Université Abdelmalek Essaadi
Ecole Nationale des Sciences Appliquées
Département de Mathématiques
Al Hoceima, Maroc

: Module Mathématiques I :

Arithmétique dans Z

Filière :

Cycle Préparatoire : Sciences et Techniques Pour l'Ingénieur

Année : 2020-2021

Professeur: Younes ABOUELHANOUNE

I Divisibilité, nombres premiers

I.1 Notion de divisibilité

Définition 18.1.1 (Divisibilité, diviseur, multiple)

- Soit a et b deux entiers relatifs, $b \neq 0$. On dit que b *divise* a, et on écrit $b \mid a$, si et seulement s'il existe $q \in \mathbb{Z}$ tel que $a = bq$.
- On dit dans ce cas que b est un *diviseur* de a, et que a est un *multiple* de b.

On note $a \mid b$ pour dire que a divise b.
Ainsi, $2 \mid 4$, $-2 \mid 4$, $2 \mid -4$, et $-2 \mid -4$.

Proposition 18.1.2 (Caractérisation de la divisibilité en termes d'idéaux)

Soit a et b deux entiers positifs, $a \neq 0$. Alors $a \mid b$ si et seulement si $b\mathbb{Z} \subset a\mathbb{Z}$.

Définition 18.1.3 (couple d'entiers associés)

On dit que deux entiers a et b sont associés si et seulement si $a \mid b$ et $b \mid a$, c'est-à-dire $a\mathbb{Z} = b\mathbb{Z}$.

Proposition 18.1.4 (Caractérisation des entiers associés)

Les entiers a et b sont associés si et seulement si il existe $\varepsilon \in \{-1, 1\}$ tel que $a = \varepsilon b$.

Remarque 18.1.5

- Ce résultat peut sembler trivial et sans intérêt. Sa version plus générale, pour un anneau intègre A, est plus intéressante, et affirme que les éléments associés diffèrent d'une constante mutliplicative appartenant au groupe A^* des inversibles de A.
- Par exemple, dans $\mathbb{K}[X]$, les éléments associés à un polynôme P sont tous les λP, pour $\lambda \in \mathbb{K}^*$.
- Dans $\mathbb{Z}[\mathrm{i}]$ (entiers de Gauss), les éléments associés à un nombre z sont les 4 éléments z, $-z$, $\mathrm{i}\,z$ et $-\mathrm{i}\,z$.
- Les éléments associés de x sont les éléments qui jouissent des mêmes propriétés de divisibilité que x.

Théorème/Définition 18.1.6 (Théorème de la division euclidienne)

Soit $(a, b) \in \mathbb{Z}^2$, $b \neq 0$.

- *Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :*

$$a = bq + r \qquad et \qquad 0 \leqslant r < |b|.$$

- *L'entier q est appelé quotient de la division euclidienne de a par b.*
- *L'entier r est appelé reste de la division euclidienne de a par b.*

Remarquez que b peut être négatif.

Exemples 18.1.7

1. $27 = 6 \times 4 + 3 = 6 \times 3 + 9 = 6 \times 6 - 3$.
   Ainsi, des identités $a = bq + r$, il y en a beaucoup, mais une seule vérifie la condition imposée sur r. Ici, le quotient de la division de 27 par 6 est 4, et son reste est 3.

2. $27 = (-6) \times (-4) + 3 = (-6) \times (-5) - 3$.
   Sans la valeur absolue dans la condition sur r, c'est la deuxième égalité qui aurait été la bonne. Mais la valeur absolue impose un reste positif. Ainsi, le quotient de la division de 27 par -6 est -4, et le reste est 3
3. $-27 = 6 \times (-4) - 3 = 6 \times (-5) + 3$.
   Ici, on voit que si on change le signe du nombre divisé, le quotient n'est pas simplement l'opposé (attention, cela ne correspond pas à la plupart des implémentations informatiques de la division euclidienne). Ainsi, la première identité ne convient pas. Le quotient de la division euclidienne de -27 par 6 est -5, le reste est 3.
   Remarquez que la situation est la même que pour la partie entière, pour laquelle $\lfloor -x \rfloor \neq -\lfloor x \rfloor$, sauf lorsque x est entier. C'est normale, puisque la partie entière n'est autre que le quotient de la division euclidienne (réelle) par 1.
4. $-27 = (-6) \times 5 + 3$.
   Sans surprise, le quotient de la division euclidienne de -27 par -6 est 5, le reste est 3.

La plupart des propriétés arithmétiques de $\mathbb{Z}$ (pour ne pas dire toutes) découlent de l'existence de cette division euclidienne. On peut définir de façon similaire dans certains anneaux une division euclidienne, la condition sur le reste étant un peu plus dure à exprimer. On parle dans ce cas d'anneau euclidien.

