ARITHMÉTIQUE

Table des matières

Contextualisation

L'arithmétique, ou théorie des nombres, est le champ mathématique qui se focalise sur les nombres entiers : les opérations que l'on peut utiliser, les propriétés qu'ils vont vérifier, et les diverses extensions à des nombres puis des structures plus compliqués.

On sait construire et décrire les ensembles d'entiers au regard de l'opération d'addition de manière extrêmement simple : c'est l'arithmétique de Peano. Mais qu'en est-il du point de vue de la multiplication ? De manière plus générale, il est en général trivial de couper un objet en une somme de deux éléments, mais difficile de le décomposer en un produit. La notion de divisibilité, au centre de ce TD, interroge ainsi sur la structure des ensembles d'entiers vis-à-vis de l'opération de produit.

L'état de l'art en arithmétique se caractérise habituellement par des propriétés d'énoncé extrêmement simples, mais recelant une complexité énorme. De nombreux théorèmes ou conjectures agitent la communauté mathématique depuis des décennies voire des siècles ; c'est un champ dans lequel les travaux soulèvent sans cesse de nouvelles difficultés.

Ces difficultés sont justement le terreau des applications de l'arithmétique à la cryptographie : il s'agit de jouer sur le fait que les solutions des problèmes de codage sont extrêmement difficiles à trouver sans information, mais très rapides à calculer moyennant la connaissance d'une étape intermédiaire (ce qui jouera le rôle de clé privée). On va ainsi construire des processus inattaquables si ce n'est par force brute, en annihilant cette possibilité par l'usage de nombres de taille gigantesque, tout en conservant une utilisation efficace par une connaissance partielle et secrète de l'architecture du problème.

Enfin, certains résultats, algorithmes, procédés que l'on utilise en arithmétique tirent leur existence de propriétés structurelles [1] des ensembles d'entiers. Il est donc possible de les étendre à des objets autres que des nombres mais qui vérifieraient ces mêmes propriétés [2] ; nous donnerons l'exemple des polynômes en seconde partie. La difficulté non négligeable de certains problèmes ne doit pas faire oublier que ceux-ci n'ont pour origine que des opérations basiques sur des objets simples, et ainsi peuvent trouver un écho dans de nombreux autres domaines.

Projet AFIT

Le projet AFIT qui se déroule en parallèle de ce TD porte sur le domaine de l'arithmétique entière. Vous trouverez dans la documentation fournie pour ce projet énormément de résultats de cours et d'exemples censés vous faire comprendre les phénomènes utilisés, ainsi que des approches différentes de certains des aspects étudiés ; vous serez amenés à comprendre et utiliser des résultats d'arithmétique pour implémenter des méthodes de chiffrement.

L'étude du poly associé est complémentaire de ce TD, et certains exercices pourront y faire référence. Prenez le temps de le lire et n'hésitez pas à demander des précisions à vos enseignants en mathématiques.

Attendus

L'arithmétique reposant en grande partie sur des calculs dont la complexité peut vite devenir ingérable manuellement, il faut distinguer ce que l'on va attendre de vous à l'écrit de ce qu'il faut que vous maîtrisiez pour pouvoir utiliser efficacement – dans votre projet par exemple – les connaissances liées au sujet.

1. En ce qui nous concerne, il s'agit en grande partie de la structure d'anneau : vous en trouverez une présentation succincte dans votre poly AFIT.

2. Plus tard au cours de votre scolarité, vous étudierez diverses structures algébriques et manipulerez différents ensembles d'objets munis de ces structures ; par exemple les espaces vectoriels dès le semestre prochain. Les propriétés purement structurelles restent vraies quel que soit le type d'objet manipulé : on a exactement les mêmes propriétés sur les espaces vectoriels de nombres, de fonctions, de matrices etc.

Approche structurelle

Ce cours d'arithmétique veut comprendre ou trouver des résultats sur "l'architecture" des entiers ou polynômes : comment on peut les construire, les décomposer etc. On attend ainsi de vous que vous soyez capables de :

— Apprécier l'intérêt de la notion de divisibilité et ses applications algorithmiques, avec les stratégies de diviser pour régner.
— Vous représenter les nombres premiers / polynômes irréductibles comme des "briques de base" de la construction par produit, et tirer les conséquences utiles de son existence et son unicité (caractérisation par bijectivité des deux représentations nombre - facteurs, application aux calculs de base, parallélisation des calculs).
— Comprendre les avantages de l'arithmétique modulaire (congruences) : simplicité, réduction de la complexité, ... , et ses inconvénients : déperdition d'information, limitations (dépassements)..., et savoir quand et comment il convient de l'utiliser.

Aspect algorithmique

Vous serez amenés à utiliser de nombreux algorithmes de résolution de problèmes (exemples : algorithme d'Euclide (étendu), factorisations, divisions polynomiales...). Pour cela il vous faut donc :

— Comprendre les objets de base associés : division euclidienne, facteurs irréductibles, exponentiation ...
— Savoir justifier les résultats qui permettent de prouver la convergence de l'algorithme vers le résultat recherché.
— Avoir une idée de la complexité des opérations.
— Le cas échéant, être capable de choisir parmi plusieurs possibilités celle qui va donner le résultat le plus rapidement (par exemple, la discussion sur les problèmes d'exponentiation).

