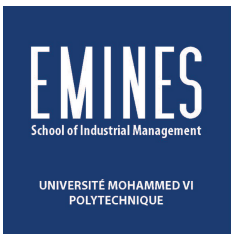

Initiation à la Cryptographie et aux codes correcteurs d'erreur

15-19 mars 2021

EMINES

Pierre-Vincent Koseleff

17 mars 2021

Table des matières

Introduction

Le but de ce cours est de proposer une première approche en algèbre appliquée avec le souci de l'effectivité.

Les problèmes abordés ici trouvent des applications pratiques et théoriques : une introduction aux codes correcteurs d'erreur et à la cryptographie à clé publique.

Le point de départ est l'algorithme d'Euclide. L'algorithme d'Euclide s'applique dans deux anneaux euclidiens en particulier : l'anneau des entiers relatifs $\mathbf{Z}$ et l'anneau des polynômes à coefficients dans un corps $\mathbf{K}$. Encore faut-il que l'on puisse effectuer efficacement les opérations arithmétiques dans le corps $\mathbf{K}$. Nous examinerons en particulier le cas où le corps de base est un corps fini $\mathbf{F}_q$ et le cas où le corps de base est celui des rationnels.

Nous verrons que l'algorithme d'Euclide permet d'effectuer rapidement des opérations arithmétiques dans l'anneau des entiers relatifs, dans l'anneau quotient $\mathbf{Z}/n\mathbf{Z}$ ou dans une algèbre quotient $\mathbf{K}[X]/(P)$.

Après un rappel d'algèbre commutative et d'arithmétique, nous examinerons les méthodes classiques de calcul dans l'anneau des entiers et l'anneau des polynômes, du point de vue de leur complexité.

La possibilité d'effectuer rapidement des calculs dans l'anneau $\mathbf{Z}/n\mathbf{Z}$ est à la base de nombreux protocoles cryptographiques, qui permettent les échanges sécurisés. D'une façon générale, le théorème chinois permet de ramener le calcul d'un objet de grande taille dans $\mathbf{Z}$ (ou dans un anneau euclidien) aux calculs simultanés dans des anneaux $\mathbf{Z}/n\mathbf{Z}$ où les opérations sont beaucoup plus rapides. A contrario, la cryptographie repose sur la difficulté algorithmique de factoriser un nombre entier ayant peu de facteurs premiers et sur la difficulté du calcul du logarithme discret.

Nous aborderons également la théorie des codes correcteurs d'erreur, qui sont largement utilisés dans la vie courante, dans la transmission des données. Ce sont les codes correcteurs, par exemple, qui permettent de lire des *compact disc* audio, qui permettent d'éviter des pannes informatiques, qui permettent les transmissions entre des satellites artificiels. Ils sont basés sur la possibilité de corriger des erreurs dans la transmission des données en autorisant une certaine redondance.

Nous nous limiterons aux codes linéaires qui sont des $\mathbf{F}_q$-espaces vectoriels. Les méthodes utilisées relèvent de la théorie des corps finis et de l'algèbre linéaire.

Ce texte contient donc les éléments nécessaires à cette introduction. Il est clair que la totalité ne pourra être utilisée, faute de temps. Nous aborderons certains aspects et les étudiants intéressés y trouveront les démonstrations ou indications nécessaires à un approfondissement.

Dans le cours dispensé cette année, les parties concernant les complément sur les corps finis ainsi que les codes cycliques n'ont pas été abordées, faute de temps. Ainsi nous nous sommes bornés aux corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

Anneaux euclidiens

Dans cette partie, nous examinons l'algorithme d'Euclide du point de vue de l'effectivité, c'est-à-dire, nous envisageons les méthodes pour calculer le pgcd de deux éléments, ainsi qu'une relation de Bézout.

Deux anneaux jouent un rôle plus particulier : l'anneau des entiers relatifs et l'anneau des polynômes à coefficients dans un corps commutatif K. Les résultats non démontrés de cette partie sont normalement connus depuis la seconde année. Une bonne référence est le cours de L2, 2M220 [5] ou le livre de P. Wassef ([8]).

L'anneau des entiers relatifs

Rappelons que $(\mathbf{Z}, +, \times)$ est un anneau commutatif unitaire et intègre. C'est un anneau euclidien :

Théorème. Division euclidienne.
Soit $(a,b) \in \mathbf{Z} \times \mathbf{Z}^*$, il existe un couple unique $(q,r) \in \mathbf{Z}^2$ tel que

$$a = bq + r, \text{ avec } 0 \leq r < |b|;$$

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

Par exemple, on a $17 = 3 \cdot 5 + 2$, $17 = -3 \cdot -5 + 2$, $-17 = -4 \cdot 5 + 3$, $-17 = 4 \cdot -5 + 3$.

Si $a = bq$ et on dit que b *divise* a dans $\mathbf{Z}$ ou que b est un *diviseur* de a. On écrit $b|a$. On dit aussi que a est un *multiple* de b. Si $a = bq + r$ avec $0 \leq r < |b|$, on notera $r = a \,(\mathrm{mod}\, b)$ le reste de la division (on dit a modulo b).

$\mathbf{Z}$ n'est pas un corps : les seuls éléments non nuls qui ont un inverse pour la multiplication sont $+1, -1$, i.e. $U_{\mathbf{Z}} = \{-1, +1\}$.

Un diviseur de a distinct de 1, -1, a et $-a$ - s'il en existe - est appelé *diviseur propre* de a.

Un *nombre premier* p est un entier > 1 dont les seuls diviseurs positifs sont 1 et p (autrement dit, un nombre premier n'a pas de diviseur propre). On montre que l'ensemble $\mathcal{P}$ des nombres premiers est infini.

Théorème fondamental de l'arithmétique - Tout entier relatif $n \in \mathbf{Z}^*$ s'écrit de manière unique (à permutation près des facteurs) sous la forme

$$n = \varepsilon(n) \prod_{p \in \mathcal{P}} p^{n_p}, \text{ où } n_p \in \mathbf{N}^*, \varepsilon(n) = \pm 1.$$

Ce dernier résultat a un inconvénient majeur : on ne connaît pas d'algorithme "rapide" pour factoriser un entier relatif. Cet inconvénient se révèle aussi un avantage, et il est à la base des méthodes de cryptographie à clé publique.

L'algèbre des polynômes

Si $\mathbf{K}$ est un corps commutatif, considérons l'ensemble $\mathbf{K}[X]$ des polynômes à coefficients dans $\mathbf{K}$ en une indéterminée X, muni des lois internes $+$ (addition des polynômes) et $\times$ (multiplication des polynômes) et de la loi externe, multiplication par les éléments de $\mathbf{K}$, notée $\cdot$. $\mathbf{K}[X]$ est une $\mathbf{K}$-algèbre, c'est-à-dire, est un anneau commutatif unitaire et intègre, et un $\mathbf{K}$-espace vectoriel.

Soit $P = a_0 + a_1X + \cdots + a_nX^n$ un polynôme non nul de $\mathbf{K}[X]$: si $a_n \neq 0$, on dit que P est de *degré* n (on note $\deg P$) et a_n s'appelle le *coefficient dominant* de P ; si P est de degré n et $a_n = 1$, on dit que P est *unitaire*. Si $P = 0$, on convient que P est de degré $-\infty$.

De plus, $\mathbf{K}[X]$ est un anneau euclidien :

Théorème. Division euclidienne.
Pour tout $(A,B) \in K[X]^2$, $B \neq 0$, il existe un couple unique $(Q,R) \in K[X]^2$ tel que

$$A = BQ + R, \text{ avec } R = 0 \text{ ou } \deg R < \deg B.$$

Si le reste de la division euclidienne de A par B est nul, on dit que B divise (ou est un *diviseur* de) A (on note $B|A$) ou que A est un *multiple* de B. On s'intéresse aux *diviseurs propres* d'un polynôme non nul A, c'est à dire aux polynômes B tels que $0 < \deg B < \deg A$ (s'il en existe) .

Un polynôme non nul P de degré ≥ 1 est dit *irréductible*, s'il n'a pas de diviseur propre. Les polynômes unitaires irréductibles sont, pour $\mathbf{K}[X]$, l'"analogue" des nombres premiers pour $\mathbf{Z}$.

Les anneaux euclidiens sont également factoriels, c'est-à-dire, tout élément s'écrit de façon unique (aux unités près) comme le produit de facteurs irréductibles

Théorème. *Soit $P \in K[X]$, $P \neq 0$, alors P s'écrit de façon unique (à l'ordre près)*

$$P = \lambda P_1^{n_1} \dots P_r^{n_r}$$

où $\lambda \in K^*$, les P_i sont unitaires et irréductibles, distincts deux à deux, et $n_i \in \mathbf{N}$.

Seuls les polynômes constants non nuls ont un inverse (pour la multiplication) dans l'anneau $\mathbf{K}[X]$, i.e. $U(K[X]) = K^*$.

Un corps $\mathbf{K}$ est un anneau euclidien, en considérant le stathme $d(a) = 0$ si $a \in K^*$ et $d(0) = -\infty$. L'anneau $\mathbf{Z}[\sqrt{-1}]$ est un anneau euclidien mais $\mathbf{Z}[\sqrt{-5}]$ n'est pas euclidien.

L'objet de cette partie est de découvrir les conséquences de l'algorithme d'Euclide. On évitera soigneusement d'utiliser la factorialité des anneaux euclidiens considérés ($\mathbf{Z}$ ou $\mathbf{K}[X]$), car c'est en général un problème difficile que de trouver la factorisation.

Définition. Soit A un anneau, on note $\mathcal{D}(a)$ l'ensemble des diviseurs de a : $\{d \in A; d \mid n\}$.

Le résultat suivant sert de point de départ à l'algorithme d'Euclide.

Lemme. *Pour tout $a,b \in A$ et tout $\mathbf{K} \in A$, on a $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a-kb) \cap \mathcal{D}(b)$.*

Preuve. Si d vise a et d divise b, alors $a = d \cdot a'$ et $b = d \cdot b'$ donc $a - kb = d(a' - b')$ est un multiple de d. Donc $\mathcal{D}(a) \cap \mathcal{D}(b) \subset \mathcal{D}(a-kb) \cap \mathcal{D}(b)$. Mais alors $\mathcal{D}(a-kb) \cap \mathcal{D}(b) \subset \mathcal{D}((a-kb) - (-kb)) \cap \mathcal{D}(b) = \mathcal{D}(a) \cap \mathcal{D}(b)$. □

1 L'anneau des entiers relatifs

On considère l'*algorithme d'Euclide* suivant, pour définir l'ensemble des diviseurs communs de a et b. Partons de $r_0 = a$, $r_1 = b$. On définit par récurrence $r_{i+1} = 0$ si $r_i = 0$, sinon $r_{i+1} = r_{i-1} \pmod{r_i}$.

Proposition 1.1. *La suite r_i est décroissante puis nulle.*

La suite des restes $(r_k)_{k\geq 2}$ étant une suite de nombres positifs strictement décroissante, on obtient un reste nul au bout d'un nombre fini de divisions. Notons n l'indice du dernier reste non nul. À chaque étape, on a $\mathcal{D}(r_i)\cap\mathcal{D}(r_{i+1}) = \mathcal{D}(r_{i-1})\cap\mathcal{D}(r_i)$, donc $\mathcal{D}(a)\cap\mathcal{D}(b) = \mathcal{D}(r_n)\cap\mathcal{D}(r_{n+1}) = \mathcal{D}(r_n)$.

$$\star^{\star}\star$$

Les diviseurs communs de a et de b sont donc exactement les diviseurs de r_n. On appelle $d = \text{pgcd}(a,b) = r_n$ le pgcd de a et b.

Exemple 1.2. $\text{pgcd}(415,175) = \text{pgcd}(175,65) = \text{pgcd}(65,45) = \text{pgcd}(45,20) = \text{pgcd}(20,5) = \text{pgcd}(5,0) = 5$.

Proposition 1.3. *Soit a et b deux entiers non nuls tel que a ne divise pas b et réciproquement. Le plus grand commun diviseur (pgcd, gcd en anglais) de a et b est le dernier reste non nul de l'algorithme d'Euclide. On le note* $\text{pgcd}(a,b)$ *ou* (a,b) *ou* $a\wedge b$. *On a donc $\mathcal{D}(a)\cap\mathcal{D}(b) = \mathcal{D}(d)$: tout diviseur commun de a et de b est un diviseur de d.*

$$(\delta|a \text{ et } \delta|b) \Longleftrightarrow \delta|d.$$

On peut borner le nombre d'étapes dans l'algorithme d'Euclide :

Théorème 1.4 (Théorème de Lamé)**.** *Considérons la suite de Fibonacci, définie par $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$. Soit a et b deux entiers naturels tels que $0 < b < a$. et $d = (a,b)$. Si l'algorithme d'Euclide s'arrête au bout de n pas, alors on a :*

$$a \geq dF_{n+2}, \quad b \geq dF_{n+1}.$$

Preuve. On raisonne par récurrence sur n. Si $n = 1$, alors $b|a$ et $b = d = dF_2$ et $a \geq b = dF_1$. Soit $n > 1$ et supposons que l'algorithme s'arrête au bout de $n+1$ pas. Appliquant la récurrence à $(b, r_2 = a - qb)$, on obtient $b \geq dF_{n+2}, r_2 \geq dF_{n+1}$. Mais $a = r_2 + qb \geq r_2 + b \geq d(F_{n+1} + F_{n+2}) = dF_{n+3}$. CQFD

Suite de Fibonacci

La suite de Fibonacci est une suite récurrente linéaire d'ordre 2. Elle vérifie l'équation (linéaire)

$$F_{n+2} = F_{n+1} + F_n, n \geq 0$$

dans $\mathbf{R}^{\mathbf{N}}$. D'après le cours de seconde année, l'ensemble des suites réelles vérifiant cette équation forme un sous-espace vectoriel de dimension 2. Une base de ce sous-espace est donné par les suites géométriques $(r^n)_{n\geq 0}$ où r est solution de l'équation caractéristique : $r^2 = r + 1$. On obtient le nombre d'or $r = \varphi = \frac{1}{2}(1+\sqrt{5})$ et $r = -\dfrac{1}{\varphi}$.