Définition 18.1.8 (Anneau euclidien, HP)

Soit A un anneau. On dit que A est euclidien s'il est intègre, et muni d'un stathme, c'est-à-dire d'une application $v : A \setminus \{0\} \to \mathbb{N}$ telle que :

$$\forall a \in A, \quad \forall b \in A \setminus \{0\}, \quad \exists (q, r)^2 \in A, \quad a = bq + r \qquad \text{et} \qquad (r = 0 \text{ ou } v(r) < v(n))$$

Exemple 18.1.9

- Quel est le stathme pour la division euclidienne dans $\mathbb{Z}$?
- Quel est le stathme pour la division euclidienne dans $\mathbb{C}[X]$?
- On peut montrer que $\mathbb{Z}[\mathrm{i}]$ est euclidien, de stathme $z \mapsto \not{z}|^2$.

Ainsi, $\mathbb{Z}$ et $\mathbb{R}[X]$ sont des anneaux euclidiens. Cette dernière propriété nous permettra d'établir un certain nombre de propriétés arithmétiques pour les polynômes, très similaires à celles qu'on a pour les entiers.

Remarques 18.1.10

- Certains auteurs appellent préstathme la notion de stathme telle que nous l'avons définie. Ils imposent une condition supplémentaire pour les stathmes. La différence n'est pas trop gênante dans la mesure où on peut montrer qu'avec leur terminologie, tout anneau intègre muni d'un préstathme peut aussi être muni d'un stathme.
- Dans la notion générale de division euclidienne définie par stathme, on n'impose pas de propriété d'unicité. Par exemple, dans $\mathbb{Z}[\mathrm{i}]$, on n'a pas de propriété d'unicité.

Note Historique 18.1.11

La division euclidienne est appelée ainsi par référence à Euclide qui décrit dans ses éléments le procédé algorithmique de soustractions répétées permettant d'obtenir le quotient et le reste. Cependant, on trouve trace de cette notion à des époques antérieures, notamment en Égypte.
C'est Gauss le premier, avec l'étude de $\mathbb{Z}[\mathrm{i}]$, qui remarque que de nombreuses propriétés arithmétiques ne sont pas spécifiques à $\mathbb{Z}$ et découlent de façon plus générale de l'existence d'une division euclidienne dans un anneau. Cette remarque est évidemment à la base de la notion d'anneau euclidien.

I.2 Congruences

De façon quasi-indissociable de la notion de division euclidienne, nous définissons :

Définition 18.1.12 (Congruences d'entiers)

Soit $n \in \mathbb{N}^*$, et $(a,b) \in \mathbb{Z}^2$. On dit que a et b sont *congrus* modulo n, et on écrit $a \equiv b\ [n]$, si et seulement si n divise $b-a$, ou encore si les divisions euclidiennes de a et b par n ont même reste.

On trouve aussi assez souvent la notation $a \equiv b \mod n$, ou un mélange des 2 : $a \equiv b\ [\text{mod } n]$.
Nous rappelons les résultats suivants, que nous avons déjà eu l'occasion de démontrer.

Théorème 18.1.13

La relation de congruence modulo n est une relation d'équivalence.

Théorème 18.1.14

La relation de congruence modulo n est compatible avec le produit et la somme : soit $(a,a',b,b') \in \mathbb{Z}^4$ tels que $a \equiv a'\ [n]$ et $b \equiv b'\ [n]$. Alors $a+b \equiv a'+b'\ [n]$ et $ab \equiv a'b'\ [n]$

En d'autre terme, c'est une congruence sur les monoïdes $(\mathbb{Z},+)$ et $(\mathbb{Z},\times)$, au sens vu dans le chapitre sur les ensembles.
Ces règles sont importantes pour pouvoir mener à bien le calcul modulaire de façon efficace : il permet de faire lors d'une succession d'opérations, des réductions modulo n étape par étape, plutôt que de tout calculer dans $\mathbb{N}$ et de réduire à la fin.

Exemples 18.1.15

- Calculer le reste de la division euclidienne de $12 \times 21 \times 28 \times 18 \times 75 \times 23$ par 11.
- Calculer le reste de la division euclidienne de 1685^{1750} par 12.

Cette possibilité de réduire les opérations à chaque étape est également important pour l'implémentation informatique du calcul modulaire, permettant ainsi de travailler avec des entiers plus petit, diminuant de la sorte la complexité des calculs. On peut ainsi, contrairement au cas du calcul dans $\mathbb{Z}$, borner explicitement le temps de calcul des opérations modulo n par un réel dépendant de n mais ne dépendant pas des opérandes.

I.3 Nombres premiers

Nous les avons déjà rencontrés, évidemment. Nous rappelons :

Définition 18.1.16 (Nombres premiers)

Soit $p \in \mathbb{N}^*$. On dit que p est un nombre premier si p admet exactement 2 diviseurs positifs distincts (à savoir 1 et p lui-même)

Remarquez que l'existence de deux diviseurs distincts exclut d'office 1 de l'ensemble des nombres premiers, puisqu'il n'a qu'un diviseur.

Définition 18.1.17 (Nombres composés)

Soit $n \in \mathbb{N}^*$. On dit que n est un nombre composé si n possède au moins 3 diviseurs positifs distincts, ou en d'autres termes, si n possède un diviseur positif distinct de 1 et de n.

Proposition 18.1.18

Tout nombre composé admet un diviseur strict premier.

