Chapitre 3

Arithmétique

L'arithmétique est l'étude des propriétés de divisibilité des entiers naturels. C'est un sujet d'étude depuis l'aube des temps, qui recèle des questions très difficiles, dont certaines ne sont pas encore résolues, comme par exemple la célèbre conjecture de Goldbach, qui affirme que tout nombre pair est la somme de deux nombres premiers.

3.1 Les ensembles $\mathbb{N}$ et $\mathbb{Z}$

Pour étudier les propriétés des nombres entiers (naturels ou relatifs), il faut tout d'abord se mettre d'accord sur ce que sont ces nombres. Plutôt que de décrire les propriétés des entiers, nous décrivons plutôt les propriétés des *ensembles* $\mathbb{N}$ des entiers naturels et $\mathbb{Z}$ des entiers relatifs. Nous en avons déjà vu quelques unes au début du chapitre dénombrement (paragraphe 2.1.1, page 19).

3.1.1 L'ensemble $\mathbb{N}$ des entiers naturels

On peut construire cet ensemble $\mathbb{N}$ dans le cadre de la théorie des ensembles. Nous ne le ferons pas ici, et procéderons de manière axiomatique, c'est à dire que nous allons décrire les propriétés de cet ensemble dont nous allons nous servir (et nous ne nous servirons que de ces propriétés).

L'étudiant(e) qui lit ce texte peut se demander quel est l'intérêt de faire une telle démarche "axiomatique". Après tout, les entiers "naturels" sont bien connus ! ! En fait, on peut considérer beaucoup d'ensembles de nombres : nous verrons les entiers relatifs, les rationnels, les nombres réels, les nombres complexes. Mais il y en a bien d'autres. Chaque famille possède ses propriétés particulières. Il est bon de savoir qu'avec les seules propriétés énoncées ci-dessous, on décrit bien l'ensemble des entiers que nous connaissons, et rien d'autre.

Nous admettrons donc qu'il existe un ensemble infini $\mathbb{N} := \{0, 1, 2, ...\}$, dont les éléments sont appelés *entiers naturels*. On notera $\mathbb{N}^*$ l'ensemble des entiers non nuls, c'est à dire $\{1, 2, \ldots\}$.

Sur $\mathbb{N}$, on a les structures et les propriétés suivantes.

(1) L'ensemble $\mathbb{N}$ est muni d'une relation d'ordre total, notée $\leq$, telle que toute partie non vide de $\mathbb{N}$ admet un plus petit élément : on dit que $\mathbb{N}$ est bien ordonné. On en déduit en particulier le principe de récurrence, énoncé au début du chapitre 2.

(2) L'ensemble $\mathbb{N}$ est muni de deux lois de composition + (addition) et $\times$ (multiplication). Très souvent, on ne note pas la multiplication, c'est à dire qu'on note ab au lieu de $a \times b$. Ces lois ont les propriétés suivantes :

(a) Elles sont "associatives", ce qui veut dire que

$$\forall a, b, c, \qquad (a+b)+c = a+(b+c) \text{ et } (ab)c = a(bc).$$

(b) Elles sont "commutatives", ce qui veut dire que

$$\forall a, b, \qquad a+b = b+a \text{ et } ab = ba.$$

(c) La multiplication est "distributive" par rapport à l'addition ce qui veut dire que

$$\forall a, b, c, \qquad c(a+b) = ca+cb.$$

(d) 0 est "élément neutre" pour l'addition et 1 est "élément neutre" pour la multiplication ce qui veut dire que

$$\forall a, \quad 0+a = a \text{ et } 1a = a.$$

(3) L'ensemble $\mathbb{N}$, muni de ces lois, n'est ni un "groupe", ni, *a fortiori*, un "corps", (ces notions n'ont pas été introduites, mais les étudiants curieux pourront en voir la définition à la fin du chapitre page 57). On a cependant les propriétés de *régularité* suivantes :

(a) $\forall a, b, c \in \mathbb{N}\ ,\ a+b = a+c \Longrightarrow b = c$;

(b) $\forall a \in \mathbb{N}^*, \forall b, c \in \mathbb{N}\ ,\ ab = ac \Longrightarrow b = c$;

(c) $\forall a, b \in \mathbb{N}\ ,\ ab = 0 \Longrightarrow (a = 0 \text{ ou } b = 0)$.

(4) La relation d'ordre est compatible avec l'addition et la multiplication, c'est dire que

$$a \leq b \Longrightarrow \big\{a+c \leq b+c\big\} \text{ et } \big\{ac \leq bc\big\}.$$

De plus, on a l'équivalence suivante :

$$\forall a, b \in \mathbb{N}\ ,\ a \leq b \Longleftrightarrow \big\{\exists c \in \mathbb{N}\ :\ b = a+c\big\}.$$

D'après la première propriété de régularité, un tel c est alors unique ; par définition, on dira que $c = b-a$.

(5) *Propriété d'Archimède* : soient a et b deux entiers naturels avec $b \neq 0$; il existe alors un entier naturel N tel que $a < Nb$.

Cette propriété est importante, car elle dit qu'en ajoutant autant de fois que l'on veut n'importe quel entier, on dépassera n'importe quel autre, aussi grand soit il.

Une remarque importante est la suivante. D'après la propriété de distributivité, on a $2a = a+a$, puisque $2 = 1+1$. De même, si on ajoute n fois a à lui même, $a+a+\ldots+a$, nous obtenons na, ce qui se démontre par le principe de récurrence. Donc, ab est à la fois le produit de a par b, mais aussi le résultat de la somme de b copies du nombre a, et aussi le résultat la somme de a copies du nombre b.

Exercice 60. Démontrer à l'aide de ces propriétés que toute partie non vide majorée de $\mathbb{N}$ possède un plus grand élément (voir la définition précise du mot "majorée" page 42). L'ensemble $\mathbb{N}$ admet-il un plus grand élément ?

3.1.2 L'ensemble $\mathbb{Z}$ des entiers relatifs

Nous avons déjà tous vu qu'un entier relatif est un entier naturel auquel on rajoute un signe $\pm$.

Nous ne traitons pas ici la construction formelle de cet ensemble $\mathbb{Z}$ mais nous en décrivons les propriétés fondamentales dont nous nous servirons.

(I) Il contient l'ensemble $\mathbb{N}$.

(II) Il est muni d'une relation d'ordre notée $\leq$ qui prolonge celle de $\mathbb{N}$. (Le mot "prolonger" signifie simplement que cette relation lorsqu'elle s'applique à des éléments de $\mathbb{N}$, est celle que nous connaissons déjà).

(III) Il est muni de deux opérations $+$ et $\times$ prolongeant également celles de $\mathbb{N}$.

Comme pour les entiers naturels, nous nous appuierons sur un certain nombre de propriétés, qu'on ne cherche pas à démontrer

(1) La relation d'ordre est totale. Tout entier relatif est donc soit positif ou nul (et c'est alors un entier naturel), soit strictement négatif (et c'est alors l'opposé d'un entier naturel non nul). Avec la notation (et la définition) ci-dessous de l'opposé, on peut donc écrire l'ensemble $\mathbb{Z}$ comme une réunion disjointe :
$$\mathbb{Z} = -\mathbb{N}^* \sqcup \{0\} \sqcup \mathbb{N}^*.$$

(2) Outre les propriétés énoncées sur $\mathbb{N}$, les opérations possèdent la suivante : tout élément $a \in \mathbb{Z}$ admet un unique *opposé* $-a$ tel que $a + (-a) = (-a) + a = 0$. On résume l'ensemble des ces propriétés en disant que $(\mathbb{Z}, +, \times)$ est un "anneau commutatif unitaire intègre" (voir les définitions dans la section 3.8.1, page 57). L'intégrité signifie que $ab = 0$ si, et seulement si, $a = 0$ ou $b = 0$.