On déduit ensuite que $F_n = \alpha\varphi^n + \beta(-1/\varphi)^n$, puis que $F_n = \dfrac{1}{\sqrt{5}}\left(\varphi^n + (-\frac{1}{\varphi})^n\right)$.

Remarquons enfin par récurrence que $\varphi^n = \varphi F_n + F_{n-1}$ pour tout n.

Corollaire 1.5. *Soit $0 \leq b < a$. L'algorithme d'Euclide calcule (a,b) en $n = \log_\varphi b + 1$ étapes.*

Preuve. On a $\varphi^{n+1} = \varphi F_{n+1} + F_n$ et $b \geq dF_{n+1} \geq F_{n+1}$ donc $n+1 = \log_\varphi(\varphi F_{n+1} + F_n) \leq \log_\varphi(\varphi F_{n+1} + F_{n+1}) = \log_\varphi(\varphi^2 F_{n+1}) \leq 2 + \log_\varphi b$. CQFD

On dira que l'algorithme d'Euclide a une *complexité arithmétique* $O(\log n)$, si $|a|, |b| \leq n$. Nous verrons ultérieurement que nous pouvons donner une estimation plus fine de la complexité de cet algorithme en considérant la façon de représenter les entiers.

1.1 Identité de Bézout

Reprenons l'exemple précédent du calcul de $(415,175)$. En effectuant des opérations élémentaires sur les lignes $(L_0) : 415 = 1\cdot 415 + 0\cdot 175$ et $(L_1) : 175 = 0\cdot 415 + 1\cdot 175$, on obtient

$$\begin{array}{rrcrcr}
(L_0) & 415 & = & 1\cdot 415 & + & 0\cdot 175 \\
(L_1) & 175 & = & 0\cdot 415 & + & 1\cdot 175 \\
(L_2 = L_0 - 2L_1) & 65 & = & 1\cdot 415 & - & 2\cdot 175 \\
(L_3 = L_1 - 2L_2) & 45 & = & -2\cdot 415 & + & 5\cdot 175 \\
(L_4 = L_2 - 2L_3) & 20 & = & 3\cdot 415 & - & 7\cdot 175 \\
(L_5 = L_3 - 2L_4) & 5 & = & -8\cdot 415 & + & 19\cdot 175 \\
(L_6 = L_4 - 4L_5) & 0 & = & 35\cdot 415 & - & 83\cdot 175
\end{array}$$

Cet algorithme s'appelle *Algorithme d'Euclide étendu*. Il permet de démontrer :

Théorème 1.6 (Bézout)**.** *Soit $(a,b) \in \mathbf{Z}^2$, non nuls et $d = (a,b)$. Alors il existe $(u,v) \in \mathbf{Z}^2$, $au + bv = d$.*

Preuve. $r_0 = a$, $r_1 = b$, étant définis, on construit q_i et r_{i+1} comme le quotient et le reste de la division euclidienne de r_{i-1} par r_i : $r_{i+1} = r_{i-1} - q_i r_i$. En ayant posé $u_0 = 1$, $u_1 = 0$, $v_0 = 0$, $v_1 = 1$, on définit ensuite, $u_{i+1} = u_{i-1} - q_i u_i$ et $v_{i+1} = v_{i-1} - q_i v_i$. On a alors, par récurrence,

$$r_i = u_i a + v_i b.$$

En particulier $r_n = u_n a + v_n b, \quad r_{n+1} = 0 = u_{n+1} a + v_{n+1} b.$ CQFD

L'algorithme d'Euclide étendu fournit donc une identité de Bézout (rang n) et une solution de l'équation homogène $ax + by = 0$, dans $\mathbf{Z}^2$ (rang $n+1$).

Utilisant l'identité de Bézout, on déduit le lemme de Gauss.

Lemme 1.7 (Lemme de Gauss)**.** *Soit a, b et c trois entiers relatifs tels que a divise bc. Si $(a,b) = 1$ alors $a|c$.*

Preuve. On écrit $au + bv = 1$. On déduit que a divise $bc \times v$ donc $a \times uc + b \times vc = c$ CQFD

Corollaire 1.8. *Soit a, b deux entiers divisant c. Si $(a,b) = 1$ alors ab divise c.*

Preuve. Si $c = \lambda a = \mu b$ alors a divise μ d'après le Lemme de Gauss 1.7 et ab divise c. □

Corollaire 1.9. *Soit a et b deux entiers. Alors pour tout entier k, on a $(k\cdot a, k\cdot b) = k\cdot(a,b)$. En particulier $a/(a,b)$ et $b/(a,b)$ sont premiers entre-eux (on dit étrangers).*

Preuve. Posons $d = (a,b) = au + bv$. Si δ divise ka et kb alors $ka = \delta a'$ et $kb = \delta b'$. Alors on obtient $kd = \delta(a'u + b'v)$ et $\delta \mid kd$. Réciproquement, si $\delta \mid kd$, alors δ divise ka et kb et dont (ka, kb). CQFD

On peut alors définir le ppcm de deux entiers.

Définition 1.10. *Soit a et b deux entiers, et d leur pgcd. $N = \dfrac{ab}{d}$ est le* ppcm (a,b)*. On a*

$$(a|n \text{ et } b|n) \Longleftrightarrow (N|n)$$

Preuve. $N = \dfrac{a}{d}b = \dfrac{b}{d}a$ est un multiple commun de a et de b. Si a et b divisent simultanément n, alors a/d et b/d divisent n/d et, par conséquent (Lemme de Gauss 1.7) leur produit N/d divise n/d donc N divise n. L'ensemble des multiples communs de a et de b est l'ensemble des multiples de N. CQFD

1.2 Résolution de l'équation diophantienne linéaire : $ax+by=c$

Commençons par remarquer que

Théorème 1.11. *Soit a, b et c des entiers relatifs. L'équation $ax+by=c$ a (au moins) une solution si et seulement si $d=\text{pgcd}(a,b)|c$.*

Preuve. Si une solution particulière (x_0,y_0) existe, nous constatons que ax_0+by_0 est un multiple de d et donc d doit diviser c Réciproquement, si $c=\lambda d$ et (u,v) sont des coefficients de Bézout vérifiant $ua+vb=d$, alors $(x_0,y_0)=\lambda(u,v)$ est une solution particulière.

Comme pour toute équation affine, toute solution de l'équation $ax+by=c$ est la somme d'une solution particulière (x_0,y_0), si elle existe, et d'une solution de l'équation homogène : $ax+by=0$.

Si (x,y) est solution de l'équation homogène $ax+by=0$ alors elle est aussi solution de $\frac{a}{d}x+\frac{b}{d}y=0$. Mais alors $\frac{a}{d}$ divise $\frac{b}{d}\cdot y$, donc $\frac{a}{d}$ divise y, d'après le corollaire du Lemme de Gauss 1.9. Donc $y=k\frac{a}{d}$ et par suite $(x,y)=k(-\frac{b}{d},\frac{a}{d})$ où $k\in\mathbf{Z}$.

Écriture matricielle dans l'algorithme d'Euclide

Posons $U_i=\begin{pmatrix}0 & 1\\ 1 & -q_i\end{pmatrix}$, on peut alors écrire

$$\begin{pmatrix} r_i & u_i & v_i \\ r_{i+1} & u_{i+1} & v_{i+1}\end{pmatrix} = U_i\begin{pmatrix} r_{i-1} & u_{i-1} & v_{i-1} \\ r_i & u_i & v_i\end{pmatrix} = U_i\cdot U_{i-1}\cdots U_1\cdot\begin{pmatrix} a & 1 & 0\\ b & 0 & 1\end{pmatrix}$$

On en déduit en particulier :

1. Dans l'algorithme d'Euclide étendu, on a à chaque étape $\begin{vmatrix} u_i & v_i \\ u_{i+1} & v_{i+1}\end{vmatrix} = (-1)^i$.
2. $u_{n+1}=\dfrac{b}{d}(-1)^{n+1}$, $v_{n+1}=\dfrac{a}{d}(-1)^n$.
3. $|u_n|\le\dfrac{b}{2d}$, $|v_n|\le\dfrac{a}{2d}$.

Preuve.

1. On a en effet $\begin{pmatrix} u_i & v_i \\ u_{i+1} & v_{i+1}\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & -q_i\end{pmatrix}\cdot\begin{pmatrix} u_{i-1} & v_{i-1} \\ u_i & v_i\end{pmatrix}$, d'où le résultat en considérant le déterminant.
2. On a aussi $\begin{vmatrix} r_{i-1} & u_{i-1} \\ r_i & u_i\end{vmatrix} = (-1)^{i-1}\begin{vmatrix} r_0 & u_0 \\ r_1 & u_1\end{vmatrix}$, soit lorsque $i=n+1$: $du_{n+1}=(-1)^n\cdot(-b)$. On fait de même avec v_{n+1}.
3. De $u_{k+1}=u_{k-1}-q_ku_k$, on déduit que la suite u_k est de signe alterné, pour $k\ge1$, puis $|u_{k+1}|=|u_{k-1}|+|q_ku_k|>|u_k|$. Mais $q_n\neq1$ car $r_{n-1}=q_nr_n>r_n$ donc $q_n\ge2$ et $|u_n|\le\frac{1}{2}|u_{n+1}|$.

L'algorithme d'Euclide étendu fournit donc une identité de Bézout et une solution de l'équation homogène (dans $\mathbf{Z}^2$) : $ax+by=0$. Il est remarquable, que la solution obtenue par l'algorithme d'Euclide étendu engendre l'ensemble des solutions de l'équation homogène et que la solution particulière soit une solution particulière minimale.

1.3 Anneau quotient

Tout sous-groupe de $(\mathbf{Z},+)$, appelé aussi *idéal* de l'anneau $\mathbf{Z}$, (voire sous $\mathbf{Z}$-module de $\mathbf{Z}$) est de la forme $n\mathbf{Z}$, car $\mathbf{Z}$ est euclidien. On dit que $\mathbf{Z}$ est un anneau *principal*.

Exercice 1.12. En terme d'idéaux, si a et b sont des entiers relatifs et d et N sont leur pgcd et leur ppcm, on a $a\mathbf{Z}\cap b\mathbf{Z}=N\mathbf{Z}$, $a\mathbf{Z}+b\mathbf{Z}=d\mathbf{Z}$.

Soit $n > 1$ un entier. Dans $\mathbf{Z}$, on définit la relation d'équivalence notée $\equiv$

$$(a,b) \in \mathbf{Z}^2, a \equiv b \iff b-a \in n\mathbf{Z}.$$

On note alors $a \equiv b \pmod{n}$ et on dit que *a est congru à b modulo n*. Si $a \in \mathbf{Z}$, la classe de a pour la relation d'équivalence $\equiv$ est le sous-ensemble de $\mathbf{Z}$ suivant

$$\overline{a} = \{a+nk, k \in \mathbf{Z}\} = a+n\mathbf{Z}.$$

L'ensemble des classes d'équivalence est noté $\mathbf{Z}/n\mathbf{Z}$. L'ensemble $\mathbf{Z}/n\mathbf{Z}$ contient exactement n éléments distincts :

$$\mathbf{Z}/n\mathbf{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Par abus de notation on notera souvent de la même façon (quand il n'y a pas d'ambiguïté) un élément de $\mathbf{Z}$ et sa classe. Donc on pourra écrire

$$\mathbf{Z}/n\mathbf{Z} = \{0, 1, \ldots, (n-1)\}.$$

On définit deux lois internes dans $\mathbf{Z}/n\mathbf{Z}$ (déduites de celles de $\mathbf{Z}$ et compatibles avec la relation d'équivalence $\equiv$) :

$$\overline{a} + \overline{b} := \overline{a+b}, \quad \overline{a} \times \overline{b} := \overline{ab}.$$

Proposition 1.13. $(\mathbf{Z}/n\mathbf{Z}, +, \times)$ *est un anneau commutatif unitaire.*

D'après l'identité de Bézout, l'ensemble $U(\mathbf{Z}/n\mathbf{Z})$ des inversibles de $\mathbf{Z}/n\mathbf{Z}$ est exactement l'ensemble des $i+n\mathbf{Z}$ tels que $(i,n) = 1$. Cet ensemble est en bijection avec $\{1 \leq i \leq n-1; (i,n) = 1\}$. Le cardinal de $U(\mathbf{Z}/n\mathbf{Z})$ est noté $\varphi(n)$. La fonction $n \mapsto \varphi(n)$ est appelée *fonction caractéristique d'Euler*. En écrivant l'ensemble $\{\frac{1}{1}, \ldots, \frac{n}{n}\} = \{\frac{a}{d}; (a,d) = 1, 0 < a < d | n\}$, (voir le cours de L. Zapponi [9]), on déduit la *formule d'Euler* : $\sum_{d|n} \varphi(d) = n$.

Générateurs

Le groupe $(\mathbf{Z}/n\mathbf{Z}, +)$ est cyclique : il est engendré par $\overline{1}$. $U(\mathbf{Z}/n\mathbf{Z})$ est également l'ensemble des générateurs du groupe $(\mathbf{Z}/n\mathbf{Z}, +)$. En effet, si $\overline{a}$ engendre $\mathbf{Z}/n\mathbf{Z}$ alors $\overline{1} = k\overline{a} = \overline{k \cdot a}$ et a est inversible modulo n, et d'ailleurs $\overline{k}$ est son inverse. L'identité de Bézout permet de déterminer si un entier m est inversible modulo n et le cas échéant de trouver son inverse.

$(\mathbf{Z}/n\mathbf{Z}, +)$ est un groupe cyclique et tout groupe cyclique de même cardinal est isomorphe à $\mathbf{Z}/n\mathbf{Z}$, par exemple le groupe des racines complexes n-èmes de l'unité. Pour déterminer un isomorphisme ψ entre un groupe cyclique $(G, \cdot)$ d'ordre n et $\mathbf{Z}/n\mathbf{Z}$, il suffit de choisir un générateur g de G et de poser $\psi(g) = \overline{1}$.