Cette proposition est à la base de l'existence de la décomposition primaire. L'unicité, quant à elle découle de ce vieux lemme, dont nous démontrons la contraposée de façon élémentaire, par descente infinie (cette démonstration est très proche de celle qu'en donne Gauss) :

Lemme 18.1.19 (Euclide)

Soit a et b deux entiers et p un entier premier tel que $p|ab$. Alors $p|a$ ou $p|b$.

Cette propriété se retraduit sur les idéaux par $ab \in p\mathbb{Z} \Longrightarrow a \in p\mathbb{Z}$ ou $b \in p\mathbb{Z}$, ou encore, dans $\mathbb{Z}/p\mathbb{Z}$:

$$\overline{a}\overline{b} = 0 \Longrightarrow \overline{a} = 0 \text{ ou } \overline{b} = 0$$

Ainsi, le lemme d'Euclide traduit le fait que $\mathbb{Z}/p\mathbb{Z}$ est intègre.

Remarque 18.1.20

Cette propriété est même une caractérisation des nombres premiers, puisque si n n'est pas premier et différent de 1, et si $n = ab$ est une décomposition non triviale, alors l'égalité $\overline{a}\overline{b} = 0$ dans $\mathbb{Z}/n\mathbb{Z}$ contredit l'intégrité. Ainsi $n > 1$ est premier si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est intègre.

De façon plus général, étant donné un anneau commutatif A, et un idéal I, I est en particulier un sous-groupe distingué de A, et on peut donc définir une structure de groupe quotient sur A/I. Il n'est pas dur de se rendre compte que la relation de congruence modulo I respecte également le produit et donc que celui-ci passe au quotient. Des vérifications immédiates montrent que A/I est alors muni d'une structure d'anneau. C'est par exemple ainsi qu'on obtient la structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$, par quotient de l'anneau $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$. La remarque précédente incite à donner la définition suivante :

Définition 18.1.21 (Idéal premier, HP)

Soit A un anneau commutatif, et I un idéal de A. On dit que I est un idéal premier de A si et seulement si A/I est intègre.

Ainsi, dans $\mathbb{Z}$, p est premier si et seulement si $p\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$ différent de $\{0\}$ et $\mathbb{Z}$ (qui sont aussi des idéaux premiers).

Théorème 18.1.22 (Combien de nombres premiers ?)

Il y a une infinité de nombres premiers.

C'est bien joli tout ça, mais comment faire pour déterminer les nombres premiers (pas trop gros) ? Erathostène, mathématicien, astronome, bibliothécaire en chef d'Alexandrie (excusez du peu), astéroïde et cratère lunaire, répondit à cette question il y a déjà très longtemps, par un procédé d'élimination.

Méthode 18.1.23 (Crible d'Érathostène)

Pour trouver tous les nombres premiers inférieurs ou égaux à n :

1. Écrire tous les nombres entiers de 2 à n.
2. Le plus petit d'eux, à savoir 2, est premier (il n'a pas de diviseur strictement plus petit que lui, autre que 1)
3. Les multiples stricts de 2 ne sont pas premiers, on les barre tous.
4. Parmi les nombres restants (en excluant les nombres premiers précédents, à savoir 2 dans la première étape, et en excluant les nombres barrés), le plus petit est premier (il n'est divisible par aucun nombre premier strictement plus petit que lui et différent de 1, sinon il serait barré). On barre tous ses multiples stricts qui ne peuvent pas être premiers, et on recommence cette étape jusqu'à épuisement de tous les entiers de la liste.

Cet algorithme est très facile à implémenter dans un langage informatique. Il n'est évidemment efficace que pour des petites valeurs de n, mais ne peut pas servir à la recherche de très grands nombres premiers. Notamment, il est à peu près inutilisable pour répondre à la question de savoir si un très grand nombre donné est premier ou non (question cruciale dans certaines situations en rapport avec des cryptages, comme la méthode RSA).

II Décomposition primaire d'un entier

II.1 Décomposition primaire

Un théorème incournable de l'arithmétique est bien sûr :

Théorème 18.2.1 (Décomposition primaire)

Tout entier strictement positif n s'écrit de façon unique sous la forme

$$n = p_1 \times \cdots \times p_k,$$

où $p_1 \leqslant \cdots \leqslant p_k$ sont des nombres premiers, ce produit étant éventuellement vide si $n = 1$.

Un anneau dans lequel on a une propriété d'existence et d'unicité (à facteurs multiplicatifs inversibles près, et à l'ordre près des facteurs) d'une décomposition en facteurs irréductibles est appelé *anneau factoriel*. Ainsi, quitte à multiplier par l'élément inversible -1 pour obtenir la décomposition d'un entier relatif, ce résultat se réexprime en disant que $\mathbb{Z}$ est un anneau factoriel. On peut montrer que tout anneau principal est factoriel. Par ailleurs tout anneau euclidien est principal. Donc tout anneau euclidien est factoriel. C'est par exemple le cas de $\mathbb{K}[X]$, lorsque $\mathbb{K}$ est un corps (ainsi tout polynôme se décompose de façon unique, à éléments inversibles près, comme produit de polynômes irréductibles). C'est par exemple aussi le cas de l'anneau $\mathbb{Z}[i]$ des entiers de Gauss. La question se pose alors, notamment dans ce dernier cas, de savoir décrire les éléments irréductibles. C'est une question pas complètement triviale dans $\mathbb{Z}[i]$, en rapport avec le théorème des deux carrés (donnant la description des entiers s'écrivant comme somme de deux carrés).