(3) La relation d'ordre et la structure de groupe sur $(\mathbb{Z}, +)$ sont liées par la règle suivante :
$$a \leq b \iff b - a \in \mathbb{N}.$$

(4) La relation $\leq$ est compatible avec $+$ et $\times$ au sens suivant :
   (a) $\forall a, b, c, d \in \mathbb{Z}\ ,\ (a \leq b \text{ et } c \leq d) \Longrightarrow (a + c \leq b + d)$,
   (b) $\forall a, b \in \mathbb{Z}\ ,\ (a \leq b) \iff (-b \leq -a)$,
   (c) $\forall a, b \in \mathbb{Z}, \forall c \in \mathbb{N}\ ,\ (a \leq b) \iff (a \times c \leq b \times c)$.
   Attention : dans la dernière formule, c est supposé être dans $\mathbb{N}$, c'est à dire qu'il est positif. Si $c \leq 0$, il faut retourner le sens dans cette inégalité : si $c \leq 0$ et $a \leq b$, alors $ca \geq cb$. Ne pas oublier donc en appliquant cette formule cete condition sur c : c'est la source de très nombreuses erreurs.

(5) Contrairement à $\mathbb{N}$, toute partie non vide n'admet pas nécessairement un plus petit élément. On dit qu'une partie $E \subset \mathbb{Z}$ est *minorée* s'il existe un élément $p \in \mathbb{Z}$ (un *minorant*) telle que
$$\forall n \in E,\ n \geq p.$$
   Un plus petit élément de E est alors un **minorant de E qui appartient à E**
   De même, on dit que E est *majorée* s'il existe $p \in \mathbb{Z}$ (un *majorant*) tel que
$$\forall n \in E,\ n \leq p.$$
   Un plus grand élément de E est alors un **majorant de E qui appartient à E**
   Alors

(i) Toute partie E de $\mathbb{Z}$ **non vide et majorée** admet un plus grand élément, qu'on note $\max(E)$.

(ii) Toute partie E de $\mathbb{Z}$ **non vide et minorée** admet un plus petit élément, qu'on note $\min(E)$.

Valeur absolue

Soit $a \in \mathbb{Z}$. Si $a > 0$, alors $a > -a$. Si $a < 0$, alors $a < -a$. Si $a = 0$, alors $a = -a$. Le plus grand des entiers a et $-a$ est donc dans tous les cas un entier naturel, appelé *valeur absolue* de a et noté $|a|$:

$$|a| := \max(a, -a) = \begin{cases} a \text{ si } a \geq 0, \\ -a \text{ si } a \leq 0. \end{cases}$$

Nous avons :

(i) $|a| = 0 \iff a = 0$,

(ii) $|-a| = |a|$,

(iii) $|a + b| \leq |a| + |b|$,

(iv) $|ab| = |a|\ |b|$.

3.2 Division euclidienne

Avant de commencer, remarquons tout d'abord une formule fondamentale qui nous sera utile tout au long de ce cours

$$\forall n \geq 1,\ \forall x \in \mathbb{Z}, \qquad \boxed{x^{n+1} - 1 = (x-1)(1 + x + \cdots + x^n)}. \tag{3.1}$$

Cette formule s'applique à tous les $x \in \mathbb{Z}$, mais on verra plus tard qu'elle s'applique à tous les x réels, et en fait plus ou moins à n'importe quoi pour lequel elle fait sens. C'est en fait une égalité entre *polynômes*.

Exercice 61. Démontrer la formule. (Indication : on pourra essayer par récurrence)

Les propriétés de divisibilité des entiers reposent sur la division euclidienne.

Théorème 3.2.1 (Division euclidienne dans $\mathbb{N}$)**.** *Soient a, b deux entiers naturels avec $b \neq 0$. Alors il existe un unique couple d'entiers naturels (q, r) vérifiant $a = bq + r$ et $r < b$.*

Démonstration. —

(i) Existence

Fixons a et b, et considérons $E := \{k \in \mathbb{N} \mid a < bk\}$. On déduit de la propriété d'Archimède que E est non vide. Il a donc un plus petit élément m. Alors $m \geq 1$ (pourquoi ?) et l'on pose $q := m - 1$, $r := a - qb$. On a bien $a = bq + r$ et de plus $(m-1)b \leq a < mb$, ou encore $qb \leq a < (q+1)b$ ce qui se récrit $0 \leq r < b$.

(ii) Unicité.

Supposons $a = bq + r = bq_1 + r_1$. Supposons par exemple que $r \leq r_1 < b$. Alors $0 \leq r_1 - r < b$ et $q_1 \leq q$. Alors $b > r_1 - r = b(q - q_1)$. On en déduit que $q - q_1$ est un entier naturel strictement inférieur à 1. Donc $q = q_1$ et par conséquent $r = r_1$.

∎

Définition 3.2.2. *Dans l'énoncé du théorème, les entiers q et r sont respectivement appelés* quotient *et* reste *de la division (euclidienne) de a par b. On peut respectivement les noter $a \div b$ et $a \pmod b$.*

La propriété de division euclidienne est aussi bien valable dans $\mathbb{Z}$ que dans $\mathbb{N}$. On a aussi

Théorème 3.2.3 (Division euclidienne dans $\mathbb{Z}$)**.** *Soient a, b deux entiers relatifs avec $b > 0$ ($a \in \mathbb{Z}$, $b \in \mathbb{N}^*$. Il existe alors un unique couple d'entiers relatifs (q, r), $q \in \mathbb{Z}$, $r \in \mathbb{N}$ tel que $a = bq + r$ et tel que $0 \leq r < b$. Les entiers q et r sont respectivement appelés* quotient *et* reste *de la division (euclidienne) de a par b. On peut respectivement les noter $a \div b$ et $a \bmod b$.*

Démonstration. — Lorsque $a \geq 0$, nous sommes ramenés à la division euclidienne dans $\mathbb{N}$, et nous avons déjà traité le sujet. On peut donc supposer $a < 0$.

Les entiers relatifs a, b étant donnés, avec $b > 0$, l'existence de r et q équivaut à l'existence d'un $q \in \mathbb{Z}$ tel que $0 \leq a - bq < b$, donc à l'existence d'un entier $q \in \mathbb{Z}$ tel que

$$bq \leq a < b(q+1). \tag{3.2}$$

On considère alors $E = \{x \in \mathbb{Z}, bx \leq a\}$. Montrons que E est non vide et majoré.

Pour voir que E est non vide, nous utilisons la propriété d'Archimède de $\mathbb{N}$: on peut choisir choisir N tel que $Nb > |a| = -a$, et on vérifie alors que $-N \in E$.

Ensuite, tous les éléments de E sont négatifs, car si $x > 0$ puisque $b > 0$, alors $bx > 0$ et $a < 0$. Donc E est majoré par 0.

On peut alors choisir $q = \max(E)$, qui vérifie l'équation (3.2) par construction. ∎

Attention : Si $a < 0$, la division euclidienne de a par b n'est pas la même chose que la division euclidienne de $-a$ par b.

Exercice 62. Lorsque $a < 0$, comparer les quotients et restes (q, r) de la division de a par b et de ceux (q_1, r_1) de $-a$ par b.

3.3 Numération en base b

Nous avons l'habitude décrire des nombres en base 10. La numérotation décimale est apparue en Inde au III$^{\text{ème}}$ siècle avant J.C. Les mathématiciens musulmans l'adoptèrent rapidement après la conquête de l'Asie. Les chiffres que nous utilisons, appellés chiffres arabes, ont été introduits en occident au X$^{\text{ème}}$ siècle.

Qu'est-ce qu'écrire un nombre en base 10 ? Par exemple, le nombre 581 est **par définition** $5 \times 100 + 8 \times 10 + 1$. On peut ainsi écrire (on le démontrera grâce à la division euclidienne) tous les entiers naturels sous la forme

$$a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0,$$

où $a_0, \ldots a_n$ ne prennent que les valeurs $0, 1, \ldots 9$ (ce sont des **chiffres**), et on note par convention ce nombre $a_n a_{n-1} \ldots a_0$. Les chiffres sont juste des symboles qu'on utilise pour désigner les nombres de 0 à 9. Le choix du nombre 10 n'a rien de fondamental (il vient du fait que nous avons dix doigts pour compter !). On peut en fait compter les nombres dans n'importe quelle base $b > 1$.

Proposition 4. *Soit $b > 1$ un entier. Tout entier $n \in \mathbb{N}^*$ peut s'écrire de manière unique sous la forme :*

$$n = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0,$$

où $k \in \mathbb{N}$ et où $c_0, ..., c_k \in \{0, 1, ..., b-1\}$ et $c_k \neq 0$: les c_i sont donc des chiffres. *On dit alors que $n = c_k c_{k-1} \cdots c_1 c_0$ est* l'écriture de n en base b. *Si la base b doit être précisée, on écrit $x = (c_k c_{k-1} \cdots c_1 c_0)_b$.*

Démonstration. — Comme souvent, la preuve de l'unicité nous mettra sur la voie pour prouver l'existence. Nous commençons donc par celle-ci.