Dans un groupe fini $(G, \cdot)$, l'*ordre* $\operatorname{ord}(a)$ d'un élément a de G est le plus petit entier d strictement positif qui vérifie $a^n = 1$. C'est le générateur positif du sous-groupe de $\mathbf{Z}$, noyau de $n \mapsto a^n$, morphisme de $(\mathbf{Z}, +)$ vers $(G, \cdot)$. Ainsi $a^n = 1$ équivaut à $\operatorname{ord}(a) \mid n$ et le théorème de Lagrange affirme que $\operatorname{ord}(a)$ divise $|G|$.

Lemme 1.14. *Soit a un élément d'ordre fini d'un groupe G. Alors a^d est d'ordre* $\dfrac{\operatorname{ord} a}{(d, \operatorname{ord}(a))}$.

Preuve. Posons $b = a^d$ et examinons l'ensemble des k tels que $b^k = 1$. $b^k = 1$ si et seulement si $a^{dk} = 1$, c'est-à-dire, $n | dk$, c'est-à-dire, $n/(d,n) | d/(d,n)k$, c'est-à-dire, $n/(d,n) | k$, d'après le Lemme de Gauss, puisque $n/(d,n)$ et $d/(d,n)$ sont premiers entre-eux. On a donc $b^k = 1$ si et seulement si $n/(d,n)$ divise k. CQFD

On déduit que $a \in \mathbf{Z}/n\mathbf{Z}$ est d'ordre d si d divise n, d'une part, et si $a = \frac{n}{d}a'$ avec $(a', d) = 1$. Il existe $\varphi(d)$ éléments d'ordre d dans $\mathbf{Z}/n\mathbf{Z}$, soit la formule d'Euler : $\sum_{d|n} \varphi(d) = n$.

Le corps $\mathbf{F}_p$

On remarque en particulier que $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est un nombre premier. Lorsque $n=p$ est un nombre premier, on note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$. Le corps $\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$ est un corps fini commutatif et nous avons, d'après le théorème de Lagrange, $x^{p-1}=1$ pour tout $x\neq 0$ dans $\mathbf{Z}/p\mathbf{Z}$.

On en déduit le

Théorème 1.15 (Théorème de Fermat)**.** *Soit p un nombre premier. Pour tout $a\in\mathbf{Z}$, on a $a^p\equiv a\pmod p$.*

Une conséquence du théorème de Fermat est que l'inverse de a dans $\mathbf{F}_p^*$ est a^{p-2}.

Nous verrons (Lemme 4.1) que $(\mathbf{Z}/p\mathbf{Z})^*$ est un groupe cyclique.

Exemple 1.16. Soit $p=7$ et $K=\mathbf{Z}/p\mathbf{Z}$. On voit que $2^3\equiv 1\pmod 7$ donc 2 est d'ordre 3. -1 est d'ordre 2 (c'est toujours le cas pour tout p), donc $-2=5$ est d'ordre 6. On a ici utilisé une propriété : *si a et b sont d'ordre n et m premiers entre-eux, alors ab est d'ordre nm*. Les 2 générateurs de $(\mathbf{Z}/7\mathbf{Z})^*$ sont 5 et 3.

Soit $p=31$ et $K=\mathbf{Z}/p\mathbf{Z}$. 2 est d'ordre 5 car $2^5\equiv 1\pmod p$. -2 est d'ordre 10, par le même argument que précédement. On a $5^2=25=-6$, donc $5^3=-30=1$. 5 est donc d'ordre 3. Par conséquent $-10=21$ est d'ordre 30 et est un générateur de K^*. Le nombre de générateurs de K^* est $\varphi(30)=8$.

Le théorème de Fermat se généralise en le théorème d'Euler.

Théorème 1.17 (Théorème d'Euler)**.** *Soit n un entier naturel. Pour tout $a\in\mathbf{Z}$, si $(a,n)=1$ alors on a $a^{\varphi(n)}\equiv 1\pmod n$.*

1.4 Théorème Chinois

Le « théorème chinois » (Chinese Remainder Theorem) apparaît pour la première fois dans un traité appelé Sun Tzu Suan Ching ou Jiuzhang Suhanshu (date estimée : entre 280 et 473). Voir [2, 7].

Il s'énonce ainsi, sous forme d'énigme, souvent associée aux généraux préoccupés par le comptage de leur troupe : *Soit des objets en nombre inconnu. Si on les range par 3 il en reste 2. Si on les range par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien a-t-on d'objets ?*

La résolution proposée : *Multiplie le reste de la division par 3, c'est-à-dire 2, par 70, ajoute-lui le produit du reste de la division par 5, c'est-à-dire 3, avec 21 puis ajoute le produit du reste de la division par 7, c'est-à-dire 2 par 15. Tant que le nombre est plus grand que 105, retire 105.*

On peut cependant remarquer que :

— 70 a pour reste 1 dans la division par 3 et pour reste 0 dans les divisions par 5 et 7 ;

— 21 a pour reste 1 dans la division par 5 et pour reste 0 dans les divisions par 3 et 7 ;

— 15 a pour reste 1 dans la division par 7 et pour reste 0 dans les divisions par 3 et 5.

Le nombre $2\times 70+3\times 21+2\times 15$ a bien alors pour restes respectifs 2, 3 et 2 dans les divisions par 3, 5 et 7. Enfin, comme 105 a pour reste 0 dans les trois types de division, on peut l'ôter ou l'ajouter autant de fois que l'on veut sans changer les valeurs des restes. La plus petite valeur pour le nombre d'objets est alors de 23.

Il correspond à l'énoncé mathématique suivant :

Théorème 1.18. *Soit $n_1,\dots,n_r$ des entiers premiers entre-eux deux-à-deux. Posons $N=n_1\cdots n_r$. Soit $x_1,\dots,x_r$ des entiers. Il existe un unique entier x modulo N, tel que $x\equiv x_1\pmod{n_1},\dots,x\equiv x_r\pmod{n_r}$.*

Preuve. L'unicité est une conséquence du Lemme de Gauss (1.7), puisque deux solutions x et x' vérifient $n_i|(x-x')$ et donc N divise leur différence. Pour ce qui est de l'existence, considérons $N_i=N/n_i$. Il existe u_i,v_i, tels que $u_in_i+v_iN_i=1$, d'après l'identité de Bézout. Posons $e_i=v_iN_i$, on en déduit alors que $e_i=\delta_{i,j}\pmod{n_j}$ et par suite, l'entier $x=x_1e_1+\cdots+x_re_r$ est une solution. CQFD

L'application $(x_1,\dots,x_r)\mapsto x_1e_1+\cdots+x_re_r\pmod N$ est un morphisme d'anneau. C'est en fait l'isomorphisme :

Théorème 1.19 (Théorème chinois)**.** *Soit $n_1,\dots,n_r$ des entiers premiers entre-eux deux-à-deux et $N = n_1\cdots n_r$. Alors on a l'isomorphisme d'anneaux suivant : $\mathbf{Z}/n_1\mathbf{Z}\times\cdots\times\mathbf{Z}/n_r\mathbf{Z}\simeq\mathbf{Z}/N\mathbf{Z}$.*

Exemple 1.20. Cherchons à résoudre $x\equiv a\,(\mathrm{mod}\,101), x\equiv b\,(\mathrm{mod}\,5)$.

De l'identité de Bézout $1\times 101-20\times 5=1$, on déduit que $x=-100\times a+101\times b$ est solution.

Dans le cas où $a=90$ et $b=4$, on obtient $x=-9000+404\,(\mathrm{mod}\,505)$.

L'exemple précédent nous montre qu'il convient d'améliorer notre méthode. On considérera plutôt : Soit n et m deux entiers premiers entre-eux. Soit (u,v) tels que $|u|<b$ et $|v|<a$ et $au+bv=1$. Alors $x=n\Big(u(b-a)\,(\mathrm{mod}\,m)\Big)+a$ est solution du système de congruence $x\equiv a\,(\mathrm{mod}\,n), x\equiv b\,(\mathrm{mod}\,m)$. À chaque étape du calcul de x, nous restons dans l'intervalle $[0, n\cdot m[$.

Remarque 1.21. En général, si n et m sont des entiers, les ensembles $\mathbf{Z}/nm\mathbf{Z}$ et $\mathbf{Z}/n\mathbf{Z}\times\mathbf{Z}/m\mathbf{Z}$ sont en bijection puisqu'ils ont le même cardinal. Ils ne sont isomorphes que si n et m sont premiers entre-eux (voir la suite du cours). Par exemple, les groupes additifs $(\mathbf{Z}/2\mathbf{Z})^2$ et $\mathbf{Z}/4\mathbf{Z}$ ne sont pas isomorphes car le premier n'a pas d'éléments d'ordre 4.

Lorsque n et m sont premiers entre-eux, on a $\mathbf{Z}/n\mathbf{Z}\times\mathbf{Z}/m\mathbf{Z}\simeq\mathbf{Z}/nm\mathbf{Z}$, d'où on déduit que $U(\mathbf{Z}/nm\mathbf{Z})\simeq U(\mathbf{Z}/n\mathbf{Z}\times\mathbf{Z}/m\mathbf{Z})=U(\mathbf{Z}/n\mathbf{Z})\times U(\mathbf{Z}/m\mathbf{Z})$. Par conséquent $\varphi(nm)=\varphi(n)\varphi(m)$. On dit que la fonction φ est *multiplicative*.

2 L'anneau des polynômes

On considère l'ensemble $A[X]$ des polynômes à coefficients dans un anneau A, commutatif et unitaire, en une indéterminée X muni des lois internes $+$ (addition des polynômes) et $\times$ (multiplication des polynômes). $(A[X],+,\times,.)$ est un anneau unitaire.

Lorsque $A=\mathbf{K}$ est un corps, on dispose de la loi externe, multiplication par les éléments de $\mathbf{K}$, notée $\cdot$. Dans ce cas $(K[X],+,\times,.)$ est une $\mathbf{K}$-*algèbre*, c'est-à-dire, $(A[X],+,\times)$ est un anneau commutatif unitaire (et intègre), $(K[X],+,.)$ est un $\mathbf{K}$-espace vectoriel (de dimension infinie).

Remarque 2.1. Lorsque A n'est pas un corps, on dispose également d'une loi externe $\cdot$. On dit que $A[X]$ est un A-module.

2.1 Algorithme d'Euclide

Soit A et B deux polynômes non nuls, $\deg A\geq\deg B$. On cherche leurs diviseurs communs (et donc leur PGCD). On pose $R_0=A, R_1=B$ et on fait les divisions euclidiennes successives

$$\begin{array}{rcll} A & = & BQ_1+R_2, & \deg R_2<\deg B\\ B & = & R_2Q_2+R_3, & \deg R_3<\deg R_2\\ R_2 & = & R_3Q_3+R_4, & \deg R_4<\deg R_3\\ & \vdots & & \vdots\\ R_{n-1} & = & R_nQ_n+0 & \end{array}$$

La suite des restes (R_k) étant une suite de polynômes dont les degrés forment une suite strictement décroissante, on obtient un reste nul au bout d'un nombre fini de divisions.

Les diviseurs communs de A et de B sont les diviseurs communs de R_k et R_{k+1} donc l'ensemble des diviseurs du dernier reste non nul : R_n. Le PGCD de A et B est donc le dernier reste non nul R_n rendu unitaire. On déduit alors

Proposition 2.2. *Soit A et B deux polynômes non nuls. A et B ont un* pgcd *D et on a : $D|A, D|B$ et tout diviseur commun de A et de B est un diviseur de D.*

Bézout

De la même façon que pour le calcul de pgcd de deux entiers relatifs, nous définissons l'algorithme d'Euclide étendu : soit $R_0 = A$, $R_1 = B$, posons $U_0 = 1$, $U_1 = 0$, $V_0 = 0$, $V_0 = 1$.

Nous calculons successivement $Q_i = R_{i-1} \div R_i$, puis $R_{i+1} := R_{i-1} \pmod{R_i} = R_{i-1} - R_i Q_i$. En posant $U_{i+1} = U_{i-1} - U_i Q_i, V_{i+1} = V_{i-1} - V_i Q_i$, nous obtenons à chaque étape $R_i = U_i A + V_i B$.

Théorème 2.3 (Identité de Bézout)**.** *Soit $(P,Q) \in K[X]^2$, non nuls. Alors $P \wedge Q = D$ existe et*

$$\text{il existe } (U,V) \in K[X]^2,\ PU + QV = D\,.$$

Corollaire 2.4.

1. $(P \wedge Q) | D \iff$ *il existe* $(U,V) \in K[X]^2,\ PU + QV = D$.
2. *Lemme de Gauss :* $A|BC$ *et* $A \wedge B = 1 \Rightarrow A|C$.
3. *Si P est irréductible et $P|AB$, alors $P|A$ ou $P|B$.*
4. *si $A \wedge B = 1$ et si $A|C$ et $B|C$, alors $AB|C$.*

2.2 Quotient de $K[X]$

Définition 2.5. *Soit $(A,+,*)$ un anneau commutatif. Un sous-ensemble I de A est un* idéal de l'anneau *A si*

— *I est un sous-groupe de $(A,+)$,*
— *pour tout $x \in A$, pour tout $a \in I, x * a \in I$.*

Soit $P \in K[X]$. $\langle P \rangle = PK[X] = \{PQ,\ Q \in K[X]\}$, l'ensemble des multiples de P est un idéal de $K[X]$. Remarquons que $\{0\} = \langle 0 \rangle$ et $K[X] = \langle \lambda \rangle$, avec $\lambda \in K^*$, sont des idéaux de $K[X]$: on dit que $\{0\}$ et $K[X]$ sont les *idéaux triviaux* de $K[X]$. Les idéaux non triviaux sont appelés *idéaux propres*. Les idéaux de $K[X]$ sont aussi des sous K-espaces vectoriels de $K[X]$.