II.2 Valuations p-adique

Un nombre premier p pouvant apparaître plusieurs fois dans la décomposition de n, nous définissons :

Définition 18.2.2 (Valuation p-adique)

Soit n un entier et p un entier premier. On appelle valuation p-adique de l'entier n le nombre d'occurrences (éventuellement nul) de l'entier p dans la décomposition primaire de n.

Il s'agit donc de l'unique entier v tel que p^v divise n mais pas p^{v+1}.
En notant $\mathbb{P}$ l'ensemble des nombres premiers, il vient donc :

Proposition 18.2.3 (Reexpression de la décomposition primaire)
Pour tout $n \in \mathbb{N}^*$

$$n = \prod_{p \in \mathbb{P}} p^{v_p(n)},$$

ce produit ayant un sens, puisque constitué d'un nombre fini de termes non égaux à 1.

Proposition 18.2.4 (Règles sur les valuations)
Soit a et b deux entiers strictement positifs, et p un nombre premier.

1. *On a : $v_p(ab) = v_p(a) + v_p(b)$.*
2. *Si b divise a, on a : $v_p\left(\frac{a}{b}\right) = v_p(b) - v_p(a)$.*

Exemples 18.2.5

1. Déterminer, pour p premier, $v_p((p^2)!)$, et plus généralement $v_p((p^k)!)$, puis plus généralement $v_p(n!)$ (formule de Legendre)
2. Déterminer $v_p\left(\binom{n}{k}\right)$ en fonction de n et k.

On obtient en particulier le :

Lemme 18.2.6
Soit p un nombre premier. Alors pour tout $k \in [\![1, p-1]\!]$, $\binom{p}{k} \equiv 0\ [p]$.

De ce lemme, on tire :

Proposition 18.2.7
Soit a et b deux entiers et p un nombre premier. Alors $(a+b)^p \equiv a^p + b^p\ [p]$.

Ce résultat affirme en fait que l'application $x \mapsto x^p$ est un endomorphisme du corps $\mathbb{F}_p$ (c'est en fait l'identité d'après le petit théorème de Fermat), et plus généralement sur tout corps de caractéristique p. Il est appelé *morphisme de Frobenius*.
La proposition précédente, ainsi que nous venons de le suggérer, a un rapport très étroit avec le petit théorème de Fermat. On peut en fait démontrer ce dernier à partir de cette proposition par une récurrence assez immédiate.

Théorème 18.2.8 (Petit théorème de Fermat)

- *Soit p un nombre premier, et $x \in \mathbb{Z}$. Alors : $x^p \equiv x\ [p]$.*
- *Si de plus, $x \not\equiv 0\ [p]$, alors $x^{p-1} \equiv 1\ [p]$.*

Évidemment, cette preuve explique moins bien la raison profonde du résultat que la preuve voyant ce résultat comme un cas particulier du théorème de Lagrange, appliqué au groupe $(\mathbb{Z}/p\mathbb{Z})^*$.

Remarque 18.2.9

Le petit de théorème de Fermat est notamment beaucoup utilisé dans les tests de non primalité (avec un ordinateur !). En effet, pour montrer qu'un entier p n'est pas premier, il suffit de trouver un entier a tel que $a^p \not\equiv a\ [p]$. Ainsi, par exemple, à l'aide d'un ordinateur, on peut trouver facilement, pour $n = \frac{1}{9}(10^{31} - 1)$ (nombre contitué de 31 chiffres 1) que $2^n \not\equiv 2\ [n]$. Ainsi, n n'est pas premier. Trouver une décomposition de n est une autre paire de manches...

En revanche, déduire de la validité de tests de Fermat qu'un nombre est premier est beaucoup plus délicat, car le petit théorème de Fermat ne caractérise pas les nombres premiers : il existe des nombres composés vérifiant les identités du théorème de Fermat (la seconde identité étant alors donnée pour tout x premier avec n). Ces nombres sont appelés *nombres de Carmichael*.

III PGCD et PPCM

III.1 PGCD et PPCM d'un couple d'entiers

Lemme 18.3.1 (Somme de deux groupes abéliens)

Soit H et K deux sous groupes d'un groupe abélien $(G, +)$. Alors $H+K$ est le plus petit groupe contenant $H \cup K$.

Proposition/Définition 18.3.2 (PGCD)

Soit a et b deux entiers positifs tels que l'un au moins des entiers a et b est non nul, et $m \in \mathbb{N}^*$. Les propositions suivantes sont équivalentes :

(i) l'entier m est le maximum (pour l'ordre usuel) de $\{d \in \mathbb{N}^* \mid d \text{ divise } a \text{ et } d \text{ divise } b\}$

(ii) l'entier m est le maximum (pour l'ordre de divisibilité) de $\{d \in \mathbb{N}^* \mid d \text{ divise } a \text{ et } d \text{ divise } b\}$.