(i) Unicité.
Elle provient de l'unicité dans la division euclidienne : on écrit

$$n = c_k b^k + \ldots + c_0 = b(c_k b^{k-1} + \ldots c_1) + c_0,$$

et c_0 est donc le reste de la division euclidienne par b (donc unique) : $n = bq_0 + c_0$, où

$$q_0 = c_k b^{k-1} + c_{k-1} b^{k-2} + \ldots + c_1,$$

c'est à dire que q_0 est le nombre dont l'écriture décimale est $c_k \ldots c_1$ (on a enlevé le dernier chiffre de n).
Il ne reste plus qu'à recommencer jusqu'à la fin.

(ii) Existence. La preuve de l'unicité fournit une idée de preuve de l'existence. On divise n par b : $n = bq_0 + c_0$, puis q_0 par b : $q_0 = bq_1 + c_1$, et on continue ainsi les divisions successives de q_i par b : $q_i = bq_{i+1} + c_i$. On a $q_{i+1} < q_i$, et on s'arrête au premier rang $k-1$ tel que $q_{k-1} < b$, auquel cas on pose $c_k = q_{k-1}$. On a alors

$$n = c_k b^k + c_{k-1} b^{k-1} + \ldots c_0.$$

∎

Remarquons que dans l'écriture en base b, lorsque

$$n = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0,$$

si on appelle

$$A_k := c_{k-1} b^{k-1} + \cdots + c_1 b + c_0,$$

alors $A_k < b^k$. En effet, puisque $c_i \leq b-1$, $(i = 0, \ldots, k-1)$, alors

$$A_k \leq (b-1)(b^{k-1} + \cdots + 1) = b^k - 1.$$

Donc A_k est le reste de la division euclidienne de n par b^k, et c_k est le quotient, et nous aurions pu faire la démonstration de l'unicité (et de l'existence) à l'envers.

La numération en base b permet d'effectuer de manière efficace les opérations sur les entiers : les algorithmes appris à l'école pour le calcul en base 10 se transposent sans peine. On consultera à ce sujet l'ouvrage L1 habituel (chapitre sur l'algorithmique).

Pour écrire en base b, on a besoin de b "chiffres". Par exemple en base 4, on utilisera $0, 1, 2, 3$. Si on veut écrire dans une base plus grande que 10, par exemple en base 12, on va avoir besoin de 12 chiffres. On peut bien sûr utiliser $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, mais après ? On ne peut pas utiliser le "chiffre 10", car dans cette base, il signifie $1 \times 12 + 0 = 12$. Ni bien sûr 11. Décidons par exemple que 10 (en base 10) s'écrit A et 11 s'écrit B, et donc notre liste des chiffres (rangés dans l'ordre) est $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathrm{A}, \mathrm{B}\}$.

Que vaut alors (écrit en base 12) 3B2A ? C'est (écrit en base 10 car on y est plus habitués) : c'est $3 \times 12^3 + 11 \times 12^2 + 2 \times 12 + 10 =$?

On se référera page 59 pour voir un algorithme explicite d'écriture en base b.

Exercice 63. (*) Avec les hypothèses et notations du théorème, montrer que k est l'unique entier tel que $b^k \leq n < b^{k+1}$. En déduire la « taille » de la représentation de n en base b, c'est-à-dire le nombre de chiffres nécessaires à l'écriture de n en base b.

3.4 Divisibilité

Définition 3.4.1 (Divisibilité dans $\mathbb{N}$)**.** *Soient a, b deux entiers naturels. On dit que a* divise *b, ou que a est un* diviseur *de b, ou encore que b est un* multiple *de a, et l'on note $a|b$, s'il existe un entier naturel c tel que $b = ac$.*

Si a divise b, il divise tous les multiples de b. Si a divise b et c, il divise $b+c$; si de plus $b \leq c$, alors il divise $c - b$.

Exercice 64. Montrer que la relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre (i.e. elle est réflexive, antisymétrique et transitive).

La notion de divisibilité dans $\mathbb{Z}$ est exactement identique à celle de $\mathbb{N}$

Définition 3.4.2 (Divisibilité dans $\mathbb{Z}$)**.** *Soient a, b deux entiers relatifs. On dit que a* divise *b, ou que a est un* diviseur *de b, ou que b est un* multiple *de a, ce que l'on note $a|b$, s'il existe un entier relatif c tel que $b = ac$.*

Attention : Ce n'est pas une relation d'ordre, contrairement à ce qui se passe dans $\mathbb{N}$.
- Elle est réflexive : $\forall a \in \mathbb{Z}\ ,\ a|a$.
- Elle est transitive : $\forall a, b, c \in \mathbb{Z}\ ,\ (a|b \text{ et } b|c) \Longrightarrow a|c$.
- **Mais elle n'est pas antisymétrique** : puisque $\forall a \in \mathbb{Z}\ ,\ a|-a$ et $-a|a$.
- On a la propriété algébrique suivante :

$$\forall a, b, c \in \mathbb{Z}\ ,\ (a|b \text{ et } a|c) \Longrightarrow a|b \pm c.$$

Nous noterons $D(x)$ l'ensemble des diviseurs de $x \in \mathbb{Z}$.
Par exemple, $D(0) = \mathbb{Z}$, $D(1) = \{+1, -1\}$

Exercice 65. Calculez $D(5)$, $D(6)$ et $D(8)$.

De manière générale, si $a \neq 0$, l'ensemble $D(a)$ est fini, car tout diviseur x de a vérifie $|x| \leq |a|$. (L'ensemble $D(a)$ admet donc au plus $2|a| + 1$ éléments.)

Il est clair que $D(a) = D(-a)$, donc que $D(a) = D(|a|)$. Réciproquement, pour que $D(a) = D(b)$, il faut, et il suffit, que $b = \pm a$ (car a divise b et b divise a).

Exercice 66. Quels sont les diviseurs, les multiples, de 0, de 1, de -1 dans $\mathbb{Z}$? Quels entiers relatifs sont diviseurs de tous les entiers relatifs ? Quels entiers relatifs sont multiples de tous les entiers relatifs ?

3.4.1 Diviseurs communs

Nous allons maintenant nous intéresser à l'ensemble des *diviseurs communs* à deux entiers relatifs a, b. Cet ensemble sera noté :

$$CD(a, b) := D(a) \cap D(b).$$

Comme $D(a) = D(|a|)$ et $D(b) = D(|b|)$, on a $CD(a, b) = CD(|a|, |b|)$, et l'on peut donc se ramener au cas de deux entiers naturels. L'algorithme repose sur les idées suivantes :

Lemme 3.4.3. *Soient a, b deux entiers naturels.*
- *Si $b = 0$, alors $CD(a, b) = D(a)$.*

– *Si $b > 0$, alors $CD(a,b) = CD(b,r)$ où r est le reste de la division euclidienne de a par b.*

Démonstration. — Puisque $D(0) = \mathbb{Z}$, la première assertion est évidente. Supposons donc $b > 0$ et soit q le reste de la division euclidienne de a par b.

On a donc $a = qb + r$. Si $x \in CD(a,b)$, alors x divise $qb + r$ et b, donc $qb + r$ et qb. Il divise donc leur différence r, donc $x \in CD(b,r)$.

Réciproquement, si $x \in CD(b,r)$, alors x divise b et r. Il divise donc qb et r, donc $qb + r = a$, donc $x \in CD(a,b)$. ∎

Proposition 5 (Plus grand diviseur commun)**.** *Soient a, b deux entiers relatifs.*

(i) Il existe un unique entier naturel $d \in \mathbb{N}$ tel que $CD(a,b) = D(d)$.

(ii) L'entier d est un diviseur commun à a et b, et tout diviseur m commun à a et b est tel que $|m| \leq d$ (c'est le plus grand **en module** *des diviseurs communs).*

(iii) L'entier d est un multiple de tous les diviseurs communs à a et b.