Utilisation pratique

L'utilisation des résultats étudiés prendra deux formes ici : utilisation manuelle via des applications numériques simples, et utilisation en machine avec des nombres gigantesques (projet AFIT). Vous devrez donc

— être capables d'appliquer les algorithmes "à la main" sur des valeurs raisonnables : c'est ce que l'on vous demandera à l'écrit (exercices et examens) mais c'est aussi une manière de vérifier les résultats de vos fonctions lors du projet (en établissant une base de données de tests simples).
— Savoir réduire au maximum les problèmes pour se limiter à des capacités gérables (notamment avec les puissances).
— Utiliser les données structurelles pour transformer les problèmes ou les réduire en sommes de petits problèmes.

Plus spécifiquement, section par section :

Divisibilité sur les entiers
— Manipuler la relation d'ordre
— Assimiler la compatibilité ou non avec les opérations algébriques (addition, multiplication)
— Comprendre la division euclidienne et identifier pourquoi le couple (q, r) résultat de cette division existe et est unique

Congruences
— Comprendre l'intérêt de la structure modulaire, l'utilisation des classes d'équivalence
— Savoir simplifier des calculs modulaires via les opérations compatibles
— Relier congruence et reste de division euclidienne

Primalité
— Décrire un nombre en produit de facteurs premiers
— Avoir une idée de la "rareté" de ces nombres
— Montrer et utiliser la primalité relative de deux nombres (simplification, parallélisation)

— Comprendre l'importance des facteurs communs à deux nombres et les limitations que cela implique dans ce qu'ils vont engendrer par opérations diverses
— Comprendre le fonctionnement de l'algorithme d'Euclide, et pourquoi il converge
— Réfléchir à la complexité de cet algorithme

Théorème de Bézout
— Savoir le retrouver de manière constructive via l'algorithme d'Euclide
— Utiliser cette méthode pour la détermination simultanée[3] des coefficients de Bézout lors de l'algorithme d'Euclide
— être capable d'utiliser ce théorème pour démontrer des résultats théoriques[4]
— Comprendre l'intérêt constructif de ce théorème dans la recherche de l'inversion d'un élément (donc la résolution d'une équation).

Petit théorème de Fermat
— Comparer la complexité d'un calcul de puissances avec ou sans le théorème de Fermat
— Remarque : il vous est difficile à l'heure actuelle de comprendre d'où vient ce théorème. Une démonstration plus structurelle est donnée dans le poly AFIT, qui vous permettra peut-être de mieux visualiser son fonctionnement.

Polynômes et opérations
— Remarquer le parallèle entre les entiers et les polynômes, comprendre qu'il n'est dû qu'à des raisons de structure (on peut utiliser les mêmes opérations avec les mêmes propriétés)
— Connaître le comportement vis-à-vis des opérations supplémentaires : dérivation et composition
— Maîtriser les opérations sur le degré

Division euclidienne (polynômes)
— Comprendre que la condition d'arrêt sur le degré garantit l'unicité, l'existence étant algorithmique
— Savoir appliquer un algorithme de division polynomiale

Racines et factorisation
— Faire le lien entre racine et factorisation par un polynôme de degré 1
— Connaître et comparer les différentes manières de faire apparaître et calculer la multiplicité d'une racine
— Utiliser les racines pour simplifier des calculs en faisant disparaître des termes non désirés
— Avoir des premières intuitions sur le nombre de racines d'un polynôme
— Savoir extraire les racines d'un polynôme de degré 2
— Réfléchir à des moyens algorithmiques de trouver des racines de polynômes de degrés supérieurs en utilisant des connaissances issues d'autres domaines.

Théorème de d'Alembert - Gauss
— Caractériser les polynômes irréductibles dans $\mathbb{R}[X]$.
— Savoir décomposer un polynôme en un produit de polynômes irréductibles dans $\mathbb{R}[X]$.

Première partie

Arithmétique sur les entiers

1 Relation de divisibilité sur les entiers et division euclidienne

1.1 Résumé

La relation de divisibilité constitue la première étape dans l'approche des ensembles d'entiers par l'opération de produit : c'est une comparaison qui détermine si un entier peut être écrit comme multiple

3. Il est très important au niveau complexité de comprendre que des objets vérifiant la même relation de récurrence peuvent être calculés en même temps sans perte d'espace

4. C'est un théorème d'existence, il faut donc être précautionneux sur l'utilisation des quantificateurs. Ce n'est pas une équivalence ou une égalité.

d'un autre, c'est-à-dire si l'on peut, en ajoutant plusieurs fois un nombre donné, obtenir le nombre voulu. Néanmoins, c'est une relation partielle ; il est en effet assez peu probable [5] que parmi deux entiers pris au hasard, l'un des deux soit multiple de l'autre. Il va donc falloir compléter cette notion par des approches plus fines : ce sera l'objet des sections suivantes.