(iii) $m = \inf_{(\mathbb{N}^*, |)}(a, b)$

(iv) $a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}$

Si l'une de ces quatre conditions équivalentes est satisfaite, on dit que m est le *plus grand commun diviseur* de a et b (en abrégé : PGCD), et on le note $a \wedge b$.

Ainsi, le PGCD de a et b est entièrement caractérisé par l'égalité des idéaux (en notant (a) l'idéal engendré par a) :

$$(a) + (b) = (a \wedge b).$$

Remarquez que pour établir ce point partant de la description usuelle (premier point), on se sert du fait que tout idéal de $\mathbb{Z}$ s'écrit $\mathbb{Z} \cdot a$, donc que $\mathbb{Z}$ est principal. Le fait que $\mathbb{Z}$ est principal nous assure également que le plus petit idéal contenant a et b est engendré par un élément. C'est là une façon de définir le pgcd, comme élément générateur de l'idéal engendré par a et b.
Cette définition est valide dans tout anneau principal :

Définition 18.3.3 (PGCD dans un anneau principal, HP)

Soit A un anneau principal et a et b deux éléments de A. Un PGCD d de a et b est un élément défini de façon unique à inversibles près par :

$$(d) = (a) + (b).$$

Dans certains cas, un choix de pgcd s'impose (le pgcd positif dans $\mathbb{Z}$ par exemple). Dans ce cas on peut utiliser une notation non ambiguë ($a \wedge b$ par exemple), et parler du PGCD. Dans les autres cas, on parle d'UN PGCD, et on ne peut utiliser une notation qu'à abus près.
Le PGCD se détermine très facilement algorithmiquement en remarquant que si $a = bq + r$, $a \wedge b = b \wedge r$. Ainsi, en prenant des restes divisions euclidiennes successives le dernier reste non nul fournira le PGCD :

Algorithme 18.1 : Algorithme d'Euclide pour le calcul du PGCD

Entrée : a, b : entiers naturels
Sortie : $a \wedge b$
tant que $b > 0$ **faire**
  $a,\ b \leftarrow b,\ a \,\%\, b$
fin tant que
renvoyer a

Proposition/Définition 18.3.4 (PPCM)

Soit a et b deux entiers non nuls, et $M \in \mathbb{N}^*$. Les propositions suivantes sont équivalentes :

(i) l'entier M est le minimum (pour l'ordre usuel) de $\{m \in \mathbb{N}^* \mid a \text{ divise } m \text{ et } b \text{ divise } m\}$

(ii) l'entier M est le minimum (pour l'ordre de divisibilité) de $\{m \in \mathbb{N}^* \mid a \text{ divise } m \text{ et } b \text{ divise } m\}$

(iii) $M = \sup_{(\mathbb{N}^*,|)}(a, b)$

(iv) $M\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

Si l'une de ces quatre propositions équivalentes est satisfaite, on dit que M est le *plus petit commun multiple* de a et b (PPCM en abrégé), et on note $M = a \vee b$.

Encore une fois, ce dernier point peut être pris comme définition dans un anneau principal.

Définition 18.3.5 (PPCM dans un anneau principal, HP)

Soit A un anneau principal et a et b deux éléments non nuls de A. Alors un PPCM de a et b est un élément m tel que

$$(m) = (a) \cap (b).$$

Ce qui est parfois évident sur les idéaux ne l'est pas toujours autant pour les autres descriptions :

Proposition 18.3.6 (Distributivité du produit sur $\wedge$ et $\vee$)

Soit a et b deux entiers naturels, et c un entier naturel non nul.

1. *Si a et b ne sont pas tous les deux nuls, $(a \wedge b) \cdot c = (ac) \wedge (bc)$.*
2. *Si a et b sont non nuls, $(a \vee b) \cdot c = (ac) \vee (bc)$.*

III.2 Identité de Bézout

L'identité de Bézout est elle aussi une conséquence immédiate de la caractérisation par les idéaux :

Théorème 18.3.7 (identité de Bézout, ou théorème de Bachet-Bézout)

1. *Soit a et b deux entiers dont l'un au moins est non nul. Alors il existe des entiers relatifs x et y tels que $ax + by = a \wedge b$.*
2. *Réciproquement, étant donné un entier $d \in \mathbb{N}^*$, s'il existe des entiers relatifs x et y tels que*

$$d = ax + by,$$

alors $a \wedge b \mid d$.