$K[X]$ est un anneau principal, c'est-à-dire, tout idéal I de $K[X]$ est de la forme $I = \langle P \rangle$, où P est unitaire. Soit $I = \langle P \rangle$ un idéal propre de $K[X]$, avec P unitaire. Dans $K[X]$ on définit une relation associée à I en posant

$$(A,B) \in K[X]^2, A \equiv B \iff B - A \in I\,.$$

On montre que c'est une relation d'équivalence et on a $\mathrm{cl}(P) = \mathrm{cl}(0)$.
Chaque classe d'équivalence a un représentant unique R tel que $R = 0$ ou $\deg R < \deg P$. On note $K[X]/\langle P \rangle$ l'ensemble des classes pour cette relation. Si $P = a_0 + a_1 X + \cdots + X^m \in K[X]$. On a alors

$$K[X]/\langle P \rangle = \{\mathrm{cl}(A), A \in K[X]\} = \{\mathrm{cl}(A), A \in K[X]\,;\, \deg A < m\}.$$

En notant $\alpha := \mathrm{cl}(X)$ dans $K[X]/\langle P \rangle$, on a

$$K[X]/\langle P \rangle = \{c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1},\ c_i \in K\}\,.$$

On écrira $K[X]/\langle P \rangle = K[\alpha]$ avec la condition $P(\alpha) = 0$.

On définit deux lois internes dans $K[X]/\langle P \rangle$ et une loi externe, toutes trois déduites des lois de $K[X]$, en posant

$$\mathrm{cl}(A) + \mathrm{cl}(B) = \mathrm{cl}(A+B), \quad \mathrm{cl}(A) * \mathrm{cl}(B) = \mathrm{cl}(AB), \quad \lambda ._K \mathrm{cl}(A) = \mathrm{cl}(\lambda A)$$

Proposition 2.6. *$(K[X]/\langle P \rangle, +, *, .{}_K)$ est une K-algèbre.*

Proposition 2.7. *Soit K un corps et $P \in K[X]$ un polynôme unitaire de degré $m \geq 1$. Alors $K[X]/\langle P \rangle$ est un K-espace vectoriel de dimension $m = \deg P$. Si on pose $\alpha := \mathrm{cl}(X)$, une base de $= K[X]/\langle P \rangle$ sur K est $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$.*

Corollaire 2.8. *Soit K un corps fini ayant q éléments et $P \in K[X]$ un polynôme unitaire de degré $m \geq 1$. Alors $|K[X]/\langle P \rangle| = q^m$.*

D'après l'identité de Bézout, les inversibles de $K[X]/\langle P\rangle$ sont les $Q \pmod P$ tels que $(P,Q)=1$.

Théorème 2.9. *Soit K un corps et $P \in K[X]$ un polynôme unitaire de degré ≥ 1. Alors $K[X]/\langle P\rangle$ est un corps si et seulement si P est irréductible dans $K[X]$*

Corollaire 2.10. *Soit K un corps fini ayant q éléments et $P \in K[X]$ un polynôme unitaire irréductible de degré $m \geq 1$. Alors $K[X]/\langle P\rangle$ est un corps fini ayant q^m éléments.*

Exemple 2.11. On pourra vérifier que

$$\mathbf{F}_2[X]/\langle X^3+X+1\rangle = \{0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1\}$$

est un corps ayant 8 éléments et que

$$\mathbf{F}_3[X]/\langle X^2+1\rangle = \{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\}$$

est un corps ayant 9 éléments.

2.3 Racines des polynômes

Définition 2.12. *Soit K un corps commutatif et $P \in K[X]$. On dit que $a \in K$ est une racine de P si et seulement si $P(a)=0$.*

Théorème 2.13. *Soit K un corps commutatif et $P \in K[X]$. Alors $(X-a)|P \Leftrightarrow P(a)=0$*

Preuve. On a pour tout k entier, $X-a|X^k-a^k$ donc $(X-a)|\sum_k p_k(X^k-a^k) = P-P(a)$. CQFD

Corollaire 2.14. *Un polynôme P de $K[X]$ a au plus n racines dans K.*

Preuve. Il suffit de remarquer que $X-a$ et $X-b$ sont premiers entre-eux, puisque $(X-a)-(X-b) = b-a$ est une constante inversible. Ainsi si $a_1,\ldots,a_m$ sont des racines distinctes de P, $(X-a_1)\cdots(X-a_m)$ divise P, en utilisant le Lemme de Gauss. Par conséquent $m \leq n$. CQFD

Remarque 2.15. Ce résultat subsiste, même si les racines ne sont pas distinctes, c'est-à-dire, en comptant l'ordre de multiplicité de chaque racine. Ce résultat subsiste si on remplace K par un anneau intègre et commutatif. En revanche, ce résultat est faux si A n'est plus intègre, par exemple, X^2-1 a 4 racines dans l'anneau $\mathbf{Z}/8\mathbf{Z}$. Ce résultat est faux si K est un corps non commutatif, par exemple le corps des quaternions $\mathbb{H}_8$.

Soit P un polynôme non constant et $P = \lambda P_1^{n_1}\ldots P_r^{n_r}$ sa factorisation dans $K[X]$. On dit que P n'a que des *facteurs simples* si $n_1=\cdots=n_r=1$; sinon, il existe $n_i \geq 2$ et on dit que P_i est un *facteur multiple* de P. En particulier, on dira que a est une *racine multiple* de P si et seulement si $(X-a)^2$ divise P.

Si $P = a_0+a_1X+a_2X^2+\cdots+a_nX^n$ est un polynôme de $K[X]$, on définit son *polynôme dérivé* $P' = a_1+2a_2X+\cdots+na_nX^{n-1}$. On a pour tous polynômes P et Q ; $(PQ)' = P'Q+PQ'$.

Théorème 2.16. *Soit* $\mathbf{K}$ *un corps. $P \in \mathbf{K}[X]$ est sans facteurs carrés si et seulement si $(P,P')=1$.*

Pour qu'un polynôme non constant n'ait que des facteurs simples, il faut et il suffit $(P,P')=1$.

Lien entre racine commune et PGCD

Soit K un corps et $P \in K[X]$. Si P n'a pas de racine dans K (par exemple X^2+X+1 n'a pas de racine ni dans $\mathbf{Q}$, ni dans $\mathbf{R}$, ni dans $\mathbf{F}_p$ si $p=2 \pmod 3$), il en a toujours une dans une extension L de K. Un des problèmes récurrent est de déterminer précisément quelle est cette extension L.

Il suffit de considérer P_1 un facteur irréductible de P dans $K[X]$. L'algèbre quotient $L = K[X]/(P_1)$ est un corps et α, la classe de X dans L, vérifie $P_1(\alpha)=0$. Par conséquent α est une racine de P_1 donc une racine de P, puisque $P = P_1Q_1$. On déduit donc que **tout polynôme P de $K[X]$ admet une racine dans un corps contenant K**. On peut à présent énoncer

Théorème 2.17. *Soit P et Q deux polynômes de $K[X]$. Alors $(P,Q)=1$ si et seulement si P et Q n'ont pas de racine commune.*

Preuve. Si $(P,Q)=1$, alors il existe U et V tels que $UP+VQ=1$. Si α était une racine commune de P et de Q, alors on aurait $1=0$, ce qui est impossible. Réciproquement, toute racine du pgcd de P et Q est une racine commune, peu importe l'extension dans laquelle elle se situe. CQFD

2.4 Théorème chinois pour les algèbres quotients $\mathcal{P}=K[X]/\langle P\rangle$

Théorème 2.18. *Soit K un corps et $P_1, P_2 \in K[X]$ deux polynômes premiers entre eux. Alors l'application*

$$\begin{array}{rcl} K[X]/\langle P_1P_2\rangle & \stackrel{\varphi}{\to} & K[X]/\langle P_1\rangle \times K[X]/\langle P_2\rangle \\ (Q \pmod{P_1P_2} & \mapsto & [Q \pmod{P_1}, Q \pmod{P_2}] \end{array}$$

est un isomorphisme de K-algèbres (morphisme d'anneaux et application linéaire bijective).

Un cas particulier très intéressant, lorsque $P_i = X-a_i, i=0,\ldots,n$.

$$K_n[X] \simeq K[X] \,/\, \langle \prod_{i=1}^{n}(X-a_i)\rangle \simeq \prod_{i=1}^{n} K[X]/(X-a_i).$$

On obtient l'isomorphisme $\begin{array}{rcl} K_n[X] & \to & K^{n+1} \\ P & \mapsto & (P(a_0),\ldots,P(a_n)) \end{array}$ et sa réciproque $\begin{array}{rcl} K^{n+1} & \to & K_n[X] \\ (y_0,\ldots,y_n) & \mapsto & \sum_{i=0}^{n} y_iL_i \end{array}$

où les

$$L_i = \frac{\prod_{j\neq i}(X-a_j)}{\prod_{j\neq i}(a_i-a_j)}$$

vérifient $L_i(a_j)=\delta_{i,j}$. Les L_i s'appellent les *polynômes d'interpolation de Lagrange*.

Un cas particulier sera étudié lorsque $P=X^n-1=\prod_{k=0}^{n-1}(X-w^i)$, donnant lieu à la transformation de Fourier.

Complexité des opérations arithmétiques

3 Complexité des opérations arithmétiques

Nous avons vu que le nombre d'étapes dans l'algorithme d'Euclide est explicitement borné par la taille des objets considérés. Cette quantité donne une indication de la complexité de l'algorithme mais il convient aussi d'examiner la nature des opérations (ici arithmétiques) effectuées et aussi les objets manipulés.

Les résultats présentés ci sont classiques. Une bonne référence est l'ouvrage AECF ([1]) qui dépassent souvent le cadre de ce cours, mais contiennent des détails et des références incontournables pour les lecteurs intéressés par ces questions.

Nous commençons par étudier les opérations arithmétiques sur les polynômes, pour en déduire des estimations avec les entiers.

Définition 3.1. *Si f et g sont deux fonctions de* $\mathbf{N}$ *dans* $\mathbf{R}$*, telles que $g(n) > 0$ pour n assez grand, on dira que $f = O(g)$ si il existe deux constantes $c \in \mathbf{R}$ et $n \in \mathbf{N}$, telles que $f(n) \leq cg(n)$ pour $n \geq N$.*

On dira que $f = O^{\sim}(g)$ si $|f(n)| \leq cg(n)\log^k(g(n)+1)$ pour des constantes c et k positives et n suffisamment grand.

Si $f = O^{\sim}(n)$, on dit que f est *quasi-linéaire*. Si $f(n) = O^{\sim}(n^2)$, on dit que f est *quasi-quadratique*.

3.1 Opérations arithmétiques sur les polynômes

Nous supposons donné ici un anneau A *effectif*, c'est-à-dire, les opérations arithmétiques sont réalisables effectivement. Les opérations arithmétiques de base de l'anneau des polynômes $A[X]$ sont l'addition, la multiplication par un scalaire, la multiplication, la division euclidienne. Il est bon également de considérer le coût de la composition, dont un cas particulier est l'évaluation en une valeur a de l'anneau A.

Si $A = \sum_{i=0}^{n} a_i X^i$ et $B = \sum_{i=0}^{n} b_i X^i$, la somme $A+B$ est donné par $\sum_{i=1}^{n}(a_i+b_i)X^i$. L'addition de deux polynômes de degrés bornés par n requiert $n+1$ additions dans l'anneau de base. On dira que la *complexité arithmétique* de l'addition des polynômes est $O(n)$, ou *linéaire en le degré*. Voici un algorithme qui réalise l'addition :

Algorithme 3.2. — *Addition*

Entrées : $f = \sum_{i=0}^{n} f_i x^i$, $g = \sum_{i=0}^{n} g_i x^i$.
Sorties : $h := f+g$. *# signifie que h prend la valeur de $f+g$.*

1. Pour i de 0 à n calculer $h_i = f_i + g_i$
2. Retourner $h = \sum_{i=0}^{n} h_i x^i$.

De la même façon, la multiplication de A par un élément λ requiert $n+1$ multiplications.

Multiplication

Quant-à la multiplication de A par B nous pouvons écrire $A \cdot B = \sum_{k=0}^{n+m} (\sum_{i+j=i} a_i b_j) X^k$. Nous pouvons calculer les coefficients de $A \cdot B$ en $(n+1)(m+1)$ multiplications et et nm additions. Nous voyons que la multiplication de deux polynômes de degré inférieur à n s'effectue en $O(n^2)$ opérations arithmétiques. La multiplication des polynômes a donc une complexité arithmétique quadratique. Voici un algorithme qui réalise la multiplication :

Algorithme 3.3. — *Multiplication des polynômes*

Entrées : $f = \sum_{i=0}^{n} f_i x^i$, $g = \sum_{i=0}^{m} g_i x^i$.
Sorties : $h := f \cdot g$.

1. Si $f = 0$ ou $g = 0$ alors retourner $h := 0$. *# ici le programme s'arrête*
2. Pour i de 0 à $m+n$ initialiser $h_i := 0$.
3. Pour i de 0 à n, pour j de 0 à m, calculer $h_{i+j} := h_{i+j} + f_i g_j$
4. Retourner $h = \sum_{i=0}^{m+n} h_i x^i$.

Algorithme de Karatsuba

Il existe une méthode plus rapide, due à Karatsuba, basée sur le fait que

$$(aX+b)\cdot(cX+d) = (ac)X^2 + ((a+b)(c+d) - ac - bd)X + bd.$$

La multiplication de ces deux polynômes requiert 3 multiplications et 4 additions au lieu de 4 multiplications et une addition, mais au final cela permet de gagner et on peut montrer que cette méthode permet de calculer deux polynômes de degrés n en $O(n^{\log_2 3})$ opérations arithmétiques.

Soit donc A et B de degré $N \leq 2^n$. Écrivons $A = A_0 + X^{2^{n-1}} A_1$ et $B = B_0 + X^{2^{n-1}} B_1$. Il vient alors

$$A \cdot B = A_1 B_1 X^{2^n} + ((A_0 + A_1)(B_0 + B_1) - A_0 B_0 - A_1 B_1) X^{2^{n-1}} + A_0 B_0.$$

On peut donc calculer $A \cdot B$ en 3 multiplications et 4 additions de polynômes de degré 2^{n-1}. Si on désigne par $M(n)$ le coût de la multiplication de deux polynômes de degré inférieur à 2^n et $S(n) = O(2^n)$ le coût de l'addition, on a $M(n) \leq 3M(n-1) + 4S(n-1) \leq 3M(n-1) + \lambda 2^n$. Il vient ensuite, en posant $u_n = \dfrac{M(n)}{3^n}$,

$$u_n - n_{n-1} \leq \lambda (2/3)^n.$$

Soit, en sommant : $u_n - u_0 \leq 3\lambda$ soit $M(n) \leq C 3^n$

Si maintenant A et B sont de degré N, on peut calculer $A \cdot B$ en $O(3^n)$ opérations dans K. Ici $n = [\log_2 N] + 1 \leq \log_2 N + 1$ et $3^n \leq 3^{\log 2N + 1} = 3n^{\log_2 3}$. Ainsi $M(n) = O(n^{\log_2 3}$. La complexité de la multiplication devient n^α où $\alpha = \log_2 3 \sim 1.585$.