Les intérêts de cette notion en informatique sont nombreux : en effet, pouvoir décomposer un entier en produit d'entiers plus petits ouvre la porte aux stratégies de diviser pour régner. Une factorisation non triviale d'un entier scinde en effet un problème en deux sous-problèmes beaucoup plus petits ; il sera en général moins coûteux de résoudre ces problèmes simplifiés et de recoller les résultats que de travailler avec des grands nombres, le côté logarithmique de la complexité des opérations impliquées offrant un gain substantiel en temps et en espace. De plus, dans le cas où les sous-problèmes sont indépendants, on peut même paralléliser les calculs ce qui permet d'avoir un gain de temps encore plus important [6].

Si la divisibilité ne permet pas toujours de comparer deux entiers positifs a et b, on peut néanmoins toujours approcher un nombre par un multiple d'un autre, moyennant un certain reste r : l'identité $a = bq + r$ est ce que l'on appelle une division de a par b. La division euclidienne est celle dont le reste r est positif mais strictement inférieur au diviseur b.

1.2 Exercices

Exercice 1.1

1. Chercher tous les diviseurs de 84 puis de 60.
2. Les diviseurs de 60, divisent-ils 120 ? divisent-ils 30 ?
3. Quels sont les diviseurs communs à 84 et 60 ?
4. 12 est un diviseur commun de 84 et 60, est-ce que 12 divise $84 + 60$? $84 - 60$?

Exercice 1.2

Soient a, b et c trois entiers relatifs, tels que $c \mid a$ et $c \mid b$.

1. Montrer que $c \mid (a + b)$.
2. Montrer que pour tout $u \in \mathbb{Z}$, $c \mid ua$.
3. En déduire que pour tout couple (u, v) de $\mathbb{Z}^2$, $c \mid (ua + vb)$.

Exercice 1.3

1. Étudier toutes les relations de divisibilité existant sur $[\![1; 12]\!]$.
2. Montrer que la relation de divisibilité sur $[\![1; 12]\!]$ est une relation d'ordre. Est-elle totale ou partielle ? Peut-on étendre ce résultat sur $\mathbb{N}$?
3. Établir le diagramme de Hasse de cette relation sur l'ensemble $[\![1; 12]\!]$.

Exercice 1.4

1. Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Rappeler l'énoncé du théorème de la division euclidienne de a par b.
2. En admettant l'existence du couple (q, r) résultat de cette division, montrer son unicité.
3. Trouver le quotient et le reste de la division euclidienne de a par b dans les cas suivants :
   (a) $a = 24$ et $b = 5$.
   (b) $a = 24$ et $b = -5$
   (c) $a = -24$ et $b = 5$
   (d) $a = -24$ et $b = -5$
   (e) $a = 5$ et $b = 24$
   (f) $a = -5$ et $b = 24$

5. Une fois les nombres choisis, la probabilité est en fait égale à l'inverse du plus petit des deux nombres.
6. Un exemple d'exploitation de la factorisation d'entiers pour paralléliser des calculs est donné dans la section 5 de votre poly AFIT.

2 Relation de congruence

2.1 Résumé

La notion de congruence tire son intérêt de la régularité de la répartition des multiples d'un entier donné : elle permet de matérialiser une symétrie profonde dans l'organisation des nombres par rapport aux multiples d'un nombre donné. C'est une relation d'équivalence, dont toutes les classes sont de structure identique : elle permet de classer simplement les entiers par rapport à un entier de référence donné, loin de l'apparence chaotique et du manque d'informations qui semblent se dégager de la relation de divisibilité.

Le reste de la division euclidienne de a par b donne un représentant simple (compris entre 0 et $b-1$) de la classe d'équivalence de a : $a \equiv r\ [b]$.

L'arithmétique modulaire (qui concerne les entiers vus via une relation de congruence) est d'intérêt fondamental en informatique : structurellement, car les opérations sur les entiers dans un ordinateur se font sur un intervalle limité (la capacité) et donc sont en fait des opérations de congruence relativement à l'entier maximum ; et de manière plus appliquée en cryptographie, où les propriétés des congruences permettent d'établir des méthodes de chiffrement faciles à calculer et implémenter et difficiles à casser.

Cette relation étant compatible avec les opérations d'addition et de multiplication, elle est d'utilisation très facile, et permet souvent de ne dégager de calculs lourds que la partie qui va nous intéresser au final. Mieux, une gestion intelligente des congruences dans lesdits calculs aide à faire disparaître des problèmes intermédiaires comme les dépassements de capacité et réduit en général drastiquement le temps nécessaire aux calculs : non seulement on fait moins d'opérations, mais elles concernent des nombres plus petits et sont donc plus rapides.

Cette notion peut être étendue à d'autres objets que les entiers. On a déjà vu comment les arguments des nombres complexes sont en fait définis via une relation de congruence modulo 2π. Mais on peut même songer à des congruences de polynômes, puisque ceux-ci vérifient toutes les propriétés structurelles des entiers qui nous intéressent ici...

2.2 Exercices

Exercice 2.5

1. Faire la division euclidienne de 158 par 6 et trouver un entier k, $0 \leqslant k < 6$, tel que : $158 \equiv k\ [6]$
2. Écrire les entiers de 0 à 30. Entourer en bleu les entiers n tels que $n \equiv 0\ [6]$. Entourer en rouge les entiers p tels que $p \equiv 2\ [6]$. Qu'observez-vous ?
3. On observe que $8 \equiv 2\ [6]$, $26 \equiv 2\ [6]$ et $15 \equiv 3\ [6]$.
   (a) Quelle est la relation de congruence entre 8 et 26 ?
   (b) Que peut-on dire de $8+15$? 8×15 ? 2×8 ?
   (c) $20 \equiv 2\ [6]$. Que peut on en déduire pour 10 ?