Note Historique 18.3.8

- C'est le nom d'Étienne Bézout, mathématicien français du 18e siècle, qui est le plus souvent associé à ce résultat. C'est pourtant à Claude-Gaspard Bachet de Méziriac que l'on doit la première preuve, parue dans son ouvrage *Problèmes plaisans et délectables qui se font par les nombres*, paru en 1624. Sa preuve est celle que nous présentons ci-dessous (par l'algorithme d'Euclide)
- Qu'a fait Bézout alors pour avoir droit à tous ces honneurs ? Il a généralisé le résultat à d'autres situations, notamment au cas des polynômes.
- Il est intéressant de noter que le fameux ouvrage dans lequel Fermat écrivit dans une marge qu'il savait démontrer ce qu'on appelle aujourd'hui le théorème de Fermat-Wiles est en fait une traduction par Bachet de Méziriac de l'*Arithmétique* de Diophante. Le monde est petit...

La démonstration passant par les idéaux peut se généraliser dans un anneau principal. Elle possède l'inconvénient de ne pas être constructive. Il peut être intéressant de trouver explicitement des entiers x et y assurant l'égalité $ax + by = a \wedge b$. L'algorithme de la division euclidienne itéré permet à la fois de déterminer $a \wedge b$, et d'obtenir une identité de Bézout : il s'agit de l'algorithme d'Euclide. Il est intéressant de noter que cet algorithme est valide à partir du moment où l'on dispose d'une notion de division euclidienne : il peut donc être généralisé à tout anneau euclidien, dans le sens évoqué précédemment. Ainsi, par exemple, il nous permettra d'obtenir des identités de Bézout dans $\mathbb{R}[X]$.

Lemme 18.3.9

Soit a et b deux entiers positifs, $b \neq 0$. Soit r le reste de la division euclidienne de a par b. Alors $a \wedge b = b \wedge r$.

Théorème 18.3.10 (Algorithme d'Euclide)

- *Soit a et b deux entiers positifs, $b \neq 0$. En effectuant la division euclidienne de a par b, puis en effectuant la division euclidienne de b par le reste obtenue, et en continuant ainsi en divisant l'ancien reste par le nouveau reste, on finit par obtenir un reste nul.*
- *Le dernier reste non nul est alors égal au PGCD de a et de b.*
- *L'identité de la division euclidienne permet alors d'écrire, étape par étape, les restes successifs comme combinaison linéaire de a et b à coefficients dans $\mathbb{Z}$. La dernière étape fournit une identité de Bézout.*

Ainsi, en écrivant $r_0 = a$, $r_1 = b$ puis les divisions euclidiennes successives :

$$\begin{cases} r_0 &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ \vdots & \\ r_{k-2} &= r_{k-1} q_k + r_k \\ r_{k-1} &= r_k q_{k+1} + r_{k+1}, \end{cases}$$

avec $r_2 \neq 0$, $r_3 \neq 0, \ldots, r_k \neq 0$ et $r_{k+1} = 0$, on a $r_k = a \wedge b$. De plus, en posant $x_0 = 1$, $x_1 = 0$, $y_0 = 0$, $y_1 = 1$ et pour tout $i \leqslant [\![3, k]\!]$

$$x_i = x_{i-2} - q_i x_{i-1} \qquad \text{et} \qquad y_i = y_{i-2} - q_i y_{i-1},$$

on obtient pour tout $i \in [\![1, n]\!]$,

$$r_i = a x_i + b y_i,$$

donc en particulier pour $i = k$, on obtient une identité de Bézout :

$$a \wedge b = a x_k + b y_k.$$

On peut donc décrire de façon plus algorithmique :

Algorithme 18.2 : Algorithme d'Euclide étendu

Entrée : a, b : entiers naturels non nuls
Sortie : m, u, v tels que $m = a \wedge b = ua + bv$
$u, v, w, x, r, s \leftarrow 1, 0, 0, 1, a, b$;
tant que $s \neq 0$ **faire**
  $q,\ s,\ r \leftarrow r \ //\ s,\ r \ \%\ s,\ s$;
  $w,\ u \leftarrow u - qw,\ w$;
  $x,\ v \leftarrow v - qx,\ x$
fin tant que
renvoyer *(r,u,v)*

En pratique, pour ne pas s'embrouiller, mieux vaut écrire les différentes relations obtenues par la division euclidienne, en remplaçant étape par étape les restes obtenus par leur expression obtenue récursivement en fonction de a et b.

Exemple 18.3.11

- Trouver à l'aide de l'algorithme d'Euclide le pgcd de 27 et 33, ainsi qu'une identité de Bézout.
- Comment trouver une autre identité de Bézout ?
- À retenir : on n'a pas unicité de la relation de Bézout !

III.3 PGCD et PPCM d'une famille finie d'entiers

La notion de PGCD et de PPCM de deux entiers peut être généralisée à un plus grand nombre d'entiers :

Proposition/Définition 18.3.12 (PGCD d'un nombre fini d'entiers)

Soit $a_1, \ldots, a_n$ des entiers naturels, non tous nuls, et m un entier naturel. Les propriétés suivantes sont équivalents :

(i) m est le maximum (au sens de l'ordre usuel) des entiers d qui divisent chacun des a_i, $i \in [\![1, n]\!]$.
(ii) m est le maximum (au sens de la divisibilité) des entiers d qui divisent chacun des a_i, $i \in [\![1, n]\!]$.
(iii) $m = \inf_{(\mathbb{N}^*, |)}(a_1, \ldots, a_n)$
(iv) $m\mathbb{Z} = a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}$.