Nous verrons plus tard qu'il existe une méthode encore plus rapide, basée sur l'interpolation en des racines n-ème de l'unité : la transformée de Fourier rapide (Fast Fourier Transform). Elle permet de multiplier deux polynômes de degrés n en $O(n \log n \log\log n) = O^\curlyvee(n)$ opérations arithmétiques.

Division euclidienne

La division euclidienne de deux polynômes est basée sur le fait que si $A = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ et $B = b_m X^m + b_{m-1} X^{n-1} + \cdots + b_0$ avec $n \geq m$, alors le polynôme $A - a_n (b_m)^{-1} X^{n-m} B$ est congru à A modulo B mais son degré est strictement inférieur à celui de A.

En réitérant le procédé, on obtient la division euclidienne. Remarquons, qu'à chaque étape, il faut que b_m soit inversible, ou, à tout le moins que b_m divise a_n. Dans le cas où l'anneau de base est un corps, cela ne pose pas de problème et on considérera $\hat{B} = (b_m)^{-1} B$, polynôme unitaire puis on effectuera la division euclidienne $A = \hat{B} \cdot Q + R = B \cdot (b_m^{-1} Q) + R$.

Algorithme 3.4. — *Division euclidienne*

Entrées : $f=\sum_{i=0}^{n} f_i x^i$, $g=\sum_{i=0}^{m} g_i x^i \neq 0$.
Sorties : (q,r) tels que $f=g\cdot q+r$ et $\deg r<\deg b$.

1. Initialiser $r:=f$, $u:=(g_m)^{-1}$.
2. Pour $i=n-m,n-m-1,\cdots,0$ faire
   (a) Si $\deg r=m+i$ alors $q_i:=r_{m+i}\cdot u$, $r=r-q_iX^i\cdot g$,
   (b) Sinon $q_i=0$.
3. Retourner $q:=\sum_{i=0}^{n-m} q_iX^i$.

Preuve. On montre qu'à chaque étape i dans cet algorithme, on a $f=(\sum_{j=i}^{n-m} q_jX^j)\cdot g+r$. Le reste r voit son degré décroître et être inférieur à i. Écrivons sur des lignes les coefficients de A et B, on a

$$\begin{array}{rcl} f & = & a_nX^n \ +a_{n-1}X^{n-1}+\cdots \qquad\qquad\qquad \cdots \ +a_0 \\ g & = & \qquad\qquad\qquad\qquad b_mX^m+b_{m-1}X^{m-1} \ +\cdots \ +b_0 \end{array}$$

$$\begin{array}{rccccccc} & a_nX^n & +a_{n-1}X^{n-1} & +\cdots & & & \cdots & +a_0 \\ (\times X^{n-m}) & b_mX^n & +b_{m-1}X^{n-1} & +\cdots & +b_0X^{n-m} & & & \\ (\times X^{n-m-1}) & & b_mX^{n-1} & & +\cdots & +b_0X^{n-m-1} & & \\ \vdots & & & \ddots & \ddots & & \ddots & \\ (\times 1) & & & & b_mX^m & +\cdots & & +b_0 \end{array}$$

On retranche à chaque étape $q_iX^{n-m-i}g$, c'est-à-dire, on effectue des opérations élémentaires sur les lignes f et $X^ig, i=0,\ldots,n-m$. CQFD

On déduit

Théorème 3.5. *Soit f et g des polynômes de $A[X]$, de degrés inférieurs à n et $m\leq n$. On peut effectuer la division euclidienne de f par g en $O(m(n-m+1))=O(n^2)$ opérations arithmétiques dans A.*

Algorithme d'Euclide

Dans l'algorithme d'Euclide étendu, on définit par récurrence

$$R_0=A, R_1=B, R_{i+1}=R_{i-1}\,(\mathrm{mod}\,R_i), Q_i=R_{i-1}\div R_i.$$

La suite des restes est de degré strictement décroissante. On a aussi $T_{i+1}=T_{i-1}-Q_iT_i$, $S_{i+1}=S_{i-1}-Q_iS_i$.

On montre que (voir [4, 7, 3])

Théorème 3.6 (Admis)**.** *Soit f et g des polynômes de $K[X]$, de degrés inférieurs à n et $m\leq n$. On peut effectuer le calcul de* $\mathrm{pgcd}(f,g)$ *en $O(n^2)$ opérations arithmétiques (additions, multiplications) dans K et $m+1$ inversions.*

Idée de la preuve. Posons $R_0=f$ et $R_1=g$ et effectuons l'algorithme d'Euclide, comme précédemment. Posons $n_i=\deg R_i$, on calcule R_{i+1} en $O((n_i+1)(n_{i-1}-n_i+1))$ opérations arithmétiques dans K.

Mais $(n_i+1)(n_{i-1}-n_i+1)=n_i(n_{i-1}-(n_i-1))+(n_{i-1}-n_i)$.

Mais la série $n_0n_1-n_1(n_1-1)+n_1n_2-n_2(n_2-1)+\cdots$ est une série alternée car $n_i\leq n_{i-1}-1$ donc est majorée par son premier terme n_0n_1. La seconde série $\sum_i(n_{i-1}-n_i)$ est majorée par n_0. Au final $\sum_i(n_i+1)(n_{i-1}-n_i+1))\leq n_0(n_1+1)\leq n_0^2$. On calcule donc la suite des restes en $O(n^2)$ opérations arithmétiques CQFD

Le nombre d'étapes dans l'algorithme d'Euclide est majoré par le degré des polynômes, le nombre d'opérations arithmétiques dans le corps K est quadratique en le degré, mais ne reflète pas nécessairement la difficulté du calcul.

Comme illustration de ce phénomène, considérons l'exemple suivant dans $\mathbf{Q}[X]$, qui est un anneau euclidien : $A=-50X^4+23X^3+75X^2-92X+6, B=74X^3+72X^2+37X-23$. Posant $R_0=A, R_1=B$, on obtient successivement

$$\begin{aligned} R_2 &= \tfrac{41464}{1369}X^2-\tfrac{10609}{74}X+\tfrac{77401}{2738}, \\ R_3 &= \tfrac{6762644142925}{3438526592}X-\tfrac{1434310205345}{3438526592}, \\ R_4 &= -\tfrac{10356972970171258216 96}{13362558306453705720 25} \end{aligned}$$

Les coefficients de Bézout sont

$$\begin{aligned} U &= -\tfrac{7310966641}{150601903069}X^2-\tfrac{43319892877}{753009515345}X-\tfrac{56801433271}{1506019030690}, \\ V &= -\tfrac{4939842325}{150601903069}X^3+\tfrac{2449241929}{301203806138}X^2+\tfrac{37715425374}{753009515345}X-\tfrac{40148426746}{753009515345} \end{aligned}$$

On observe une grande croissance des coefficients de Bézout. Nous montrerons, par la suite, que si A et B sont premiers entre-eux, alors l'équation $UA+VB=1$ a une solution unique dans $K_{<m}[X]\times K_{<n}[X]$ et que les coefficients des polynômes U et V sont solutions d'un système de Cramer à coefficients entiers, dont nous pouvons borner les solutions.

Le pgcd étant normalisé, il est plus judicieux (voir [7]) d'effectuer une normalisation à chaque étape, c'est-à-dire, de rendre les polynômes unitaires. On constate une légère décroissance des coefficients et on obtient

$$R_0=X^4-\tfrac{23}{50}X^3-\tfrac{3}{2}X^2+\tfrac{46}{25}X-\tfrac{3}{25}, R_1=X^3+\tfrac{36}{37}X^2+\tfrac{1}{2}X-\tfrac{23}{74}, R_2=X^2-\tfrac{392533}{82928}X+\tfrac{77401}{82928}, R_3=X-\tfrac{209541301}{987968465}, R_4=1.$$

On modifie légèrement l'algorithme, de telle sorte qu'on a $\rho_0 R_0=A$, $\rho_1 R_1=B$, où R_i est unitaire. Puis nous calculons $Q_i=R_{i-1}\div R_i$ et $\rho_{i+1}R_{i+1}=R_{i-1}-Q_iR_i$. Notons que Q_i est unitaire comme quotient de deux polynômes unitaires.

Evaluation

Nous présentons ici le schéma d'évaluation de Horner.

Théorème 3.7 (Schéma de Horner)**.** *Soit $P\in K[X]$ de degré n et soit $a\in K$. On peut calculer $P(a)=\sum_{i=0}^n p_i a^i$ en n multiplications et $n-1$ additions dans K.*

Preuve. L'idée n'est pas de calculer successivement a^i pour i variant de 1 à n en $O(n^2)$ multiplications, puis de calculer $\sum_i p_i a^i$. L'idée est plutôt de considérer que $P(a)=(((p_n a+p_{n-1})a+p_{n-2})a+\cdots)a+p_0)$. On calcule donc successivement : $r_0=p_n$ et $r_{i+1}=r_i a+p_{n-i}$, pour i de 1 à n. La suite $v_i=r_i a^{n-i}$ vérifie $v_{i+1}-v_i=p_{n-i}a^{n-i}$ d'où l'on déduit que $r_n=P(a)$. CQFD

On peut démontrer que cette méthode est optimale en général, en particulier lorsque les a_i sont linéairement indépendants, mais ce résultat sort du cadre de ce cours. Il existe des cas particuliers où on peut calculer plus rapidement.

Exponentiation dichotomique

Dans le cas où $P(x)=x^n$, on peut utiliser une méthode plus rapide.

Exemple 3.8. Calculons par exemple a^{37}, en remarquant que $37=32+4+1$. On a alors $a^{37}=a\cdot a^4\cdot a^{32}$. Nous obtenons ce résultat en calculant successivement $a^2, a^4, a^8, a^{16}, a^{32}$ puis encore deux multiplications : $a^5:=a\cdot a^4, a^{37}:=a^5\cdot a^{32}$, soit au total 7 multiplications, au lieu de 36 par la méthode de Horner.

Écrivons, pour n général, $n=\sum_{i=0}^k \alpha_i 2^i$. On a alors

$$a^n=\prod_{\alpha_i=1} a^{2^i}.$$

Théorème 3.9 (Exponentiation rapide)**.** *On peut calculer a^n en $2\lfloor \log_2 n \rfloor + 1$ multiplications dans A.*

On peut alors imaginer plusieurs algorithmes (voir exercices en TD), par exemple

Algorithme 3.10. — *Exponentiation rapide*

Entrées : $n \geq 0$ et $a \in A$.
Sorties : $r = a^n$.

1. Initialiser $b := 1$, $q := n$, $r := 0$, $\mathbf{a} := a$.
2. Tant que $q > 0$ faire
   (a) $r := q \pmod 2$, $q := q \div 2$
   (b) Si $r = 1$ alors $b := b \cdot \mathbf{a}$
   (c) Si $q > 0$ alors $\mathbf{a} := \mathbf{a}^2$
3. Retourner b.

A chaque étape de l'algorithme on a $r \cdot \mathbf{a}^q = a^n$. A chaque étape, q est divisé par 2 au moins donc l'algorithme s'arrête lorsque $q = 0$ et on a bien $r = a^n$. Cet algorithme est basé aussi sur la possibilité d'écrire n en base 2, plus précisément la possibilité d'effectuer la division euclidienne $n = 2q + r$. Nous étudions cette question ultérieurement.

Remarque 3.11. Il y a des variantes à cet algorithme (voir [2]), qui de toute façon s'effectue en $O(\log n)$ multiplications arithmétiques dans l'anneau A.

Cet algorithme trouve de nombreuses applications, par exemple dans les protocoles cryptographiques.

3.2 Opérations arithmétiques sur les entiers

Ici il faut distinguer le cas où l'anneau dans lequel nous calculons est fini et où donc tous les calculs arithmétiques de base (addition, soustraction, multiplication, division, calcul de l'inverse) ont un coût fixe, lui même fonction de la *taille de l'anneau*. On parle ici de modèle de calcul à coût fixe.

C'est le cas par exemple, si on se fixe en entier B et que nous calculons modulo B. C'est le cas si nous calculons dans un corps fini de cardinal q.

Soit $B > 1$ un entier. Tout entier relatif n s'écrit de façon unique $\varepsilon(n) \sum_{k=0}^{d} b_i B^i$ avec $0 \leq b_i < B$. Il s'agit de l'écriture en base B de l'entier n. On note alors $n = (b_d b_{d-1} \cdots b_0)_B$ pour indiquer qu'il s'agit de l'écriture de n en base B. Dans ce cas, nous dirons que $d+1$ est la *taille* de l'entier en base B. On a $d = \lfloor \log_B n \rfloor = O(\log n)$.

Dans ce cours, nous ne cherchons pas à expliciter trop précisément le nombre d'opérations mais plutôt à donner un ordre de grandeur. Bien sûr, on peut affiner l'étude et considérer que la multiplication est toujours plus coûteuse que l'addition, mais nous contentons ici de supposer que toutes les opérations arithmétiques dans $[0, B-1]$ ont un coût majoré par une constante $O(1)$.

Un modèle réaliste, qui est d'ailleurs utilisé par les processeurs informatiques actuels consiste à prendre $B = 2^k$, en particulier $B = 2^{64}$ pour les processeurs 64 bits.

Chaque entier est représenté alors par un tableau $(a_d a_{d-1} \ldots a_0)$, avec $n = \varepsilon \sum_{k=0}^{d} a_i 2^{64 \cdot i}$.

Nous étudions à présent, pour chaque algorithme, la *complexité en temps* (running time en anglais) ou la *complexité binaire* (bit-complexity ou binary complexity) qui estime le temps nécessaire à la réalisation de l'algorithme. Cette complexité est plus fine que la complexité arithmétique car chaque opération arithmétique n'a pas le même coût, suivant la nature des objets manipulés.