Exercice 2.6

Soit $n \in \mathbb{N}^*$.

1. Montrer que la relation de congruence modulo n est une relation d'équivalence.
2. Montrer que cette relation est compatible avec l'addition et la multiplication, c'est-à-dire :

$$\text{Si } a \equiv c\ [n] \text{ et } b \equiv d\ [n] \text{ alors } a+b \equiv c+d\ [n] \text{ et } ab \equiv cd\ [n].$$

Exercice 2.7

Critères de divisibilité

On note b_i les digits d'un entier n en base 10, de telle sorte que n s'écrive $n = \sum_{i \geqslant 0} b_i 10^i$ avec $0 \leqslant b_i \leqslant 9$ pour tout $i \geqslant 0$.

1. a. Montrer que $n \equiv b_0$ [2] et $n \equiv b_0$ [5].
   b. En déduire un critère de divisibilité par 2 et par 5.
2. a. Montrer que $n \equiv \sum_{i \geqslant 0} b_i$ [3] et $n \equiv \sum_{i \geqslant 0} b_i$ [9].
   b. En déduire un critère de divisibilité par 3 et par 9.
3. a. Montrer que $n \equiv \sum_{i \geqslant 0} (-1)^i b_i$ [11].
   b. En déduire un critère de divisibilité par 11.
4. Tester ces critères sur 239 734.

Exercice 2.8

1. Montrer (sans récurrence) que pour tout $n \in \mathbb{N}$, $3^{2n+1} + 2^{n+2}$ est divisible par 7.
2. Montrer (sans récurrence) que pour tout $n \in \mathbb{N}$, $3^{n+3} - 5.4^{4n}$ est divisible par 11.

3 Primalité et primalité relative

3.1 Résumé

Les nombres premiers sont en quelque sorte les briques de base de l'ensemble des entiers, quand on essaie de le construire par des multiplications : ce sont les nombres qui ne peuvent pas être scindés en produit d'entiers inférieurs. Un résultat crucial de l'arithmétique des entiers est que tout entier non nul s'écrit de manière unique comme un produit de facteurs premiers, ce qui implique qu'on peut entièrement caractériser l'ensemble des entiers par celui des nombres premiers, au regard de la multiplication. Cette connaissance structurelle ouvre la porte à des approches de type "diviser pour régner" pour tout ce qui concerne des calculs ou raisonnements pour lesquels la multiplication est l'opération cruciale.

Cependant, la difficulté de cette modélisation réside dans le fait qu'il est difficile (coûteux) de déterminer si un nombre est un nombre premier, de trouver des nombres premiers, d'effectuer une décomposition en produit de nombres premiers. Si l'on connaît de plus en plus de résultats théoriques sur les nombres premiers, ceux-ci sont en général loin d'être exploitables et il n'existe à l'heure actuelle aucune méthode efficace pour générer des nombres premiers. La difficulté de ce problème est ce qui en fait un candidat idéal pour la cryptographie, où la résolution de telles questions sera une manière d'implémenter une couche de difficulté dans les questions de chiffrement et déchiffrement.

S'il est peu aisé de déterminer les facteurs d'un nombre (sauf bien sûr par force brute), on a en revanche un algorithme efficace qui permet de déterminer si deux nombres ont des facteurs en commun : l'algorithme d'Euclide. Fondé sur la division euclidienne, cet algorithme permet de déterminer facilement le PGCD de deux entiers : en effet, on peut y parvenir en itérant des divisions euclidiennes (cf. exercice 3-15).

De la simplicité de cet algorithme, on déduit qu'il est en fait plus facile de trouver des facteurs communs à deux entiers que de trouver un facteur d'un seul entier, on peut donc imaginer une recherche de décomposition comme une suite de recherches de PGCD [7]...

Ainsi, la notion de primalité relative occupe un rôle important en arithmétique modulaire, non seulement car elle permet de faciliter de nombreuses approches (diviser pour régner, parallélisation de sous-problèmes indépendants, simplifications via le lemme de Gauss), mais aussi car c'est un problème que l'on sait résoudre facilement.

7. Cette méthode est notamment utilisée pour factoriser des polynômes, étant par exemple à la base des algorithmes de Berlekamp ou de Cantor-Zassenhaus.

3.2 Exercices

Exercice 3.9

1. Reprendre le diagramme de Hasse de l'exercice 1-3
   (a) Quels sont les nombres premiers compris dans $[\![1;12]\!]$?
   (b) Comment se positionnent-ils dans ce diagramme ?
2. Reprendre les diviseurs de 84 à l'exercice 1-1 .
   (a) Remarquer que ces diviseurs vont par couples (d, d') tels que $d \leqslant d'$ et $dd' = 84$.
   (b) En déduire que, dans chacun de ces couples, $d \leqslant \sqrt{84}$.