Si l'une de ces quatre propositions équivalentes est satisfaite, on dit que m est le PGCD de la famille $(a_1, \ldots, a_n)$ et on note $m = a_1 \wedge a_2 \wedge \cdots \wedge a_n$.

De la même façon :

Proposition/Définition 18.3.13 (PPCM d'un nombre fini d'entiers)

Soit $a_1, \ldots, a_n$ des entiers naturels, non nuls, et m un entier naturel. Les propriétés suivantes sont équivalents :

(i) m est le minimum (au sens de l'ordre usuel) des entiers m multiples de chacun des a_i, $i \in [\![1, n]\!]$.
(ii) m est le minimum (au sens de la divisibilité) des entiers m multiples de chacun des a_i, $i \in [\![1, n]\!]$.
(iii) $m = \sup_{(\mathbb{N}^*, |)}(a_1, \ldots, a_n)$
(iv) $m\mathbb{Z} = a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z}$.

Si l'une de ces quatre propositions équivalentes est satisfaite, on dit que m est le PPCM de la famille $(a_1, \ldots, a_n)$ et on note $m = a_1 \vee a_2 \vee \cdots \vee a_n$.

La caractérisation par idéaux, ou encore la caractérisation par borne inférieure (et l'associativité des

bornes inférieures) nous assure que ces notions correspondent aux PGCD et PPCM itérés :

$$a_1 \wedge \cdots \wedge a_n = ((a_1 \wedge a_2) \wedge \dots) \wedge a_n \qquad \text{et} \qquad a_1 \vee \cdots \vee a_n = ((a_1 \vee a_2) \vee \dots) \vee a_n.$$

En particulier, on en tire l'associativité de $\wedge$ et de $\vee$.
On peut étendre le théorème de Bachet-Bézout à cette situation, toujours en utilisant la caractérisation par les idéaux :

Théorème 18.3.14 (Relation de Bézout)
Soit $a_1, \dots, a_n$ des entiers naturels non tous nuls. Alors il existe des entiers relatifs $x_1, \dots, x_n$ tels que

$$a_1 \wedge \cdots \wedge a_n = x_1 a_1 + \cdots + x_n a_n.$$

Réciproquement, s'il existe des entiers $x_1, \dots, x_n$ tels que

$$d = x_1 a_1 + \cdots + x_n a_n,$$

alors d est un multiple de $a_1 \wedge \cdots \wedge a_n$.

Méthode 18.3.15
Les coefficients $x_1, \dots, x_n$ peuvent se trouver explicitement, par itération de l'algorithme d'Euclide : on cherche d'abord une relation de Bézout entre $d_1 = a_1 \wedge a_2$, a_1 et a_2, puis entre $d_2 = d_1 \wedge a_3$, d_1 et a_2 ; en substituant à d_1 la première relation trouvée, on obtient une relation de Bézout entre $a_1 \wedge a_2 \wedge a_3$, a_1, a_2 et a_3. On continue alors de la sorte, de proche en proche.

Enfin, toutes les notions introduites dans ce paragraphe peuvent être généralisées à des entiers relatifs quelconques ; le pgcd et le ppcm ne sont alors définis correctement qu'au signe près (c'est le cas général dans un anneau principal, ou le pgcd ne peut être déterminé qu'à un facteur multiplicatif inversible près). Dans le cas de $\mathbb{Z}$, on a un choix privilégié qui consiste à prendre la valeur positive. Le pgcd et les relations de Bézout se trouvent de la même façon, en les cherchant d'abord pour les valeurs absolues, puis en modifiant les signes de façon adéquate.

III.4 PGCD et PPCM vus sous l'angle de la décomposition primaire

Nous traduisons d'abord la divisibilité en terme de dévomposition primaire :

Lemme 18.3.16 (Caractérisation de la divisibilité par les valuations)
Soit a et b deux entiers non nuls. Alors $a|b$ si et seulement si pour tout $p \in \mathbb{P}$, $v_p(a) \leqslant v_p(b)$.

Étant donné deux nombres a et b, le pgcd et le ppcm de a et b s'obtiennent facilement à l'aide de leur décomposition primaire. Par exemple :

$$150 = 2 \times 3 \times 5^2 \qquad \text{et} \qquad 180 = 2^2 \times 3^2 \times 5.$$

Ainsi, $150 \wedge 180 = 2 \times 3 \times 5 = 30$ et $150 \vee 180 = 2^2 \times 3^2 \times 5^2 = 900$.
Plus généralement, en utilisant le lemme énoncé ci-dessus, on obtient :

Proposition 18.3.17
Soit a et b deux entiers strictement positifs. Alors, pour tout $p \in \mathbb{P}$,

$$v_p(a \wedge b) = \min(v_p(a), v_p(b)) \qquad \text{et} \qquad v_p(a \vee b) = \max(v_p(a), v_p(b)).$$

Cette propriété peut bien sûr être généralisée au calcul du PGCD et du PPCM d'une famille finie quelconque d'entiers naturels. On en déduit en particulier la relation suivante entre PGCD et PPCM :

Proposition 18.3.18 (relation liant le PGCD et le PPCM)

Soit a et b deux entiers naturels non nuls. Alors

$$(a \wedge b) \times (a \vee b) = ab.$$

Nous retrouverons cette relation plus tard sans nous servir de la décomposition primaire.