Démonstration. — Commençons par montrer l'existence de d. On se ramène bien sûr au cas où a et b sont dans $\mathbb{N}$. Nous allons montrer la propriété par récurrence sur b. L'hypothèse de récurrence est la suivante

$$H(n) \quad : \quad \forall a \in \mathbb{N}, \exists d \in \mathbb{N}, CD(a,n) = D(d).$$

La propriété est bien sûr vraie lorsque $n = 0$, puisque qu'alors $CD(a,0) = D(a)$.

Nous appliquons le principe de la récurrence complète, et nous supposons donc que $H(r)$ est vraie pour tous les entiers $r \leq n$. Démontrons alors $H(n+1)$.

Choisissons $a \in \mathbb{N}$, et faisons la division euclidienne de a par $b = n + 1$: $a = bq + r$, avec $0 \leq r < b$, ou encore $0 \leq r \leq n$. On a

$$D(a, n+1) = D(n+1, r).$$

Puisque $r \leq n$, par l'hypothèse de récurrence,

$$\exists d \in \mathbb{N},\ CD(n+1, r) = D(d).$$

Donc, $H(n+1)$ est vraie et la preuve de l'existence est établie.

Montrons maintenant l'unicité : si $D(d) = D(d')$, alors $d = \pm d'$. Mais ces deux entiers sont dans $\mathbb{N}$ et donc $d = d'$.

Ensuite, par construction, d est bien un diviseur commun à a et b, puisque $d \in D(d)$. De plus, si $m \in CD(a,b)$, alors $m \in D(d)$ et donc $|m| \leq d$.

Ensuite, puisqu'un diviseur commun m à a et b est un élément de $D(d)$, alors $m \mid d$ et donc d est un multiple de m. ∎

Définition 3.4.4. *Soient a, b deux entiers relatifs. L'unique entier naturel d tel que $CD(a,b) = D(d)$ est appelé* plus grand commun diviseur *de a et b, et noté $pgcd(a,b)$.*

Si $pgcd(a,b) = 1$, on dit que a et b sont premiers entre eux*.*

Attention : il ne faut pas confondre "premiers entre eux" avec la notion de "nombre premier".

3.4.2 Algorithme d'Euclide et coefficients de Bézout

La démonstration de l'existence du pgcd de a et b nous donne un algorithme pour le calculer, qui s'appelle **l'algorithme d'Euclide**. En résumé, il consiste à opérer les divisions euclidiennes successives des restes jusqu'à l'obtention d'un reste nul. Le dernier reste non nul est alors le pgcd. Nous le présentons maintenant plus en détail. Soient $(a, b) \in \mathbb{N} \times \mathbb{N}^*$. On veut calculer $CD(a, b)$. On pose $r_0 := a$, $r_1 := b$. On effectue des divisions euclidiennes successives :

$$\begin{aligned} r_0 &= q_0 r_1 + r_2 \\ r_1 &= q_1 r_2 + r_3 \text{ si } r_2 \neq 0 \\ r_2 &= q_2 r_3 + r_4 \text{ si } r_3 \neq 0 \\ &\cdots \\ r_k &= q_k r_{k+1} + r_{k+2} \text{ si } r_{k+1} \neq 0 \\ &\cdots \end{aligned}$$

Comme $b = r_1 > r_2 > \cdots \geq 0$, il existe $N \geq 2$ tel que $r_{N-1} \neq 0$ et $r_N = 0$. On a alors

$$CD(a, b) = CD(r_0, r_1) = CD(r_1, r_2) = \cdots = CD(r_{N-1}, r_N) = CD(r_{N-1}, 0) = D(r_{N-1}),$$

où r_{N-1} est le dernier reste non nul. Ainsi $r_{N-1} = \text{pgcd}(a, b)$.

Dans cet algorithme, on peut calculer les r_i en fonction de a et b et des quotients q_i comme suit : $r_0 = a$, $r_1 = b$, puis

$$\begin{aligned} r_2 &= r_0 - q_0 r_1 = a - q_0 b \\ r_3 &= r_1 - q_1 r_2 = -q_1 a + (1 + q_1 q_0) b \\ r_4 &= r_2 - q_2 r_3 = (1 + q_1 q_2) a - (q_0 + q_2 + q_1 q_0 q_2) b \\ &\cdots \end{aligned}$$

A chaque étape, nous voyons que r_i s'obtient comme "combinaison linéaire à coefficients entiers" de a et b, c'est à dire qu'il existe $p_i, q_i \in \mathbb{Z}$ tels que

$$r_i = p_i a + q_i b.$$

On obtient en particulier que $\text{pgcd}(a, b) = r_{N-1} = p_{N-1}\, a + q_{N-1}\, b$. Illustrons ceci par un exemple concret.

Exemple.
Le pgcd de $a = 215$ et $b = 150$ s'obtient par les divisions euclidiennes suivantes :

$$215 = 1 \times 150 + 65,\ 150 = 2 \times 65 + 20,\ 65 = 3 \times 20 + 5,\ 20 = 4 \times 5 + 0.$$

On a donc $\text{pgcd}(215, 150) = 5$. On peut "remonter" ces égalités :

$$5 = 65 - 3 \times 20 = 65 - 3 \times (150 - 2 \times 65) = 7 \times 65 - 3 \times 150 = 7 \times (215 - 150) - 3 \times 150 = 7 \times 215 - 10 \times 150.$$

Nous renvoyons les lecteurs à la page 60 pour la forme programmable de l'algorithme d'Euclide, et nous énonçons la propriété importante qu'il permet d'établir.

Théorème 3.4.5 (Théorème de Bézout)**.** *Soient a et b deux entiers relatifs.*

(i) Il existe alors deux entiers $u, v \in \mathbb{Z}$ vérifiant la relation de Bézout *:*

$$au + bv = pgcd(a, b).$$

(ii) a et b sont premiers entre eux si, et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Attention : dans la relation de Bézout, même lorsque a et b sont dans $\mathbb{N}$, u et v sont dans $\mathbb{Z}$ en général.

Démonstration. — Montrons d'abord le premier point. On se ramène bien sûr au cas ou a et b sont dans $\mathbb{N}$. Appelons $R(a, b)$ le reste r obtenu dans la division euclidienne de a par b : $a = bq+r$. Nous avons vu dans l'algorithme d'Euclide que si nous définissons $r_0 = a$, $r_1 = b$ et

$$r_{i+2} = R(r_i, r_{i+1}),$$

alors la suite r_i est strictement décroissante, et que si n est le premier indice où $r_n = 0$, alors $\text{pgcd}(a, b) = r_{n-1}$.

Montrons donc par récurrence sur i qu'il existe deux entiers $p_i, q_i \in \mathbb{Z}$ tels que $r_i = u_i a + v_i b$. On l'établit en une récurrence à deux étapes : la propriété est vraie pour $i = 0$ et $i = 1$. Montrons que si elle est vraie pour i et $i + 1$, elle est vraie pour $i + 2$. En effet, on écrit

$$\begin{cases} r_i = u_i a + v_i b, \\ r_{i+1} = u_{i+1} a + v_{i+1} b \\ r_i = q_i r_{i+1} + r_{i+2} \end{cases}$$

On a alors

$$r_{i+2} = u_i a + v_i b - q_i(u_{i+1} a + v_{i+1} b) = (u_i - q_i u_{i+1})a + (v_i - q_i v_{i+1})b.$$

On a donc bien le résultat pour r_{i+2} avec $u_{i+2} = u_i - q_i u_{i+1}$ et $v_{i+2} = v_i - q_i v_{i+1}$.

Pour le second point, on voit donc que si $\text{pgcd}(a, b) = 1$, alors il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$. Pour la réciproque, il suffit d'observer que si $au + bv = 1$ et si d est un diviseur commun à a et b, alors d divise $au + bv$ et donc d divise 1. Donc $d = \pm 1$ et a et b sont premiers entre eux. ∎

3.5 Factorisation en nombres premiers

Nous allons démontrer le "Théorème fondamental de l'arithmétique" : l'écriture d'un entier naturel $n \geq 2$ en produit de facteurs premiers est unique, à l'ordre des facteurs près.

La plupart des énoncés ci-dessous sont déjà bien connus des étudiants, mais ils n'en n'ont sans doute pas vu la preuve formelle. Les arguments employés dans ces preuves se retrouveront dans d'autres domaines où l'on dispose aussi d'une division euclidienne, comme dans l'étude des polynômes. C'est pourquoi il est important de bien voir quel est l'enchaînement des idées qui amènent à la décomposition d'un nombre en facteurs premiers.

