l'équation $MX = V$ basé sur le théorème chinois.

b. Résoudre le système :

$$\begin{pmatrix} 1 & -3 & 2 \\ 2 & 4 & -1 \\ 1 & 5 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 16 \\ 77 \\ 69 \end{pmatrix}$$

Plus généralement, plaçons nous dans le cas où $m \leq n$ et où r le rang de M vérifie $r < m$.

Question 26. Comparer le rang de M et celui de $M \bmod p$ sa réduction modulo p .

Question 27. Pour fixer les idées, supposons que Δ le mineur $r \times r$ en haut à gauche de M est non nul.

a. Pour tout $r + 1 \leq i \leq n$, montrer que le système $MX = 0$ admet une unique solution de la forme

$${}^t(x_1, \dots, x_r, 0, \dots, 0, \Delta, 0, \dots, 0), \quad x_1, \dots, x_r \in \mathbb{Z}$$

où la coordonnée valant Δ se trouve en i -ème position.

b. Soit p un premier ne divisant pas Δ . Montrer que deux solutions de $MX = 0 \pmod{p}$ dont les $(n - r)$ dernières coordonnées coïncident sont égales modulo p .

c. Montrer que l'on peut adapter la stratégie du cas simple pour calculer les solutions de la question précédente.

Question 28. Résoudre avec la méthode précédente le système $MX = 0$ avec :

$$M = \begin{pmatrix} 1 & 2 & 2 & -3 \\ -1 & -3 & 1 & -14 \\ 3 & 1 & 21 & -94 \end{pmatrix}.$$