Exercice 3.10

Soit n un entier supérieur ou égal à 2. On note d son plus petit diviseur strictement supérieur à 1 (remarque : un tel entier existe, car l'ensemble des diviseurs strictement supérieurs à 1 étant une partie non vide – elle contient n – de $\mathbb{N}$, elle admet un plus petit élément).

1. Montrer que d est un nombre premier.
2. Montrer que si n n'est pas premier alors $d \leqslant \sqrt{n}$.
3. En déduire que si aucun nombre premier inférieur ou égal à $\sqrt{n}$ ne divise n, alors n est premier.

Exercice 3.11

En utilisant le crible d'ératosthène, trouver tous les nombres premiers inférieurs à 100.

★ **Exercice 3.12**

Montrer que l'ensemble des nombres premiers $\mathcal{P}$ est infini.

Exercice 3.13

1. Décomposer en facteurs premiers 84 et 60.
2. Reprendre les diviseurs de 84 et de 60 énumérés à l'exercice 1-1. Quel est leur lien avec les facteurs premiers de 84 et 60 ?
3. Que peut-on dire des diviseurs communs à 84 et 60 ?

Exercice 3.14

Décomposer en produit de facteurs premiers les nombres 9360 et 4200. En déduire leur PGCD.

Exercice 3.15

1. Soit $(a, b) \in \mathbb{Z}^2 \backslash \{(0, 0)\}$, on écrit la division $a = bq + r$.
   Montrer que $a \wedge b = b \wedge r$.
2. Expliquer pourquoi l'algorithme d'Euclide converge, et pourquoi le dernier reste non nul est le PGCD des deux entiers de départ.

Exercice 3.16

En utilisant l'algorithme d'Euclide, calculer le PGCD de 9360 et 4200.
Comparer avec la méthode utilisée dans l'exercice 3-14.

4 Théorème de Bézout

4.1 Résumé

Le théorème de Bézout est un théorème existentiel, c'est-à-dire qu'il énonce qu'il existe des solutions à un problème donné : ici écrire le PGCD de deux nombres comme une somme de multiples de ces nombres. Souvent, ce genre de résultat est difficilement utilisable de manière appliquée ; mais ce n'est pas le cas ici puisque l'on dispose d'un méthode constructive et efficace pour démontrer le théorème

en en donnant une solution particulière : celle-ci utilise l'algorithme d'Euclide, et la compatibilité de la forme voulue (combinaision entière) avec les opérations de la division euclidienne (addition et multiplication). Vous trouverez une explication détaillée de cette méthode ainsi que des conseils pour une implémentation intelligente dans votre poly AFIT.

Remarquez que si précédemment on pouvait se cantonner aux entiers positifs, ce n'est plus le cas avec le théorème de Bézout qui trouve des coefficients sous forme d'entiers relatifs.

Le théorème de Bézout trouve des applications pratiques en cryptographie : la recherche de coefficients de Bézout donne un moyen de résoudre des équations diophantiennes qui peuvent correspondre à des inversions modulaires, permettant le décodage efficace d'un message, voire le cassage d'un code.

4.2 Exercices

Exercice 4.17

1. Reprendre les diviseurs communs de 84 et 60, identifier le pgcd. Quel est le lien entre les diviseurs communs et le pgcd en termes de divisibilité.
2. On considère deux nombres relatifs a et b tels que $(a, b) \neq (0, 0)$.
   (a) Montrer que tout diviseur commun de a et b divise aussi $a \wedge b$.
   (b) Montrer que tout nombre peut s'écrire sous la forme $ua + vb$ si et seulement si c'est un multiple de $a \wedge b$.

Exercice 4.18

Soit $(a, b, c) \in \mathbb{N}^3$.

1. À l'aide du théorème de Bézout, montrer que a est premier avec b et c si et seulement si a est premier avec bc.
2. À l'aide du théorème de Bézout, montrer que a est premier avec b si et seulement si $a + b$ est premier avec ab.

Exercice 4.19

1. A quelle condition sur $n \in \mathbb{N}$, le nombre entier $3^{n+3} + n.4^{4n}$ est-il divisible par 11 ?

Exercice 4.20

1. à l'aide de l'algorithme d'Euclide, calculer le PGCD de 237 et 156 et donner un couple de coefficients de Bézout associés.
2. Résoudre dans $\mathbb{Z}^2$ l'équation $237x + 156y = 3$.
3. Trouver tous les entiers $z \in \mathbb{Z}$ tels que $52z \equiv 1$ [79].

Exercice 4.21

Résoudre dans $\mathbb{Z}^2$ les équations ci-dessous en respectant les étapes suivantes :

a. Trouver une solution particulière.

b. Déterminer l'ensemble des solutions en citant le Lemme de Gauss au moment où vous l'utilisez.

(E1) $544x - 944y = 160$

(E2) $134x - 56y = 24$

5 Petit théorème de Fermat

5.1 Résumé

Le petit théorème de Fermat donne un résultat simple sur le calcul de puissances modulo un nombre premier. L'exponentiation modulaire est un problème crucial en cryptographie : pour les algorithmes

RSA et ElGamal étudiés dans le projet AFIT, c'est l'opération qui permet le chiffrement et le déchiffrement des messages. Cette opération très coûteuse [8] par la méthode naïve se retrouve extrêmement simplifiée grâce au résultat énoncé par le petit théorème de Fermat, qui réduit énormément le nombre d'opérations nécessaires tout en utilisant des nombres plus petits. C'est donc un résultat théorique structurel qui permet d'améliorer la facilité et la rapidité des calculs, ce qui est d'autant plus important que la solidité des algorithmes énoncés vient de l'utilisation de nombres extrêmement grands pour limiter les possibilités de résolution par force brute. Ainsi, on peut augmenter la complexité de cassage du problème avec des nombres gigantesques sans impact négatif sur son efficacité pour l'utilisateur.