Définition 3.5.1. *On dit qu'un entier naturel p est* premier*, ou encore que c'est* un nombre premier*, si $p \geq 2$ et si les seuls diviseurs de p sont 1 et p.*

Pour qu'un entier $p > 1$ soit premier, il faut et il suffit qu'il ne soit pas produit de deux entiers strictement plus grands que 1. De manière équivalente :

$$p = ab \text{ avec } a, b \in \mathbb{N} \Longrightarrow a = 1 \text{ ou } b = 1.$$

Autre caractérisation : n n'est pas premier si $n = 1$, ou si l'on peut écrire $n = ab$ avec $a, b < n$. Les premiers nombres premiers sont $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$.

Remarquons que si un nombre n n'est pas premier, alors il admet un facteur premier inférieur à $\sqrt{n}$. En effet, s'il n'est pas premier, alors il s'écrit ab, où $a, b \neq 1$. Les facteurs premiers de a et b (qui peuvent être a et b eux mêmes), sont aussi des facteurs premiers de n. Donc, si p est le plus petit facteur premier de n, alors $a \geq p$ et $b \geq p$, et par conséquent $n \geq p^2$, ou encore $p \leq \sqrt{n}$.

Par exemple, puisque les nombres premiers inférieurs à 10 sont $2, 3, 5, 7$, pour vérifier qu'un entier inférieur à 100 est premier, il suffit de vérifier qu'il n'est pas divisible par $2, 3, 5, 7$.

Exercice 67. Combien y a-t-il de nombres premiers inférieurs à 100 ? (On n'en demande pas la liste). Indication : utilisez la formule du crible.

Théorème 3.5.2. *Tout entier naturel est produit de nombres premiers.*

Démonstration. — Nous l'avons déjà vue dans le chapitre précédent (Exemple 2.1.1, page 20). ∎

Corollaire 3.5.3. *Il y a une infinité de nombres premiers.*

Démonstration. — Raisonnons par l'absurde : notons $p_1, \ldots, p_k$ tous les nombres premiers et soit $n := p_1 \cdots p_k + 1$. Puisque $n \geq 2$, il est divisible par un nombre premier, donc par l'un des p_i. Ce p_i divise $n = p_1 \cdots p_k + 1$ et aussi bien entendu, $p_1 \cdots p_k \leq n$; il divise donc $n - p_1 \cdots p_k = 1$, d'où une contradiction. ∎

Exercice 68. (*) Notons $p_1, \ldots, p_k, \ldots$ les nombres premiers rangés par ordre croissant. Démontrer que $p_{k+1} \leq p_1 \cdots p_k + 1$. En déduire par récurrence que $p_k \leq 2^{2^k - 1}$.

Rappelons que $a, b \in \mathbb{Z}$ sont dits premiers entre eux si leurs seuls diviseurs communs sont $+1$ et -1 ; et que cette relation équivaut à l'existence de $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$ (relation de Bézout).

Proposition 6 (Lemme de Gauss)**.** *Soient $a, b, c \in \mathbb{Z}$. Si a divise bc et si a et b sont premiers entre eux, alors a divise c.*

Démonstration. — L'hypothèse que a divise bc s'écrit $bc = ax$, avec $x \in \mathbb{Z}$. L'hypothèse que a et b sont premiers entre eux s'écrit $ua + vb = 1$ avec $u, v \in \mathbb{Z}$. On a alors :

$$c = (ua + vb)c = uac + vbc = uac + vax = ay,$$

avec $y := uc + vx \in \mathbb{Z}$, de sorte que a divise c. ∎

Lemme 3.5.4. *Soient p un nombre premier et n un entier. Alors ou bien p divise n, ou bien p et n sont premiers entre eux.*

Démonstration. — Les seuls diviseurs de p sont ± 1 et $\pm p$. Si p et n ne sont pas premiers entre eux, ils admettent d'autres diviseurs communs que $+1$ et -1, donc p ou $-p$ divise n, donc, dans tous les cas, p divise n. ∎

Proposition 7 (Lemme d'Euclide)**.** *Soient p un nombre premier et $b, c \in \mathbb{Z}$. Si p divise bc, alors p divise b ou p divise c. Plus généralement, si p divise un produit $b_1 \cdots b_k$, alors il divise l'un des b_i.*

Démonstration. — La première assertion vient immédiatement en combinant le lemme ci-dessus avec le lemme de Gauss. La deuxième se prouve par application réitérée de la première. ∎

Voici quelques conséquences immédiates.

Corollaire 3.5.5. *Les diviseurs premiers de $n!$ sont les nombres premiers $\leq n$.*

Démonstration. — Tout diviseur premier de $n! = \prod_{k=1}^{n} k$ est diviseur de l'un des $k \in \{1, \ldots, n\}$ donc est $\leq n$. Réciproquement, tout nombre premier $\leq n$ figure parmi les $k \in \{1, \ldots, n\}$, donc divise $n!$. ∎

Corollaire 3.5.6. *Soient p un nombre premier et k un entier tel que $1 \leq k \leq p-1$. Alors p divise $C_p^k = \binom{p}{k}$.*

Démonstration. — Soient $x := \binom{p}{k} \in \mathbb{Z}$. Rappelons que $p! = k!(n-k)!x$.

Or, p ne divise ni $k!$ ni $(p-k)!$ (d'après le corollaire précédent) ni donc leur produit $y := k!\,(p-k)!$ (d'après le lemme d'Euclide). Comme p divise $p! = xy$, il divise donc x (toujours d'après le lemme d'Euclide). ∎

Théorème 3.5.7 (Théorème fondamental de l'arithmétique)**.** *Tout entier naturel $n \geq 2$ peut s'écrire comme un produit de nombres premiers, et cette factorisation est unique à l'ordre près.*

Démonstration. — L'existence d'une telle factorisation a déjà été mentionnée au paragraphe 3.4, page 46, et démontrée dans le chapitre dénombrement (Exemple 2.1.1, page 20). L'unicité se prouve ainsi. Supposons que l'on ait :

$$n = p_1 \ldots p_r = q_1 \ldots q_s,$$

où les p_i et les q_j sont premiers. Alors, par application du lemme d'Euclide, on voit que p_r divise l'un des q_j ; ce dernier étant premier, on a donc $p_r = q_j$. Quitte à modifier la numérotation, on peut supposer que $j = s$. Le facteur premier $p := p_r = q_s$ est donc présent dans les deux factorisations, et l'on en déduit en le simplifiant les deux factorisations $p_1 \ldots p_{r-1} = q_1 \ldots q_{s-1}$ de n/p_1. On peut alors renouveler l'argument. ∎

Tout entier est donc produit de ses *facteurs premiers*, éventuellement comptés plusieurs fois (autrement dit, munis d'exposants). On conviendra de faire figurer *tous les nombres premiers* dans une telle factorisation (ou *décomposition*), tout simplement en affectant d'un exposant nul ceux qui ne divisent pas l'entier concerné ! Notant $p_1, p_2, \ldots$ la suite de tous les nombres premiers, rangés par ordre croissant, on voit donc que tout entier naturel non nul s'écrit de manière unique :

$$n = \prod_{i \geq 1} p_i^{e_i},$$

les entiers e_i étant presque tous nuls.

Cette notation est un peu formelle (qu'est ce que ça veut dire qu'un produit infini ?) Mais il faut remarquer que multiplier par $p^0 = 1$ ne fait rien. Dans l'écriture qui précède, il n'y a qu'un nombre fini de e_i qui sont non nuls : ce sont ceux qui correspondent à des nombres premiers qui apparaissent effectivement dans la décomposition de n en facteurs premiers. Donc en fait, ce "produit infini" n'est qu'en fait que le produit d'un nombre fini de termes.