Addition

Considérons $n = \sum_{i=0}^{d} n_i B^i$ et $m = \sum_{i=0}^{d} m_i B^i$. On a alors clairement $n+m = \sum_{i=0}^{d} (n_i + m_i) B^i$. Contrairement au cas des polynômes, il faut ensuite veiller à ce que $0 \leq n_i + m_i < B$, sans quoi il faut ajouter une retenue.

Théorème 3.12. *Soit a et b des entiers de taille bornée par n. Alors on peut effectuer l'addition de a et de b en temps $O(n)$.*

On peut réaliser l'addition par cet algorithme :

Algorithme 3.13. — *Addition des entiers*

Entrées : $a = (a_d \dots a_0)_B$ et $b = (b_d \dots b_0)_B$.
Sorties : $n+m = (x_{d'} \dots x_0)$.

1. r :=0
2. Pour i variant de 0 à $d-1$ faire
   (a) $\texttt{tmp} := n_i + m_i + r$, $r := \texttt{tmp} \div B$, $c_i = \texttt{tmp} \pmod B$
3. $c_{d+1} := r$.

Durant l'algorithme, tmp appartient à $[0, 2B-2]$ donc le calcul de $\texttt{tmp} \div B$ et $\texttt{tmp} \pmod B$ a un coût fixe. Cet algorithme a une complexité binaire $O(n)$, où les tailles de a et de b sont majorées par d.

Lorsque a ou b est négatif, il convient de considérer la soustraction plutôt que l'addition et une étude similaire montre qu'elle a une complexité linéaire en la taille des entiers.

Multiplication des entiers

On peut utiliser l'algorithme de multiplication usuel avec propagation de retenue de la façon suivante.

Algorithme 3.14. — *Multiplication des entiers*

Entrées : $a = (a_k \dots a_0)_B$ et $b = (b_\ell \dots b_0)_B$.
Sorties : $a \cdot b = (c_d \dots c_0)_B$.

1. Pour i de 0 à $k+\ell$ faire $c_i = 0$.
2. Pour i de 0 à k faire
   (a) $r := 0$
   (b) Pour j de 0 à ℓ faire
      i. $\texttt{tmp} := a_i \cdot b_j + c_{i+j} + r$,
      ii. $c_{i+j} := \texttt{tmp} \pmod B$,
      iii. $r := \texttt{tmp} \div B$
   (c) $c_{i+\ell+1} := r$

Division euclidienne

On ne peut utiliser la division euclidienne des polynômes et propager des retenues comme pour l'addition ou la multiplication. Commençons par effectuer la division de $a = (a_k \cdots a_0)_B$ par $b = (b_0)_B$.

Nous devons obtenir $a = b_0 q + h$ et $q = (q_k \cdots q_0)_B$. Définissons $h_{k+1} = 0$ et par récurrence la suite (h_i, q_i) est définie par $h_{i+1}B + a_i = q_i b_0 + h_i$, c'est-à-dire, q_i et h_i sont le quotient et le reste de la division euclidienne de $h_{i+1}B + a_i$ par b_0. On obtient alors, en sommant les égalités

$$0 = \sum_{i=0}^{k} (h_{i+1}B + a_i)B^i - (q_i b_0 + h_i)B^i = h_{k+1}B^{k+1} + a - q \cdot b_0 - h_0$$

c'est-à-dire, $a = bq + r$. On obtient donc la division de $(a)_B$ par b_0 en $O(k)$ opérations binaires, car la quantité $h_{i+1}B + a_i$ est bornée. On montre ensuite, mais cela sort du cadre du cours, que la division euclidienne de deux entiers $a = (a_k \cdots a_0)_B$ et $b = (b_\ell \cdots b_0)$ peut s'effectuer en $O(\ell(k-\ell+1))$ opérations arithmétiques dans $[0, \ldots, B^2 - 1]$, c'est-à-dire, B étant fixé en $O(\ell(k-\ell+1))$ opérations binaires. Voir [4], [6, Ex. I.37-39].

Algorithme d'Euclide pour les entiers

Nous avons vu que l'algorithme d'Euclide entre deux entiers de taille inférieure à n peut se réaliser en $O(n)$ opérations arithmétiques.

Proposition 3.15 (Coût de l'algorithme d'Euclide)**.** *Soit a et b deux entiers naturels de taille inférieur à n. On peut calculer le pgcd de a et de b et les coefficients de Bézout de a et de b en $O(n^2)$ opérations binaires.*

Preuve. Dans l'algorithme d'Euclide on calcule (q_i, r_{i+1}) comme le quotient de r_{i-1} par r_i. Cela peut se faire en $O(\log r_i(\log(r_{i-1}) - \log r_i))$ opérations binaires. Considérons la somme alternée

$$\log r_0 \log r_1 - (\log r_1)^2 + \log r_1 \log r_2 - (\log r_2)^2 + \cdots,$$

Elle est majorée par son premier terme $\log r_0 \log r_1 \leq n^2$. On déduit le résultat pour le calcul du pgcd. Les coefficients de Bézout sont définis par $x_{i+1} = x_{i-1} - q_i x_i$. Prenons le cas des u_i. La suite $|u_i|$ est croissante pour $i \geq 1$ et bornée par $|b/d| \leq b$. On obtient donc $q_i x_i$ en $O(\log b \log q_i)$ opérations binaires, puis x_{i+1} comme la somme de deux éléments de taille bornée par $\log q_i + \log b$, en $O(\log q_i + \log b)$ opérations binaires. En sommant ces quantités on obtient une majoration en $O(\log b)\sum_i \log q_i = O(\log b \log \prod q_i) = O(n \log b)$, puisque $\prod q_i \leq a$. CQFD

3.3 Complexité du calcul modulo N

Ici N est un entier, on peut donc effectuer l'addition et la soustraction modulo N en $O(\log N)$ opérations binaires. Il convient essentiellement de s'assurer que $a + b < N$ et sinon on a $a + b \equiv a + b - N \pmod N$.

On peut effectuer le produit de deux éléments de $\mathbf{Z}/N\mathbf{Z}$ en $O((\log N)^2)$ opérations. En effet, il suffit de calculer le produit $a \cdot b \in [0, (N-1)^2]$ puis d'effectuer la division euclidienne $a \cdot b \bmod N$ en $O((\log N)^2)$ opérations binaires.

On peut tester si a est inversible modulo N en $O((\log N)^2)$ opérations et calculer son inverse, par l'algorithme d'Euclide également en $O((\log N)^2)$ opérations binaires.

Résumé à retenir

Si A et B sont des polynômes de degré n et $m \leq n$, on peut

1. Calculer $A \pm B$ en $O(n)$ opérations arithmétiques dans K.
2. Calculer $A \cdot B$ en $O(nm)$ opérations arithmétiques dans K.
3. Calculer (Q, R) tels que $A = BQ + R$ est la division euclidienne de A par B en $O(n(n-m+1))$ opérations arithmétiques dans K.

Si $a \in K$, on peut calculer $P(a)$ en $O(n)$ opérations arithmétiques dans K. On peut calculer a^n en $O(\log n)$ opérations arithmétiques.

Si a et b sont des entiers de tailles n et $m \leq n$, on peut

1. Calculer $a \pm b$ en $O(n)$ opérations binaires.
2. Calculer $a \cdot b$ en $O(nm)$ opérations binaires.

3. Calculer (q,r) tels que $a = bq + r$ est la division euclidienne de a par b en $O(n^2)$ opérations binaires.
4. Calculer $\text{pgcd}(a,b)$ en $O(n^2)$ opérations binaires.
5. Calculer une relation de Bézout entre a et b en $O(n^2)$ opérations binaires.

Si a et b sont définis modulo n. On peut calculer

1. $a \cdot b \,(\text{mod}\, n))$ en $O((\log n)^2)$ opérations binaires.
2. $a \pm b \,(\text{mod}\, n))$ en $O((\log n)^2)$ opérations binaires.
3. Tester si $(a,n) = 1$ et calculer $a^{-1} \,(\text{mod}\, n)$ en $O((\log n)^2)$ opérations binaires.

Compléments sur les corps finis

4 Extensions de corps finis

Dans cette partie nous examinons les extensions de corps $\mathbf{F}_p$: d'une part les corps finis $\mathbf{F}_q$, et d'autre part les algèbres $\mathbf{F}_p[X]/(P)$ où P n'est pas nécessairement un polynôme irréductible.

Cette partie reprend le cours de seconde année [5, 8], complété par des résultats que le lecteur intéressé pourra trouver développés dans [2].

4.1 Rappels sur les corps finis

Si n est un entier, l'anneau $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est premier. On note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$.

Si K est un corps fini, le théorème de Wedderburn enseigne que K est commutatif. En conséquence, dans K, l'équation $x^k = 1$ a au plus k solutions, d'après le corollaire 2.14 : ce sont les racines k-èmes de l'unité dans K, et nous déduisons.

Lemme 4.1. *Soit K un corps fini, alors K^* est cyclique.*

Preuve. Notons $K_d : \{x \in K^*, x^d = 1\}$ et $H_d = \{x \in K^*, \mathrm{ord}\,(x) = d\}$. On a $N = |K^*| = \sum_{d|N} H_d$, puisque les H_d sont disjoints et que d'après le théorème de Lagrange, l'ordre de $x \in K^*$ divise N. Soit d divisant N, supposons que H_d contienne au moins un élément x_d. Alors le groupe $\langle x_d$ enegendré par x_d est de cardinal d et est contenu dans K_d. Donc K_d est le groupe cyclique $\langle x_d \rangle$. Dans K_d cyclique, il y a exactement $\varphi(d)$ éléments d'ordre d. On déduit qu'il y a soit 0, soit $\varphi(d)$ éléments d'ordre d pour d divisant N. Par ailleurs, d'après la formule d'Euler, nous avons $N = \sum_{d|N} \varphi(d)$ soit en soustrayant $0 = \sum_{d|N} (\varphi(d) - |H_d|)$ d'où l'on déduit que K^* a exactement $\varphi(d)$ éléments d'ordre d pour tout diviseur d de N. En particulier K^* est cyclique. CQFD

Définition 4.2. *Un générateur de K^* est* un élément primitif *de K^*.*

Caractéristique

Soit K un corps fini. Le noyau du morphisme de groupe additif $\mathbf{Z} \to K, n \mapsto n \cdot 1_K$ est un sous-groupe de $\mathbf{Z}$, donc de la forme $p\mathbf{Z}$ où p est l'ordre de 1 dans le groupe fini $(K, +)$. Si $p = p_1 p_2$, alors $(p_1 1\!\!1) \cdot (p_2 1\!\!1) = 0$ et, par suite puisque K est intègre, p divise p_1 ou p divise p_2. p n'a pas de diviseur propre et p est donc premier.

Le groupe additif engendré par 1_K, $\langle 1_K \rangle = \{0, 1, \ldots, (p-1) \cdot 1\}$ est un corps, c'est le *sous-corps premier* de K. Il est isomorphe à $\mathbf{Z}/p\mathbf{Z}$ et l'unique isomorphisme est $1 \mapsto 1_K$, nous le noterons $\mathbf{F}_p$. K est alors un $\mathbf{F}_p$-espace vectoriel, de dimension finie n et $|K| = p^n$. [1].

Morphisme de Froebenius

Proposition 4.3. *Soit K un corps fini de cardinal p^n. Notons $\sigma : K \to K$, $x \mapsto x^p$,* le morphisme de Froebenius *et $\mathbf{F}_p$ le sous-corps premier de K. Alors*

1. C'est un résultat classique : si $k \subset K$ sont deux corps, alors K est un k-espace vectoriel

1. σ *est un endomorphisme du* $\mathbf{F}_p$*-espace-vectoriel* K.
2. σ *est un automorphisme et* $\sigma^n = \mathbb{1}$.
3. *Pour tout* $x \in K$*, on a* $x \in \mathbf{F}_p \iff \sigma(x) = x$.

Preuve. Dans le corps $\mathbf{Z}/p\mathbf{Z}$, on a d'après le théorème de Fermat, $x^p = x$, pour tout $x \in \mathbf{F}_p$. On déduit l'identité dans $\mathbf{F}_p[X]$: $X^p - X = \prod_{\alpha \in \mathbf{F}_p}(X - \alpha)$. Effectuons le changement de variable $X \mapsto X+1$, on en déduit, puisque $\alpha \mapsto \alpha - 1$ est une bijection de $\mathbf{F}_p$, que

$$(X+1)^p - (X+1) \equiv X^p - X \,(\mathrm{mod}\, p)$$

c'est-à-dire, $\binom{p}{i} \equiv 0 \,(\mathrm{mod}\, p)$, $1 \leq i \leq p-1$.

1. On déduit, en utilisant la formule du binôme de Newton, que $\sigma(x+y) = \sigma(x) + \sigma(y)$. Par ailleurs il est clair que $\sigma(xy) = \sigma(x)\sigma(y)$.
2. $|K^*| = p^n - 1$, donc, pour tout $x \in K^*$, on a $x^{p^n-1} = 1$ d'après le théorème de Lagrange, et $x^{p^n} = x$. On en déduit que $\sigma^n = \mathbb{1}$. σ est donc inversible d'inverse σ^{n-1}.
3. L'équation $\sigma(x) = x$ admet $\mathbf{F}_p$ comme ensemble de racines et possède au plus p racines. CQFD

L'automorphisme σ laisse stable le sous-corps premier de K. De façon générale, si τ est un automorphisme du corps K, alors l'ensemble des points fixes de τ est un sous-corps de K.

On déduit une caractérisation des sous-corps d'un corps fini K de cardinal p^n.

Corollaire 4.4. *Les sous-corps de* K *sont exactement les* $\ker \sigma^d - \mathbb{1}$*, pour* d *divisant* n.