Le théorème de Fermat peut être reformulé ainsi : (p premier) $\Longrightarrow$ ($a \wedge p = 1 \Longrightarrow a^{p-1} \equiv 1\ [p]$). Cette implication n'est pas une équivalence : il existe en effet des nombres [9] qui ne sont pas premiers mais vérifient la propriété de droite. Ainsi on ne peut pas utiliser cette relation pour caractériser à coup sûr un nombre premier. On peut néanmoins en déduire des tests probabilistes de primalité ; on peut également considérer que les nombres en question sont aussi utiles que les nombres premiers pour l'utilisation que l'on compte en faire. On parle alors de pseudo-primalité : un nombre n est pseudo-premier de base a si $a^{n-1} \equiv 1\ [n]$, et absolument pseudo-premier s'il vérifie la propriété pour tout a premier avec lui.

5.2 Exercices

Exercice 5.22

1. Calculer le reste dans la division euclidienne de 529^{326} par 17.
2. Calculer le reste dans la division euclidienne de 288^{288} par 29.

Exercice 5.23

Le but de cet exercice est de donner une preuve différente [10] du petit théorème de Fermat : une démonstration par récurrence qui utilise le lemme de Gauss et la formule du binôme.

Soit p un nombre premier.

1. Montrer que pour tout entier k vérifiant $0 < k < p$, alors p divise C_p^k.
   Remarque : ce résultat n'est pas vrai pour un nombre composé [11] (vous pouvez chercher des contre-exemples).
2. Montrer par récurrence sur $n \in \mathbb{N}$ que $n^p \equiv n\ [p]$.
3. On suppose maintenant que n n'est pas un multiple de p. Montrer alors que $n \wedge p = 1$, puis en déduire que $n^{p-1} \equiv 1\ [p]$.

8. voire impossible pour des raisons de capacité
9. appelés pseudo-premiers, ou nombres de Carmichael. Les plus petits sont 561, 1105 et 1729.
10. Vous trouverez dans votre poly AFIT une preuve du théorème d'Euler : si $a \wedge n = 1$ alors $a^{\varphi(n)} \equiv 1\ [n]$, où φ désigne la fonction indicatrice d'Euler. Le petit théorème de Fermat en est un cas particulier.
11. c'est-à-dire un nombre qui peut s'écrire comme un produit d'au moins deux facteurs premiers (possiblement identiques), ce qui équivaut à dire qu'il admet un diviseur strictement compris entre 1 et lui-même ; il s'agit donc de tout nombre non premier supérieur ou égal à 4.

Deuxième partie
Arithmétique sur les polynômes

6 Polynômes et opérations

6.1 Résumé

Un polynôme à coefficients dans un ensemble donné est une expression que l'on obtient en faisant uniquement des additions, des produits d'indéterminées et des multiplications par les coefficients. Formellement, un polynôme à une indéterminée sera représenté [12] par la suite à support fini [13] de ses coefficients.

Sur les ensembles de polynômes à une indéterminée à coefficients réels, ou complexes – notés $\mathbb{R}[X]$ et $\mathbb{C}[X]$ – on a naturellement des opérations d'addition et de multiplication qui vérifient les mêmes propriétés que sur les entiers [14], ainsi on va pouvoir prolonger les concepts définis pour les entiers : divisibilité, division euclidienne, PGCD, théorème de Bézout... Les polynômes irréductibles sont le pendant des facteurs premiers : on ne peut pas les scinder en un produit de deux polynômes de degrés strictement inférieurs. Et tout polynôme se décompose de manière unique comme le produit d'une constante et de polynômes irréductibles unitaires [15].

On ne peut cependant pas réduire les polynômes à un calque des entiers : ce sont des objets plus complexes, ainsi leur utilisation est beaucoup plus large, comprenant d'autres opérations comme la composition et la dérivation. Ce sont néanmoins des objets engendrés par des opérations basiques et qui gardent une relative simplicité d'utilisation, c'est pourquoi ce sont de très bons candidats pour les problèmes d'interpolation (approximation par des objets plus faciles à manipuler) : on pourra penser plus tard aux formules de Taylor, à l'interpolation de Lagrange, au théorème de Weierstrass et aux séries de Fourier via des polynômes trigonométriques [16].

6.2 Exercices

Exercice 6.24

Soit P un polynôme de degré m et Q un polynôme de degré n avec $n \leqslant m$.

Donner une condition nécessaire et suffisante sur les coefficients de P et Q pour que le degré de $P+Q$ soit égal à m.

Exercice 6.25

Montrer qu'un polynôme P est de degré n si et seulement si $P^{(n)}$ est une constante non nulle, et dans ce cas donner la valeur de cette constante en fonction des coefficients de P.