Alors, pourquoi s'embêter avec cette écriture ? C'est pour une raison bien simple : cela nous évite d'écrire explicitement pour un nombre donné la liste des nombres premiers qui apparaissent dans sa décomposition en facteurs premiers, et d'ainsi écrire par exemple la formule

$$\left\{ a = \prod_{i \geq 1} p_i^{e_i},\ b = \prod_{i \geq 1} p_i^{f_i} \right\} \Longrightarrow ab = \prod_{i \geq 1} p_i^{e_i + f_i}.$$

On en déduit facilement les règles suivantes :

$$\big(a|b \iff \forall i \geq 1\ ,\ e_i \leq f_i\big),\ \text{et}\ \operatorname{pgcd}(a,b) = \prod_{i \geq 1} p_i^{\min(e_i, f_i)}.$$

3.6 Congruences

La notion de congruence est un outil très efficace pour calculer des restes dans des divisions euclidiennes. Nous en verrons de nombreux exemples.

Définition 3.6.1. *Soient $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$. On dit que a* est congru à b modulo n *si n divise $a - b$. On écrit alors $a \equiv b \pmod{n}$.*

Proposition 8.

(1) La relation de congruence est une relation d'équivalence. Plus précisément :

(a) (réflexivité) $\forall a \in \mathbb{Z}\ ,\ a \equiv a \pmod{n}$,

(b) (symétrie) $\forall a, b \in \mathbb{Z}\ ,\ \Big\{a \equiv b \pmod{n}\Big\} \Longrightarrow \Big\{b \equiv a \pmod{n}\Big\}$,

(c) (transitivité) $\forall a, b, c \in \mathbb{Z}\ ,\ \Big\{a \equiv b \pmod{n} \text{ et } b \equiv c \pmod{n}\Big\} \Longrightarrow \Big\{a \equiv c \pmod{n}\Big\}$.

(2) Cette relation d'équivalence est compatible avec l'addition et la multiplication. Plus précisément :

(a) $\forall a, b, a', b' \in \mathbb{Z}\ ,\ \Big\{a \equiv a' \pmod{n} \text{ et } b \equiv b' \pmod{n}\Big\} \Longrightarrow \Big\{a + a' \equiv b + b' \pmod{n}\Big\}$,

(b) $\forall a, b, a', b' \in \mathbb{Z}\ ,\ \Big\{a \equiv a' \pmod{n} \text{ et } b \equiv b' \pmod{n}\Big\} \Longrightarrow \Big\{aa' \equiv bb' \pmod{n}\Big\}$.

Démonstration. — Toutes ces propriétés sont très faciles à démontrer. Nous ne démontrons à titre d'exemple que les points (1c) (2a), les autres sont laissés au lecteur (lectrice) à titre l'exercice.

Commençons donc par le point (1c). Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a - b = kn$ et $b - c = k'n$, pour deux entiers relatifs k et k'. Donc, en sommant, $a - c = (k + k')n$, et par conséquent $a \equiv c \pmod{n}$.

Passons au point (2a). Supposons donc que $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$. Alors, $a - a' = kn$ et $b - b' = k'n$. Sommons à nouveau. Nous avons $(a + b) - (a' + b') = (k + k')n$, et donc $a + a' \equiv a + b' \pmod{n}$. ∎

Application : critères de divisibilité par $b \pm 1$

Nous avons tous appris que pour qu'un nombre soit divisible par 9, il faut et il suffit que la somme de ses chiffres le soit. Ce n'est pas une propriété spécifique à la base 10. Soit $b \geq 2$ un entier. De la proposition 8, on déduit les congruences :

$$\begin{aligned} b \equiv 1 \pmod{b-1} &\Longrightarrow \forall k \in \mathbb{N}\ ,\quad b^k \equiv 1 \pmod{b-1}, \\ b \equiv -1 \pmod{b+1} &\Longrightarrow \forall k \in \mathbb{N}\ ,\quad b^k \equiv (-1)^k \pmod{b+1}. \end{aligned}$$

Soit maintenant x un entier naturel écrit en base b :

$$x = (c_k c_{k-1} \cdots c_1 c_0)_b = \sum_{i=0}^{k} c_i b^i.$$

Toujours de la proposition 8, on déduit les congruences :

$$x \equiv \sum_{i=0}^{k} c_i \pmod{b-1} \qquad \text{et} \qquad x \equiv \sum_{i=0}^{k} (-1)^i c_i \pmod{b+1}.$$

En particulier :

– Pour que l'entier x soit divisible par $b-1$, il faut et il suffit, que la somme $c_0 + \cdots + c_k$ de ses chiffres soit divisible par $b-1$.
– Pour que l'entier x soit divisible par $b+1$, il faut et il suffit, que la somme "alternée" $c_0 - c_1 + c_2 + \cdots + (-1)^k c_k$ de ses chiffres soit divisible par $b+1$.

En base 10, on reconnait les critères classiques de divisibilité par 9 et par 11.

La congruence module n est une relation déquivalence sur $\mathbb{Z}$. Comme nous l'avons vu au premier chapitre, elle induit une **partition** de $\mathbb{Z}$ en **classes d'équivalences**. Tout entier relatif est dans l'une de ces classes et dans une seule. Ces classes s'appellent les *classes de congruence modulo n*. La proposition suivante montre qu'il y a exactement n classes.

Proposition 9. *Soient a un entier relatif quelconque et n un entier naturel non nul. Il existe alors un unique "représentant" $r \in \{0, \ldots, n-1\}$ tel que $a \equiv r \pmod{n}$.*

Démonstration. — Écrivons $a = qn + r$ (division euclidienne de a par n), de sorte que $a \equiv r \pmod{n}$ et que $r \in \{0, \ldots, n-1\}$: cela prouve l'existence du représentant r de la "classe de congruence" de a.
Pour établir l'unicité de ce représentant dans $\{0, \ldots, n-1\}$, on suppose que l'on a trouvé $r, r' \in \{0, \ldots, n-1\}$ tels que $a \equiv r \pmod{n}$ et $a \equiv r' \pmod{n}$. Puisque la relation de congruence est symétrique et transitive, on a $r \equiv r' \pmod{n}$. Comme $|r - r'| < n$, cela implique que $r = r'$. ∎

Cette proposition permet de démontrer beaucoup de propriétés générales des entiers relatifs par examen d'un nombre fini de cas. Voici trois exemples :

(i) Pour tout $a \in \mathbb{Z}$, l'entier $a^3 - a$ est divisible par 6. Pour le voir, on raisonne ainsi : si $a \equiv r \pmod{6}$, alors $a^3 - a \equiv r^3 - r \pmod{6}$ (cela vient du fait que l'on a une relation d'équivalence compatible avec l'addition et la multiplication). Il suffit donc de vérifier que $r^3 - r \pmod{6}$ lorsque $r \in \{0, \ldots, 5\}$: on laisse au lecteur (lectrice) le plaisir de contrôler ces six cas.

(ii) Tout carré est congru modulo 4 à 0 ou 1 (il suffit de le vérifier pour les carrés de $0, 1, 2, 3$). Donc la somme de deux carrés est congrue modulo 4 à 0, 1 ou 2. Ainsi l'égalité $a^2 + b^2 = 4n + 3$ est impossible en nombres entiers.

(iii) De même, tout carré est congru modulo 8 à 0, 1 ou 4. Il suffit de le vérifier pour les carrés de $0, 1, \ldots, 7$. On en déduit que l'égalité $a^2 + b^2 + c^2 = 8n + 7$ est impossible en nombres entiers.

Pour trouver des divisibilités avec des très grands divisieurs, on peut avoir intérêt à décomposer ce diviseur en nombres premiers, ou en facteurs premiers entre eux. En effet, d'après le lemme de Gauss 6, on a

Proposition 10. *Si $x \equiv y \pmod{a}$ et $x \equiv y \pmod{b}$,* **et si a et b sont premiers entre eux**, *alors $x \equiv y \pmod{ab}$.*

Démonstration. — Exercice ! ∎

Le résultat qui suit permet de simplifier les calculs de congruences des puissances.

Théorème 3.6.2 (Petit théorème de Fermat)**.** *Soient p un nombre premier et a un entier. Alors, $a^p \equiv a \pmod{p}$.*

Démonstration. — Posons $f(a) = a^p - a$. On a donc :

$$f(a+1) - f(a) = \big((a+1)^p - (a+1)\big) - (a^p - a) = (a+1)^p - a - 1 = \sum_{k=1}^{p-1} \binom{p}{k} a^k,$$

qui est un multiple de p, en vertu du corollaire 3.5.6. On en déduit la congruence :

$$\forall a \in \mathbb{Z}\ ,\ f(a+1) \equiv f(a) \pmod{p}.$$

Comme $f(0) = 0$, la propriété est alors immédiate pour $a \in \mathbb{N}$, par récurrence sur a ; puis, pour $-a \in \mathbb{N}$, par récurrence sur $-a$. ∎

Exercice 69. Nous avons établi dans le premier exemple après la proposition 9 que pour tout $a \in \mathbb{Z}$, $a^3 \equiv a \pmod 6$. Redémontrez-le
(i) en utilisant que le produit de trois entiers consécutifs est divisible par 2 et par 3, donc par 6.
(ii) en le déduisant du fait que lorsque $a \in \mathbb{N}$, $\binom{a}{3}$ est entier. Comment passer au cas $a \in \mathbb{Z}$?