Preuve. Si $\mathbf{F}_p \subset k \subset K$, alors k est également de caractéristique p (c'est l'ordre de 1, commun à k et K). k est de cardinal p^d et k^* est cyclique. Soit x un élément primitif de k. Comme $x \in K$, on a $\mathrm{ord}\,(x) | p^n - 1$, donc $p^d - 1$ divise $p^n - 1$. Mais, si $n = qd + r$ est la division euclidienne de n par d, on a $p^n - 1 = (p^{qd} - 1) \cdot p^r + (p^r - 1)$, alors $p^d - 1$ divise $p^r - 1$ ce qui n'est possible que lorsque $r = 0$. Donc d divise n. Tous les éléments de k vérifient $\sigma^d(x) = x$. Réciproquement, si d divise n il existe $\varphi(p^d - 1)$ éléments d'ordre $p^d - 1$. Si x_d est d'ordre $p^d - 1$, l'équation $x^{p^d-1} = 1$ contient le groupe $\langle x_d \rangle$. $\sigma^d(x) = x$ contient p^d éléments qui forment un sous-corps de K. CQFD

L'automorphisme de Froebenius agit également sur $K[X]$.

Corollaire 4.5. *Soit* $\mathbf{F}_p \subset K$ *et* $P \in K[X]$*. On pose* $|K| = q = p^n$*. Alors*

1. *On a* $P(X^q) = P(X)^q$*, c'est-à-dire,* $\sigma^n(P) = P(\sigma^n X))$.
2. *En particulier* $P \in \mathbf{F}_p[X] \iff P(X^p) = P(X)^p$.

Preuve. On a $\sigma \cdot (\sum_i a_i X^i) = \sum_i a_i^p X^{p^i}$, d'où l'on déduit les résultats. CQFD

Exemple 4.6. Soit $\Phi_9 = X^6 + X^3 + 1 \in \mathbf{F}_2[X]$. Admettons que ce polynôme est irréductible pour l'instant. Alors $K = \mathbf{F}_2[X]/(\Phi_9)$ est un corps de dimension 6 sur $\mathbf{F}_2$. Notons $\alpha = \overline{X}$, α est une racine de Φ_9 dans K. K contient un sous-corps à 8 éléments : $K_8 = \{x \in K, x^8 = x\}$ et un sous-corps à 4 éléments : $K_4 = \{x \in K, x^4 = x\}$.

D'après ce qui précède $K_8 = \ker \sigma^3 - \mathbb{1}$ et $K_8 = \ker \sigma^2 - 1$.

On obtient que $K_4 = \mathrm{vect}\,(1, \alpha^3)$ tandis que $K_8 = \mathrm{vect}\,(1, \alpha + \alpha^2 + \alpha^5, \alpha^4 + \alpha^5)$.

On remarque également que $\alpha^6 = \alpha^3 + 1$ donc $\alpha^9 = \alpha^6 + \alpha^3 = 1$. α est d'ordre 9.

4.2 Polynôme minimal

Définition 4.7. *Soit* K *un corps et* k *un sous-corps de* K*. On dit que* $\alpha \in K$ *est* algébrique sur k *si* α *est racine d'un polynôme* $P \in k[X]$.

Proposition 4.8. *Soit* K *un corps fini et* $\mathbf{F}_p$ *son sous-corps premier. Tout élément de* K *est algébrique sur* $\mathbf{F}_p$.

Preuve. Soit $|K| = q = p^n$. K est de dimension n donc la famille $(1, \alpha, \ldots, \alpha^n)$ est liée. α est donc algébrique. CQFD

Soit $\alpha \in K$ algébrique sur k. On note $k(\alpha)$ le plus petit corps contenant k et α. On a donc $k \subset k(\alpha) \subset K$.

L'ensemble $I_\alpha = \{P \in k[X] \,|\, P(\alpha) = 0\}$ est un idéal de $k[X]$. I_α est principal donc admet un unique générateur unitaire, noté P_α.

Définition 4.9. *On appelle* polynôme minimal *de* α *le générateur unitaire de* I_α. *On a* $P(\alpha) = 0 \iff P_\alpha | P$. *Le degré de* P_α *est* le degré *de* α *(dans k).*

On a $P_\alpha(\alpha) = 0$ donc $P_\alpha(\alpha^p) = \big(P_\alpha(\alpha)\big)^p$, d'après le corollaire 4.5. D'une façon générale, pour tout entier i, α^{p^i} est une racine de P_α. Nous allons examiner quelles sont exactement les racines de P_α.

Proposition 4.10. *Soit K un corps fini de cardinal p^n et $\alpha \in K^*$. Notons $P_\alpha \in \mathbf{F}_p[X]$ son polynôme minimal et $d = \deg P_\alpha$.*

1. *P_α est irréductible dans $\mathbf{F}_p[X]$.*
2. *$(1, \alpha, \ldots, \alpha^{d-1})$ est une base de $\mathbf{F}_p(\alpha)$. En particulier d divise n.*
3. *$\{r \in \mathbf{Z} | \alpha^{p^r} = \alpha\} = d\mathbf{Z}$.*
4. *Le polynôme minimal de α est $P_\alpha = (X-\alpha)(X-\alpha^p)\cdots(X-\alpha^{p^{d-1}})$.*

Preuve. Si $P_\alpha = P_1 \cdot P_2$ alors $P_1(\alpha) \cdot P_2(\alpha) = 0$. Mais K est intègre d'où on déduit que $P_1(\alpha) = 0$ ou $P_2(\alpha) = 0$, soit P_α divise P_1 ou P_2. P_α est donc irréductible.

$\mathbf{F}_p(\alpha)$ est un sous-corps de K isomorphe à $\mathbf{F}_p[X]/(P_\alpha)$, par $\alpha \mapsto X \pmod{P_\alpha}$. $(1, \alpha, \ldots, \alpha^{d-1})$ est donc une base de $\mathbf{F}_p(\alpha)$.

Si $\alpha = 0$ alors $\{r \in \mathbf{Z} | \alpha^{p^r} = \alpha\} = \mathbf{Z}$. α est de degré 1, son polynôme minimal est X. Si $\alpha \neq 0$, et $\alpha^{p^r} = \alpha$ alors $\alpha^{p^r - 1} = 1$, ce qui équivaut à $\mathrm{ord}\,(\alpha) | p^r - 1$. Mais l'ordre N de α dans K^* divise $p^n - 1$ donc N est premier avec p. p est inversible dans $\mathbf{Z}/N\mathbf{Z}$ et la dernière propriété équivaut à $D|r$, où D est l'ordre de p dans $(\mathbf{Z}/N\mathbf{Z})^*$. On a donc $\{r \in \mathbf{Z} | \alpha^{p^r} = \alpha\} = D\mathbf{Z}$

De la même façon, $\alpha^{p^i} = \alpha^{p^j}$ équivaut à $\alpha^{p^{i-j}} = \alpha$. On a donc

$$\mathcal{S} = \{\alpha^{p^i}, i = 0, \ldots, D-1\} = \{\alpha^{p^i}, i \in \mathbf{Z}\}.$$

$\mathcal{S}$ contient D racines distinctes de P_α et $\mathcal{S}$ est stable par le morphisme de Froebenius $\sigma : x \mapsto x^p$. Le polynôme $Q_\alpha = \prod_{\beta \in \mathcal{S}} (X - \beta)$ vérifie $Q_\alpha(X^p) = \prod_{\beta \in \mathcal{S}} (X^p - \beta) = \prod_{\beta \in \mathcal{S}} (X^p - \beta^p) = Q_\alpha^p$ donc $Q_\alpha \in \mathbf{F}_p[X]$. α est une racine de Q_α donc $P_\alpha \mid Q_\alpha$. On a donc $P_\alpha = Q_\alpha$ et $\deg P_\alpha = D = d$. CQFD

Corollaire 4.11. *Soit P un polynôme irréductible de $\mathbf{F}_p[X]$ et $q = p^n$. Alors $P | X^q - X \Leftrightarrow \deg(P) | n$.*

Preuve. Si P est irréductible de degré d alors le corps $k = \mathbf{F}_p[X]/(P)$ a pour cardinal p^d. Dans k, $\alpha = \overline{X}$ est racine de P donc P est le polynôme minimal de α. P divise $X^{p^d} - X$ car $\alpha^{p^d} = \alpha$. Si P divise $X^q - X$ alors $\alpha^q = \alpha$ donc, utilisant la proposition précédente, on déduit que d divise n. Réciproquement, si d divise n, alors $p^d - 1$ divise $p^n - 1$ donc $X^{p^d-1} - 1$ divise $X^{p^n-1} - 1$ donc $X^{p^d} - X$ divise $X^{p^n} - X$.
CQFD
On déduit alors

Corollaire 4.12. *Le nombre $m_p(k)$ de polynômes unitaires irréductibles de degré k sur $\mathbf{F}_p$ vérifie la relation*

$$\sum_{d|n} d\, m_p(d) = p^n.$$

Pour tout entier n, il existe un polynôme unitaire irréductible de degré n sur $\mathbf{F}_p$ et donc il existe un corps $\mathbf{F}_q$ de cardinal $q = p^n$.

On a donc démontré l'existence d'un corps fini de cardinal $q = p^n$ pour tout nombre premier p et tout entier n.

4.3 Racines de l'unité

On voit que tout élément de K^* est une racine de l'unité, dont l'ordre divise p^n-1 donc est premier avec p.

Proposition 4.13. *Soit K un corps fini de cardinal $q=p^d$ et $\alpha \in K^*$ d'ordre n. Soit d l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^*$. Alors α est algébrique de degré d.*

Preuve. C'est la proposition 4.10, point 3. CQFD

Polynômes cyclotomiques

D'un autre côté, les racines n-èmes de l'unité sont les racines des polynômes cyclotomiques Φ_n. En particulier, dans $\mathbf{C}^*$, les racines n-èmes de l'unité sont les $\exp(2\mathbf{i}k\pi/n), k \in \mathbf{Z}$. Notons $\xi = \exp(2\mathbf{i}\pi/n)$. ξ est d'ordre n (on dit que ξ est une *racine primitive n-ème de l'unité*) et les n racines n-èmes de l'unité dans $\mathbf{C}^*$ sont les ξ^k, $k=0,\dots,n-1\}$.

Définition 4.14. *Soit $n>0$ un entier. On définit* $\Phi_n = \prod_{\substack{k=1,\dots,n \\ (k,n)=1}} (X-\xi^k)$.

Les racines de Φ_n sont donc exactement les $\varphi(n)$ racines de l'unité d'ordre n, dites *racines primitives n-èmes*, de $\mathbf{C}^*$. Notons qu'on a $X^n-1 = \prod_{k=1}^{n}(X-\xi^k)$. En regroupant les racines suivant leur ordre on obtient

$$X^n-1 = \prod_{d|n} \Phi_d.$$

On déduit

Proposition 4.15. *Φ_n est un polynôme unitaire, à coefficients dans $\mathbf{Z}$ et de degré $\varphi(n)$. On a $\Phi_1 = X-1$ et $X^n-1 = \prod_{d|n}\Phi_d$.*

Preuve. Lorsque $\Phi_1,\dots,\Phi_{n-1}$ sont unitaires à coefficients entiers, alors $\Psi_n = \prod_{\substack{d|n \\ d\neq n}} \Phi_d$ est unitaire à coefficients entiers. On a donc $X^n-1 = Q\cdot\Psi_n + R$ dans $\mathbf{Q}[X]$. Puisque Ψ_n est unitaire, Q et R sont dans $\mathbf{Z}[X]$, et par unicité de la division euclidienne dans $\mathbf{C}[X]$, on déduit que $R=0$ et $Q=\Phi_n$. CQFD

Remarque 4.16. Cette factorisation est également valable dans $K[X]$ pour tout corps K fini, puisque le morphisme d'anneau $\mathbf{Z}\to K$, défini par $n\mapsto n\cdot 1$ s'étend en un morphisme d'anneaux de polynômes de $\mathbf{Z}[X]\to K[X]$.

Citons le théorème bien connu, dont une preuve (du niveau L3) peut se trouver dans [2],

Théorème 4.17. *Le polynôme cyclotomique Φ_n est irréductible dans $\mathbf{Q}[X]$.*

Nous n'utiliserons pas ici cette propriété. Citons simplement ces propriétés, voir en TD,

Lemme 4.18. *Si n est un nombre premier impair, on a $\Phi_{2n}=\Phi_n(-X)$. Soit p un nombre premier. Si $p\nmid n$, alors $\Phi_{np}\cdot\Phi_n = \Phi_n(X^p)$. Si $p\mid n$, alors $\Phi_{np}=\Phi_n(X^p)$.*

On peut calculer les premiers polynômes cyclotomiques $\Phi_1=X-1$, $\Phi_2=X+1$, $\Phi_3=X^2+X+1$, $\Phi_4=X^2+1$, $\Phi_5=X^4+X^3+X^2+X+1$, $\Phi_6=X^2-X+1$.

On voit donc que si α est un élément algébrique de K, d'ordre n, alors le sous-groupe $\langle\alpha\rangle$ de K^* est cyclique et est exactement l'ensemble de toutes les solutions de $X^n-1=0$. Les $\varphi(n)$ éléments d'ordre n de $\langle\alpha\rangle$ sont exactement les racines de Φ_n. En particulier le polynôme minimal de α divise Φ_n.

On en déduit

Proposition 4.19. *Soit K un corps de caractéristique p et $\alpha \in K^*$ d'ordre n. Le polynôme minimal P_α de α a pour degré l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^*$.*

Preuve. Considérons r tel que $\alpha^{p^r} = \alpha$. Alors n divise $p^r - 1$ et $\mathrm{ord}_n(p)$ divise r. On a donc $\deg(\alpha) = \mathrm{ord}_n(p)$. CQFD

On en déduit que Φ_n se décompose dans $\mathbf{F}_p[X]$ en produit de polynômes irréductibles de même degré r.

Corollaire 4.20. *Soit p un nombre premier ne divisant pas n. Soit d l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^*$. Φ_n se décompose en produit de polynômes irréductibles unitaires distincts de degré d.*

En particulier si α est un élément primitif de K de cardinal p^d alors P_α est de degré d.

Exemple 4.21. Soit $\Phi_8 = X^4 + 1$. Dans $\mathbf{F}_2[X]$, on a $\Phi_8 = (X+1)^4$. Si p est impair alors soit $p \equiv 1 \pmod 4$ et Φ_8 est scindé dans $\mathbf{F}_p[X]$, soit $p \equiv -1 \pmod 4$ et Φ_8 se factorise en produits de facteurs de degré 2 dans $\mathbf{F}_p[X]$.