Exercice 6.26

Déterminer tous les polynômes P tels que $P(2)=6,\ P'(2)=1,\ P''(2)=4$ et $\forall n \geqslant 3 \quad P^{(n)}(2)=0$.

7 Division euclidienne de polynômes

7.1 Résumé

La division euclidienne sur les polynômes est similaire à celle sur les entiers, avec une condition sur le reste un peu différente puisqu'elle porte sur son degré. C'est cette condition qui nous garantit

12. C'est également un représentation possible en machine, via une liste par exemple.
13. c'est-à-dire nulle à partir d'un certain rang
14. C'est la structure d'anneau, cf. poly AFIT
15. Un polynôme est dit unitaire si son coefficient dominant, c'est-à-dire lié au monôme de plus haut degré, est 1. La multiplication par une constante non nulle ne changeant rien à la divisibilité des polynômes, on se restreint à des polynômes unitaires pour conserver un caractère unique et limiter les calculs qui se compensent.
16. Ces procédés permettent même de définir des suites de polynômes convergeant vers ce que l'on veut modéliser, tout en donnant une maîtrise de la vitesse de convergence.

encore une fois la convergence de l'algorithme d'Euclide, car la suite des degrés des restes est positive et strictement décroissante tant que le reste est non nul. On peut donc une fois encore calculer algorithmiquement le PGCD de deux polynômes.

La division euclidienne simple est déjà en elle-même résolue de manière algorithmique : on procède étape par étape en décrémentant le degré d'un reste provisoire jusqu'à ce qu'il vérifie la condition voulue (ce qui correspond au moment où l'on ne peut plus pratiquer l'algorithme). Réitérer ce procédé pour calculer un PGCD peut donc être assez long à la main, mais ne pose aucun problème en machine, si ce n'est la forte séquentialité.

En ce qui concerne le PGCD, afin d'obtenir son unicité on fixe le coefficient dominant comme étant égal à 1 : on dit alors que le polynôme est unitaire. En effet, la multiplication par une constante non nulle n'a aucun effet sur la divisibilité de polynômes. Cette convention sera souvent reprise, permettant de se restreindre "à une constante multiplicative près" à des opérations sur les polynômes unitaires.

Enfin, remarquons qu'il existe d'autres types de division que la division euclidienne pour les polynômes [17], qui trouvent des niches d'utilisation différentes : c'est par exemple le cas de la division selon les puissances croissantes, qui utilise un procédé semblable à celui de la division euclidienne mais dans l'autre sens (en augmentant les degrés).

7.2 Exercices

Exercice 7.27

à l'aide de l'algorithme d'Euclide, déterminer le PGCD de $X^2 + X - 2$ et $X^3 - 2X^2 + 3X - 2$.

Exercice 7.28

1. Effectuer la division euclidienne de $X^4 + 2X^3 + X$ par $X^2 + 1$.
2. En déduire une primitive sur $\mathbb{R}$ de la fonction $\left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \dfrac{x^4 + 2x^3 + x}{x^2 + 1} \end{array} \right.$

8 Racines et factorisation

8.1 Résumé

Les racines d'un polynôme représentent les solutions de l'équation polynomiale associée, c'est-à-dire les valeurs de l'indéterminée pour lesquelles l'expression va s'annuler. L'étude des racines permet donc de résoudre les nombreux problèmes faisant intervenir des modélisations polynomiales. D'autre part, le lien entre racine et factorisation vu à l'exercice 8-29 permet d'imaginer un procédé itératif de factorisation polynomiale, moyennant une méthode efficace pour trouver des racines.

Comme pour la multiplicité d'un facteur premier dans la décomposition d'un entier, la multiplicité d'une racine a d'un polynôme P correspond à la puissance de $(X - a)$ dans la décomposition en irréductibles de P. Une caractérisation par les dérivées successives est possible, puisque *grosso modo* la multiplicité d'une racine est décrémentée de 1 par la dérivation. Le fait qu'une racine est de multiplicité au moins 2 si et seulement si c'est aussi une racine de P' donne une manière assez simple d'isoler la partie d'un polynôme qui contient les facteurs au moins carrés : il suffit de calculer le PGCD de ce polynôme et de son polynôme dérivé [18].

Si l'on connaît des méthodes pour extraire les racines d'un polynôme de degré 2 (et également de degré 3 ou 4 via de longs changements de variables et l'utilisation des nombres complexes), il n'existe plus de résolution par radicaux [19] pour les degrés supérieurs. La recherche de racines de

17. C'est déjà le cas pour les entiers, mais peu ont un réel intérêt. On peut néanmoins citer la division qui choisit un reste de plus petite valeur absolue possible : $-\frac{b}{2} < r \leqslant \frac{b}{2}$ que CamL utilise par exemple, qui donne un algorithme d'Euclide modifié un peu plus rapide.

18. C'est pourquoi la plupart des algorithmes de factorisation polynomiale, comme les algorithmes de Berlekamp et Cantor-Zassenhaus précédemment cités, se contentent de chercher à factoriser des polynômes sans facteur carré : le traitement qui consiste à traquer les facteurs multiples via un PGCD est une première étape implicite.