3.7 Equations diophantiennes

Du nom du mathématicien grec Diophante d'Alexandrie (env. 200/214 - env. 284/298), il s'agit d'équations dont on cherche les solutions en nombres entiers. Il n'y a pas de méthode générale pour les résoudre. La plupart du temps, on exploite des propriétés de divisibilité pour simplifier le problème. On essaie souvent de majorer la valeur absolue des solutions, dans l'espoir de n'avoir qu'un nombre fini de cas à explorer. Nous allons donner deux exemples de telles équations, parmi les plus célèbres, mais nous en traiterons d'autres en exercice.

3.7.1 Equation de Bézout

Etant donnés des entiers relatifs a, b, c, on s'intéresse aux solutions $(x, y) \in \mathbb{Z}^2$ de l'équation

$$ax + by = c.$$

Ceci revient à chercher les points à coordonnées entières de la droite d'équation $ax + by = c$.

Nous allons supposer que a et b ne sont pas nuls, sinon l'équation est très simple. Soit $d := \text{pgcd}(a, b)$. Si notre équation admet une solution $(x, y) \in \mathbb{Z}^2$ alors comme d divise a et b, d divise aussi $c = ax + by$. Par conséquent, si c n'est pas un multiple de d, l'équation n'admet pas de solutions entières.

Suppossons maintenant que $d|c$ et introduisons les entiers relatifs $a' := a/d$, $b' := b/d$ et $c' := c/d$. L'équation est donc équivalente à

$$a'x + b'y = c'.$$

De plus a' et b' sont maintenant premiers entre eux. Par le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $a'u + b'v = 1$ (on peut les obtenir par l'algorithme d'Euclide étendu). On en déduit que $(x_0, y_0) := (c'u, c'v) \in \mathbb{Z}^2$ est une solution de l'équation.

L'équation peut donc s'écrire $a'x + b'y = a'x_0 + b'y_0$, ce qui est équivalent à

$$a'(x - x_0) = b'(y_0 - y).$$

Nous allons travailler par condition nécessaire : supposons que x, y sont des solutions entières. Alors comme a' divise $b'(y_0 - y)$ et que a' est premier avec b', le lemme de Gauss nous assure que a' divise $y - y_0$. Il existe donc un entier relatif h tel que $y - y_0 = ha'$. Par le même raisonnement, on obtient que b' divise $x - x_0$ et qu'il existe $k \in \mathbb{Z}$ tel que $x - x_0 = kb'$. Léquation $a'(x - x_0) = b'(y_0 - y)$ devient donc $ka'b' = -ha'b'$ dont on déduit (puisque a, b et donc a', b' ne sont pas nuls) que $k = -h$. On obtient donc qu'une solution est forcément de la forme $(x_0 + kb', y_0 - ka')$ pour un $k \in \mathbb{Z}$.

Réciproquement tout couple de cette forme est solution puisque

$$a'(x_0 + kb') + b'(y_0 - ka') = a'x_0 + ka'b' + b'y_0 - ka'b' = a'x_0 + b'y_0 = c'.$$

En conclusion l'ensemble des solutions de notre équation diophantienne est

$$\Big\{ (x_0 + kb', y_0 - ka');\ k \in \mathbb{Z} \Big\}.$$

Exercice 70. Trouver toutes les solutions dans $\mathbb{Z}$ de l'équation $3x - 2y = 1$.

3.7.2 Un théorème grec en rapport avec le théorème de Pythagore

Voici un problème *antique* : quels triangles rectangles ont trois côtés entiers (on appelle de tels triangles des triangles pythagoriciens) ? D'après le théorème de Pythagore, on est ramené résoudre l'équation "diophantienne" :

$$a^2 + b^2 = c^2, a, b, c \in \mathbb{N}. \tag{3.3}$$

Il y a bien entendu les solutions "triviales", telles que $a = 0$ et $b = c$, ou $b = 0$ et $a = c$. Les premiers exemples non triviaux sont bien connus : $3^2 + 4^2 = 5^2$ et $12^2 + 5^2 = 13^2$. La solution $(3, 4, 5)$ est utilisée depuis très longtemps par la "corde à 13 noeuds", qui permettait de vérifier qu'un angle est droit.

On vérifie que, si $(a, b, c) \in \mathbb{N}^3$ est solution de (3.3), alors, pour tout $d \in \mathbb{N}$, le triplet (da, db, dc) est également solution de (3.3). Pour aller plus loin, nous aurons besoin d'un lemme.

Lemme 3.7.1.

(i) Si $x, y \in \mathbb{N}$ sont tels que x^2 divise y^2, alors x divise y.

(ii) Si $x, y \in \mathbb{N}$ ont pour pgcd d et sont tels que le produit xy est un carré (d'entier naturel), alors $x = du^2$ et $y = dv^2$, où $u, v \in \mathbb{N}$.

Démonstration. —
(i) On écrit les décompositions en facteurs premiers $x = \prod_{i \geq 1} p_i^{e_i}$ et $y = \prod_{i \geq 1} p_i^{f_i}$, et l'on remarque que, si x^2 divise y^2, alors pour tout i $2e_i \leq 2f_i$, dont on déduite que $e_i \leq f_i$, ce qui veut dire que x divise y.
(ii) Commençons par le cas où $d = 1$, *i.e.* x, y sont premiers entre eux. On écrit les décompositions en facteurs premiers $x = \prod_{i \geq 1} p_i^{e_i}$ et $y = \prod_{i \geq 1} p_i^{f_i}$. Dire que x, y sont premiers entre eux revient à dire que, pour tout i, l'un au moins des exposants e_i ou f_i est nul. Dire que xy est un carré revient à dire que, pour tout i, l'exposant $e_i + f_i$ est pair. Il en découle que tous les e_i et tous les f_i sont pairs, donc que x et y sont des carrés. Dans le cas général, on pose $x = dx'$ et $y = dy'$. Puisque $d^2x'y'$ est un carré, on déduit facilement de l'assertion (i) que $x'y'$ est un carré, et l'on est ramené au premier cas. ∎

Proposition 11. *Toute solution de (3.3) est de la forme (da, db, dc), où $(a, b, c) \in \mathbb{N}^3$ est solution de (3.3) et où a, b, c sont premiers entre eux deux à deux.*

Démonstration. — Soit $(a', b', c') \in \mathbb{N}^3$ une solution de (3.3) et soit d le pgcd de a' et b'. On a donc $a' = da$ et $b' = db$, où les entiers a et b sont premiers entre eux. On a alors $c'^2 = d^2(a^2 + b^2)$, et, d'après l'assertion (i) du lemme ci-dessus, d divise c'. On écrit $c' = dc$ et l'on a évidemment $a^2 + b^2 = c^2$ et $(a', b', c') = (da, db, dc)$.

Reste à voir que a, b, c sont premiers entre eux deux à deux. C'est vrai par construction pour a et b. On va le prouver pour b et c (le cas de a et c est similaire). S'ils n'étaient pas premiers entre eux, ils admettraient un facteur premier commun p, lequel diviserait b^2 et c^2, donc $a^2 = c^2 - b^2$, donc a (lemme d'Euclide), contredisant le fait que a et b sont premiers entre eux. ∎

Une solution $(a, b, c) \in \mathbb{N}^3$ de (3.3) telle que a, b, c sont premiers entre eux deux à deux sera dite *primitive*. Il suffit de les déterminer toutes ; le résultat suivant apparaît déjà dans les *Éléments d'Euclide*.