IV Entiers premiers entre eux

IV.1 Couple d'entiers premiers entre eux

Définition 18.4.1 (Entiers premiers entre eux)

Soit a et b deux entiers naturels non tous les deux nuls. On dit que a et b sont premiers entre eux si et seulement si $a \wedge b = 1$, donc si a et b n'ont pas d'autre diviseur positif commun que 1.

Cela peut aussi s'exprimer par la relation $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.

Note Historique 18.4.2

La première apparition de cette notion est dans le Livre VII des *Éléments* d'Euclide.

Proposition 18.4.3 (Simplification des fractions)

- *Soit a et b deux entiers naturels, $b \neq 0$. Alors $\frac{a}{a\wedge b}$ et $\frac{b}{a\wedge b}$ sont premiers entre eux.*
- *En particulier, il est toujours possible d'écrire un rationnel $\frac{a}{b}$ sous forme irréductible $\frac{a'}{b'}$, c'est-à-dire de sorte que $a' \wedge b' = 1$, en simplifiant par $a \wedge b$.*

On déduit des résultats de la section précédente :

Théorème 18.4.4 (Bézout, ou Bachet-Bézout)

Deux entiers naturels a et b sont premiers entre eux si et seulement s'il existe des entiers relatifs x et y tels que $ax + by = 1$.

En particulier :

Corollaire 18.4.5 (Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, HP)

1. *Soit $n \in \mathbb{N}^*$, et $k \in [\![0, n-1]\!]$. La classe de k modulo n est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k et n sont premiers entre eux.*
2. *En particulier, si p est premier, $\mathbb{Z}/p\mathbb{Z}$ et un corps.*

Méthode 18.4.6 (Calcul d'un inverse modulo n)

Soit k premier avec n. Pour calculer l'inverse de k modulo n, c'est-à-dire l'inverse de k dans $\mathbb{Z}/n\mathbb{Z}$, déterminer une relation de Bézout $xk+yn = 1$, par l'algorithme d'Euclide. On obtient alors $xk \equiv 1\ [n]$.

Un résultat souvent très utile pour les propriétés de divisibilité, et assez voisin du lemme d'Euclide (le lemme d'Euclide est d'ailleurs un cas particulier du lemme de Gauss) :

Lemme 18.4.7 (Lemme ou théorème de Gauss)

Soit a, b et c trois entiers naturels tels que $a \mid bc$ et $a \wedge b = 1$. Alors $a \mid c$.

Note Historique 18.4.8

Gauss démontre le lemme d'Euclide de façon élémentaire (la démonstration qu'on en a donnée), puis en déduit l'existence et l'unicité de la décomposition primaire, qu'il utilise pour démontrer son propre théorème ci-dessus. La démonstration que nous en donnons est indépendante du lemme d'Euclide, et le lemme d'Euclide peut alors être vu comme conséquence du lemme de Gauss.

En utilisant le lemme de Gauss de façon convenable sur une relation de Bézout, on obtient, indépendamment de la décomposition primaire :

Proposition 18.4.9

Si a et b sont premiers entre eux et $a|c$ et $b|c$, alors $ab|c$.

Corollaire 18.4.10 (PPCM de deux nombres premiers entre eux)

Si a et b sont premiers entre eux, $a \vee b = ab$

Cela permet de retrouver, indépendamment de la décomposition primaire, la relation entre PGCD et PPCM :

Proposition 18.4.11 (relation liant PGCD et PPCM)

Soit a et b deux entiers strictement positifs. Alors $ab = (a \wedge b)(a \vee b)$.

IV.2 Famille finie d'entiers premiers entre eux

Enfin, nous définissons deux notions sur un nombre quelconque d'entiers, à bien distinguer l'une de l'autre :

Définition 18.4.12 (Nombres premiers entre eux deux à deux)

Soit $a_1, \ldots, a_n$ des entiers naturels. On dit que $a_1, \ldots, a_n$ sont premiers entre eux deux à deux si deux entiers pris au hasard parmi ces n entiers sont toujours premiers entre eux, c'est-à-dire :

$$\forall (i,j) \in [\![1,n]\!]^2, \quad (i \neq j) \Longrightarrow a_i \wedge a_j = 1.$$

La notion suivante est moins forte :

Définition 18.4.13 (Nombres premiers entre eux dans leur ensemble)

Soit $a_1, \ldots, a_n$ des entiers naturels. On dit que $(a_1, \ldots, a_n)$ sont premiers entre eux dans leur ensemble si $a_1 \wedge \cdots \wedge a_n = 1$, ou de façon équivalente, s'il existe des entiers $x_1, \ldots, x_n$ tels que

$$x_1 a_1 + \cdots + x_n a_n = 1.$$