19. c'est-à-dire par des opérations arithmétiques basiques sur les coefficients et des extractions de racines.

polynômes est encore un problème qui fait l'objet d'une abondante production d'algorithmes. Si pour les solutions réelles on peut imaginer utiliser des résultats d'analyse fonctionnelle (exemple : une recherche dichotomique grâce au théorème des valeurs intermédiaires), cela n'est plus valable pour les racines complexes. Ainsi, même des problèmes concernant des expressions polynomiales, c'est-à-dire engendrées par les opérations arithmétiques les plus simples, peuvent présenter une résolution extrêmement compliquée...

De même que pour les entiers, la factorisation de polynômes permet l'utilisation de stratégies diviser pour régner et la mise en place de moyens de parallélisation des calculs. Nous verrons plus tard l'intérêt des polynômes en algèbre linéaire (notamment en ce qui concerne la réduction des matrices carrées) et en quoi leur utilisation et leurs factorisations permettent de trivialiser des calculs à l'apparence complètement chaotique [20].

8.2 Exercices

Exercice 8.29

1. Soit $P \in \mathbb{K}[X]$ avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et $a \in \mathbb{K}$. Quel est le reste dans la division euclidienne de P par $X - a$?
2. En déduire la propriété suivante :

$$(X - a) \mid P \iff P(a) = 0$$

Exercice 8.30

On considère dans $\mathbb{R}[X]$ le polynôme $P(X) = X^3 + 3X - 6\sqrt{3}$.

1. Montrer que $\sqrt{3}$ est l'unique racine réelle de P.
2. Posons $a = \sqrt[3]{2\sqrt{7} + 3\sqrt{3}}$ et $b = \sqrt[3]{2\sqrt{7} - 3\sqrt{3}}$. Calculer $a^3 - b^3$ puis ab et en déduire que $a - b$ est une racine de P.
3. En déduire que $\sqrt[3]{2\sqrt{7} + 3\sqrt{3}} - \sqrt[3]{2\sqrt{7} - 3\sqrt{3}} = \sqrt{3}$.

Exercice 8.31

Soit $n \geqslant 2$.

1. Montrer que le polynôme $P(X) = (X + 1)^{2n} - 1$ est divisible par $X^2 + 2X$.
2. Montrer que $(X - 1)^2$ divise $nX^{n+1} - (n + 1)X^n + 1$.
3. Montrer que 1 est racine du polynôme $nX^{n+2} - (n + 2)X^{n+1} + (n + 2)X - n$. Quelle est sa multiplicité ?

Exercice 8.32

Déterminer le reste de la division euclidienne de $Q(X) = (X - 2)^{2n} + (X - 1)^n - 2$ par

1. $(X - 2)(X - 1)$.
2. $(X - 1)^2$.

Exercice 8.33

Trouver tous les polynômes unitaires de degré 3, divisibles par $X - 1$ et dont les restes lors des divisions par $X - 2$, $X - 3$ et $X - 4$ sont égaux.

20. Et *vice versa*, comment on peut utiliser des méthodes de calcul matriciel et des résultats théoriques pour trouver des racines de polynômes. On peut par exemple imaginer une recherche récursive de racines d'un polynôme à l'aide de l'algorithme des puissances itérées appliqué à sa matrice compagnon.

9 Théorème de d'Alembert-Gauss

9.1 Résumé

Ce théorème d'énoncé très simple est d'une puissance fondamentale pour la manipulation des polynômes de notre point de vue : on en déduit par exemple que tout polynôme complexe est le produit d'une constante et de polynômes (unitaires) de degré 1. Ainsi, toutes les pathologies du cas réel disparaissent : le nombre de racines (comptées avec multiplicité) est égal au degré du polynôme, il n'y a jamais de racine non complexe etc. Cela a un impact important sur les théories utilisant des polynômes de manière sous-jacente : la réduction matricielle est plus simple avec des complexes qu'avec des réels, les résultats (décomposition en séries de Fourier, formules des racines, etc.) obéissent à une formule et non à divers sous-cas ...

Il permet également de résoudre le problème réel : en effet, au contraire de ce qui se passe avec les nombres premiers, on peut caractériser exactement les polynômes irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$ grâce à ce théorème. La divisibilité polynomiale est donc en réalité beaucoup plus simple que la divisibilité des entiers.

9.2 Exercice

Exercice 9.34

1. On considère le polynôme $P(X) = X^4 + 2X^3 - X - 2$.
   (a) Montrer que 1 et -2 sont racines de P.
   (b) En vous aidant d'une division euclidienne, factoriser P en produit de polynômes irréductibles dans $\mathbb{R}[X]$.

2. On considère le polynôme $Q(X) = X^4 - 2X^3 - 3X^2 + 8X - 4$.
   (a) Montrer que 2 et -2 sont racines de Q.
   (b) En vous aidant d'une division euclidienne, factoriser Q en produit de polynômes irréductibles dans $\mathbb{R}[X]$.

3. On considère le polynôme $R(X) = X^4 - 3X^3 - 3X^2 + 11X - 6$.
   (a) Montrer que 1 est racine de R. Quelle est sa multiplicité ?
   (b) En vous aidant d'une division euclidienne, factoriser R en produit de polynômes irréductibles dans $\mathbb{R}[X]$.