Racines d'ordre n dans $\mathbf{F}_q$

Soit α un élément d'un corps fini K de cardinal $q = p^d$. L'ordre de α dans K^* divise $q-1$ donc est premier avec p (et avec tout diviseur de q d'ailleurs). Alors α est racine de $X^n - 1$ et plus précisément α est racine de Φ_n.

Proposition 4.22. *Soit k un corps fini de caractéristique p ne divisant pas n. Alors*
- *Les racines de $\Phi_n \in k[X]$ sont toutes d'ordre n.*
- *Les éléments de k^* d'ordre n sont exactement les racines de Φ_n.*

Parmi les éléments de K de cardinal p^n, nous recherchons en particulier les éléments primitifs, c'est-à-dire, les racines primitives (p^n-1)-èmes. Nous pouvons donc construire directement explicitement le corps $K = \mathbf{F}_p[X]/(P)$ où P est un facteur irréductible de Φ_{p^n-1}, donc de degré n. Nous noterons $\mathbf{F}_q$ un tel corps (qui est de toute façon, isomorphe à tout autre corps de même cardinal).

4.4 Calcul dans les corps finis

Pour construire un corps fini de cardinal $q = p^n$, on doit recherche un polynôme irréductible de degré n sur $\mathbf{F}_p[X]$. C'est par exemple un facteur de Φ_{p^n-1}. On peut aussi tirer au hasard un polynôme de degré n dans $\mathbf{F}_p[X]$, (il y en a p^n) et tester si il est irréductible.

Théorème 4.23. *Soit $P \in \mathbf{F}_p[X]$ de degré n. P est irréductible si et seulement si* $\mathrm{pgcd}(P, X^{p^k} - X) = 1$, *pour tout $k \leq n/2$.*

Preuve. Un polynôme non irréductible admet un facteur irréductible de degré $d \leq n/2$, qui est donc un diviseur de $X^{p^d} - X$. CQFD

Il existe un toute généralité un algorithme de factorisation des polynômes à coefficients dans $\mathbf{F}_p[X]$, c'est l'algorithme de Berlekamp.

Une fois donné un polynôme P de degré n, irréductible, on écrit que le corps $\mathbf{K} = \mathbf{F}_p[X]/(P)$ est un corps à $q = p^n$ élément. Notant $\alpha = \overline{X}$, la classe de X dans $\mathbf{K}$, les éléments de $\mathbf{K}$ s'écrivent $x = \sum_{i=0}^{n-1} a_i \alpha^i$, de façon unique. Le polynôme minimal de α est P.

Il est commode par la suite de trouver un générateur de $\mathbf{K}^*$. Soit parce que son polynôme minimal est un des facteurs de Φ_{p^n-1}, soit parce que nous avons trouvé un générateur en tirant au hasard un élément de $\mathbf{K}^*$. La probabilité est $\varphi(p-1)/(p-1)$.

Applications à la cryptographie

5 Applications à la cryptographie

Le lecteur intéressé pourra lire avec intérêt les ouvrages de G. Zémor ([10]) ou de P. Wassef ([2]).

5.1 Principe de la cryptologie

C'est la communication entre deux ("Bob" et "Alice") individus (ou un individu et une machine ou deux machines) sur un réseau, sachant que les informations transitant sur ce canal peuvent être écoutées (par un "pirate"). De quelque nature que soit l'information (chiffres, lettres, etc), on peut supposer que celle-ci consiste en une suite d'entiers.

Par exemple pour représenter une information utilisant les 26 lettres de l'alphabet romain $\mathcal{F} = \{a, b, c, \ldots\}$, on choisit une bijection entre $\mathcal{F}$ et $\{0, 1, \ldots, 25\}$.

Longtemps, on a utilisé un algorithme de substitution basé sur une bijection de $\mathcal{F}$. Jules César avait imaginé un décalage de trois lettres. Ces méthodes, plus ou moins élaborées, basés sur un mécanisme de substitution souffraient de plusieurs défauts :

1. Les lettres de l'alphabet n'apparaissent pas avec la même fréquence dans une phrase (par exemple les lettres *e, s*, si bien qu'en étudiant les propriétés statistiques des textes codés, on pouvait les décoder.
2. Le chiffrement et le déchiffrement reposait sur le partage par l'expéditeur et le ou les destinataires d'une clé secrète commune. ceci implique un risque de divulgation sans parler du risque d'usurpation.

Avec les algorithmes à clé publique, ces problèmes disparaissent. Il n'est pas nécessaire de partager une clé secrète. Seul le destinataire sait décoder le message en disant publiquement de quelle façon il convient de crypter les messages à son intention.

L'idée générale est basée sur le fait que certaines fonctions f, même connues de tous sont extrêmement difficile à inverser.

5.2 Algorithme RSA

L'algorithme RSA, inventé par Rivest-Shamir-Adleman (1978), est un *cryptosystème à clé publique*. Il repose sur la propriété suivante.

Lemme 5.1. *Soit n un entier tel que $n = pq$, avec p et q deux nombres premiers distincts. Alors*

$$ed = 1 + k\varphi(n) \Rightarrow a^{ed} \equiv a \pmod{n} \text{ pour tout } a \in \mathbf{N}.$$

Chaque utilisateur du réseau se construit une clé publique et une clé secrète de la façon suivante :

1. Choisir deux nombres premiers grands (de l'ordre de 100 chiffres) p et q. Calculer $n = pq$. Connaissant n, il est très difficile de retrouver p et q (difficulté de factoriser un grand entier naturel n).
   L'entier n est rendu public mais p et q sont secrets.

2. Choisir un entier d premier avec $\varphi(n)$ (rappelons que $\varphi(n) = (p-1)(q-1)$).
   Remarque : d est donc inversible dans $\mathbf{Z}/\varphi(n)\mathbf{Z}$. L'entier d est secret.
3. Calculer l'inverse e de d dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$.
4. La *clé publique* de l'utilisateur est (e,n) et sa *clé secrète* est $(d,\varphi(n))$.

Si "Alice" veut envoyer un message à un utilisateur "Bob" dont la clé publique est (e,n), elle procède de la façon suivante.

1. "Alice" représente le message devant être transmis comme un entier $M \in [0,\dots,n-1]$, i.e. $M \in \mathbb{Z}/n\mathbb{Z}$.
2. "Alice" encrypte M par le cryptogramme $C = M^e \pmod n$.
3. "Bob" reçoit C et le décrypte (i.e. retrouve le message M) en calculant $C^d \pmod n$, car, d'après le Lemme 5.1, $C^d \mod n = M^{ed} \mod n = M$.

5.3 Cryptanalyse

Avec les notations précédentes, une personne souhaitant déchiffrer M, est ramené au problème de calculer $\varphi(n)$, ce qui est équivalent à connaître p et q, tels que $n = pq$. En effet

Lemme 5.2. *Connaître n et $\varphi(n)$ est équivalent à la connaissance de p et q.*

Preuve. En effet, si on connaît p et q, on calcule $n = pq$ et $\varphi(n) = (p-1)(q-1)$.

Mais si on connaît $n = pq$ et $\varphi(n) = (p-1)(q-1) = n-(p+q)+1$, alors, on connaît $pq = n$ et $p+q = n-\varphi(n)+1$, c'est-à-dire, on connaît p et q. CQFD

On doit donc choisir p et q suffisamment grand (de l'ordre de 150 chiffres décimaux), pour qu'il ne soit pas possible de factoriser n en un temps raisonnable. Aujourd'hui, avec les algorithmes les plus sophistiqués, il faudrait 1500 ans à un processeur 2.GHz pour factoriser un entier RSA de taille 768 (231 chiffres décimaux). Les algorithmes efficaces ont une complexité de l'ordre de $O(\ell^{1/4})$ où ℓ est un majorant du plus grand facteur premier de n.

p et q ne doivent pas être trop proches l'un de l'autre. En effet, en posant $s = 1/2(p-q)$ et $t = 1/2(p+q)$, on a l'égalité $n = t^2 - s^2$ et donc $t^2 - n$ est un carré. Si p et q sont proches, alors on peut chercher des carrés de la forme $t^2 - n$ où t est proche de $\sqrt{n}$.

$p-1$ et $q-1$ ne doivent pas avoir trop de petits facteurs (friabilité).

On peut ensuite se poser la question de savoir si il est difficile de trouver m, connaissant $c = m^e$. Ce problème est réputé difficile et on pense qu'il est équivalent à celui de factoriser n en $n = p \cdot q$.

5.4 Signature

Imaginons un observateur Oscar, qui intercepte le message crypté et qui le remplace par un autre, en voulant se faire passer pour Alice. Il doit être nécessaire à Bob de pouvoir être certain que l'expéditeur du message est bien Alice. C'est un problème d'authentification.

L'algorithme RSA fournit aussi un procédé de signature (ou d'authentification). "Bob" a pour clé publique (e,n) et pour clé secrète $(d,\varphi(n))$. Supposons que "Bob" veuille envoyer un message $M \in \mathbf{Z}/n\mathbf{Z}$ à "Alice" sans se préoccuper de confidentialité mais en sorte que "Alice" puisse vérifier que l'expéditeur est bien "Bob". Pour cela "Bob" envoie le couple (M,M'), où $M' = M^d \pmod n$. Alors "Alice" peut calculer (e étant public) $M'^e = M^{de} = M \pmod n$.
Comme seul "Bob" connaît d, si la propriété précédente est vraie, "Bob" est bien l'expéditeur.

5.5 Problème du logarithme discret

Soit $\mathbf{F}_q$ un corps fini et g un générateur de son groupe multiplicatif $\mathbf{F}_q{}^*$. L'application

$$\begin{array}{ccc} \mathbb{Z}/(q-1)\mathbb{Z} & \overset{\exp_g}{\to} & \mathbf{F}_q{}^* \\ i & \mapsto & g^i \end{array}$$

est un isomorphisme de groupes. Si on connaît g et i, il est facile de calculer $\exp(i) = g^i$. Par contre l'isomorphisme inverse appelé *logarithme discret de base g"* est difficile à calculer (si certaines conditions sont remplies : q est grand, q n'est pas une puissance de 2 et $(q-1)$ a un facteur premier grand...). Il s'agit du morphisme

$$\begin{array}{rcl} \mathbf{F}_q{}^* & \stackrel{l_g}{\to} & \mathbb{Z}/(q-1)\mathbb{Z} \\ u & \mapsto & i \text{ tel que } u = g^i. \end{array}$$

Le *problème du logarithme discret* s'énonce ainsi : étant donnés q, cardinal d'un corps fini, g un élément primitif de $\mathbf{F}_q$, u un élément de $\mathbf{F}_q{}^*$, trouver l'entier i, $0 \leq i \leq q-2$, tel que $u = g^i$. On note alors $u = \log_g i$.

Certains algorithmes de cryptographie sont basés sur le fait que le problème du logarithme discret est difficile dans certains corps $\mathbf{F}_q$. Aujourd'hui les meilleurs algorithmes requièrent une complexité en $O(\sqrt{q})$.

5.6 Algorithme de chiffrement à clé publique de El Gamal

Soit $\mathbf{F}_q$ un corps fini dans lequel le problème du logarithme discret est difficile et g un élément primitif. Le couple $(\mathbf{F}_q, g)$ est public.

Supposons que Alice veuille permettre à quiconque de lui envoyer confidentiellement un message.
Alice choisit un entier e tel que $1 < e < q-1$ et rend public g^e qui est sa clé publique.
Un autre utilisateur, disons Bob, peut envoyer à Alice un message $M \in \mathbf{F}_q{}^*$ de façon confidentielle en procédant comme suit.
Bob choisit un entier x tel que $1 < x < q-1$ et transmet le couple (g^x, Mg^{xe}) à Alice.
Alice, connaissant e, peut alors trouver le message M puisque
$g^{-ex} = (g^x)^{(q-2)e}$ d'où $M = (Mg^{xe})g^{-ex}$.

5.7 Protocole d'échange de clés de Diffie-Helman

Soit $\mathbf{F}_q$ un corps fini dans lequel le problème du logarithme discret est difficile et g un élément primitif. Le couple $(\mathbf{F}_q, g)$ est public.

Supposons que Alice et Bob veuillent se construire une clé secrète commune en communiquant sur un canal non secret.

Alice choisit un entier a tel que $1 < a < q-1$ et transmet g^a à Bob.

Bob choisit de son côté un entier b tel que $1 < b < q-1$ et transmet g^b à Alice.

La clé secrète sera g^{ab}. Alice peut calculer la clé secrète ($g^{ab} = (g^b)^a$), Bob aussi ($g^{ab} = (g^a)^b$), mais aucun intrus connaissant g^a et g^b ne peut calculer g^{ab} sauf s'il peut résoudre le problème du logarithme discret de base g dans $\mathbf{F}_q$.

Bibliographie

[1] Alin Bostan, Frédéric Chyzak, Marc Giusti, Romain Lebreton, Grégoire Lecerf, Bruno Salvy, and Éric Schost. *Algorithmes Efficaces en Calcul Formel*. Frédéric Chyzak (auto-édit.), Palaiseau, September 2017. 686 pages. Imprimé par CreateSpace. [PDF].

[2] M. Demazure. *Cours d'Algèbre*. Cassini, 2008.

[3] J. von zur. Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 03 edition, juin 2013.

[4] D. E. Knuth. *The Art of Computer Programming, volume 2*. Addison-Wesley, 1997.

[5] A. Kraus. *Arithmétique, 2M220*. L2 Mathématiques, UPMC, 2016.

[6] P. Naudin and Cl. Quitté. *Algorithmique algébrique*. Masson, 1992.

[7] V. Shoup. A computational introduction to number theory and algebra, 2008. [PDF].

[8] P. Wassef. *Arithmétique : application aux codes correcteurs et à la cryptographie : cours et 122 exercices corrigés : licence de mathématiques*. Vuibert, 2008.

[9] L. Zapponi. *Cryptologie algébrique*. M1 Mathématiques, UPMC, 2018.

[10] G. Zémor. *Cours de cryptographie*. Cassini, 2017.