Théorème 3.7.2. *Toute solution primitive de (3.3) est (quitte à permuter a et b) de la forme* $(2uv, u^2 - v^2, u^2 + v^2)$*, où* $u, v \in \mathbb{N}$ *sont premiers entre eux et* $v \leq u$*.*

Démonstration. — Seul au plus l'un des entiers a, b, c est pair (sinon, la solution ne serait pas primitive). Si a et b étaient impairs, on aurait $a^2, b^2 \equiv 1 \pmod 4$, donc $c^2 = a^2 + b^2 \equiv 2 \pmod 4$, et c'est impossible car un carré est toujours congru à 0 ou 1 modula 4. Ainsi, c est impair ainsi que l'un des entiers a ou b. Disons que c'est b qui est impair. Alors a est pair.
On tire de (3.3) l'égalité $a^2 = (c - b)(c + b)$, dans laquelle $c - b$ et $c + b$ sont naturels et sont pairs.
Montrons que leur pgcd est 2. Ils sont pairs, et, si p est un nombre premier qui les divise tous les deux, il divise leur somme $2c$ et leur différence $2b$ dont le pgcd est 2 (puisque b et c sont premiers entre eux). Le seul nombre premier qui les divise tous les deux est donc $p = 2$. Leur pgcd est donc une puissance de 2. Maintenant, 4 n'est pas un diviseur commun, puisque sinon, 4 diviserait $2b$ et $2c$, donc 2 serait un diviseur commun à b et c. Donc, le pgcd de $b - c$ et $b + c$ est bien 2.
D'après l'assertion (ii) du lemme ci-dessus, $c + b = 2u^2$ et $c - b = 2v^2$, où $u, v \in \mathbb{N}$. La fin de la démonstration est alors facile ... et laissée au lecteur ! ∎

Exercice 71. Vérifier que, si $u, v \in \mathbb{N}$ et $v \leq u$, alors $(2uv, u^2 - v^2, u^2 + v^2)$ est bien solution de (3.3). À quelle condition cette solution est-elle primitive ?

Remarque 2. *La solution du problème des triangles pythagoriciens date de très longtemps. On trouve sur une tablette égyptienne du XVIII*$^{\text{ème}}$ *siècle avant J.-C. un tableau de tels triplets sur 15 lignes et 4 colonnes. La solution générale du problème remonte sans doute à Euclide (environ* -365 *—*-225*). On s'est très vite posé la question de généraliser ce problème à d'autres puissances : résoudre en nombres entiers l'équation* $n^p + m^p = q^p$*, pour* $p \geq 3$*. En 1641, Pierre de Fermat a annoncé qu'il avait montré que ce problème n'avait pas de solutions non nulles. Il n'en donne pas de preuve, mais il est à peu près certain qu'il a réussi à le démontrer pour* $p = 4$*, par exemple. Il a fallu attendre 353 années pour que le mathématicien anglais Andrew Wiles le démontre entièrement en 1996. La démonstration fait appel à des outils mathématiques très sophistiqués qui dépassent de loin le cadre de l'arithmétique.*

Remarque 3. *On peut se poser le même problème que celui des rectangles pythagoriciens en dimension 3. On cherche alors un paralépipède rectangle (une brique) tel que les côtés soient entiers, les diagonales des faces soient entières, et la "grande diagonale" de la brique soit entière. En terme mathématiques, cela revient à trouver des (les) triplets d'entiers non nuls* (a, b, c) *tels que*

$$a^2 + b^2 = d^2,\ b^2 + c^2 = e^2,\ c^2 + a^2 = f^2,\ a^2 + b^2 + c^2 = g^2,$$

où d, e, f, g *sont des entiers. Ce problème s'appelle le problème de la brique d'Euler.*

A l'heure actuelle, on ne connaît aucune solution à ces équations, mais on ne sait pas non plus montrer qu'il n'y en a pas.

3.8 Compléments

3.8.1 Groupes, anneaux, corps

Nous avons déjà vu plusieurs fois au long de ce cours des mots comme "groupe", "anneau" ou "corps". Elles concernent des ensembles sur lesquels on a des opérations qu'on appelle *loi de composition*, c'est à dire une application de $E \times E \to E$ qui à deux éléments a et b associe un nouvel élément $a * b$. Nous en avons vu de nombreux exemples, comme l'addition et la multiplication sur $\mathbb{N}$ ou $\mathbb{Z}$, ou bien encore l'intersection ou l'union sur $\mathcal{P}(E)$.

Les lois de composition apparaissent dans différents domaines des mathématiques. Elles permettent de manipuler les objets de ces ensembles plus ou moins comme des nombres. Nous présentons maintenant quelques propriétés courantes que ces lois peuvent posséder. On dit qu'une loi de composition

(1) est *associative* si l'on a toujours $(a * b) * c = a * (b * c)$,

(2) est *commutative* si l'on a toujours $a * b = b * a$,

(3) admet un *élément neutre* s'il existe un élément $e \in E$ tel que, pour tout $a \in E$, on a $e * a = a$ et $a * e = a$. Un tel élément neutre est toujours unique, et un élément neutre à droite ($\forall a, a * e = a$) est toujours égal à un élément neutre à gauche ($\forall a, e * a = a$).

(4) Lorsqu'on a un élément neutre e, un *inverse* (ou l'opposé lorsque le groupe est commutatif) de a est un élément b tel que $a * b = b * a = e$. Un tel inverse est unique, et un inverse à droite est toujours égal à un inverse à gauche.

On dit que l'ensemble E muni d'une loi de composition $* : (E, *)$ est

(i) un *groupe* lorsqu'il est muni d'une loi associative, qu'elle a un élément neutre, et que tout élément a un inverse (ainsi, $\mathbb{N}$ n'est pas un groupe pour l'addition, mais $\mathbb{Z}$ en est un). On dit que le groupe est commutatif lorsque la loi $*$ est commutative. Lorsque c'est le cas, on la note très souvent $+$, par abus de langage (bien qu'elle puisse ne rien avoir avec l'addition à laquelle nous sommes habitués, mais c'est pour ne pas introduire trop de symboles exotiques).

(ii) Lorsque qu'on dispose de deux lois de compositions $+$ et $*$, on dit que $(E, +, *)$, est un anneau lorsque

  (a) $+$ est commutative, et $(E, +)$ est un groupe. On note 0 son élément neutre, et $-x$ l'opposé de x.

  (b) La loi $*$ est distributive par rapport à l'addition $+$.

  (c) Lorsque de plus $*$ est commutative, on a un *anneau commutatif*.

  (d) Enfin, on dit que l'anneau est *unitaire* si la loi $*$ admet un élément neutre, qu'on note en général 1.

Dans un anneau, on a toujours $a * 0 = 0$, puisque $a * 0 = a * (0 + 0) = a * 0 + a * 0$ et donc en ajoutant $-a * 0$ aux deux membres, on trouve $a * 0 = 0$.

(iii) On dit que l'anneau est intègre si $a * b = 0 \Longrightarrow (a = 0 \text{ ou } b = 0)$.

(iv) Si on a un anneau unitaire A dans lequel, $\forall a \neq 0, \exists b, ab = 1$ (c'est à dire que $A \setminus 0 := A^*$, muni de la loi $*$ est un groupe), on dit qu'on a un *corps*. Cet anneau est toujours intègre.

3.8.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$

La proposition 9 nous montre qu'il y a exactement n classes de congruence modulo n. Les propriétés énoncées dans la proposition 8 nous autorisent à "additionner" les classes entre elles, et aussi à les multiplier. Pour les additionner une classe x et une classe y, on choisit un "représentant" $a \in x$ (c'est à dire un élément de la classe x), et un représentant $b \in y$. Alors, la classe de $a + b$ ne dépend pas du choix de a et b, (donc elle ne dépend que de x et y). On l'appelle $x + y$. On fait de même pour le produit.

Sur l'ensemble des classes, nous avons alors une addition que nous pouvons noter $+$, une multiplication que nous notons xy comme pour les entiers. Toutes les propriétés de l'addition et de la multiplication des entiers se propagent aux additions et multiplications sur les classes. Ainsi, l'addition est associative, commutative, elle admet un élément neutre (lequel ?), tout élément a un opposé. La multiplication est aussi associative et commutative, elle est distributive par rapport à l'addition, elle admet un élément neutre (lequel ?). Toutes ces propriétés font de l'ensemble des classes un anneau commutatif unitaire, tel qu'ils sont définis ci-dessus. On le note $\mathbb{Z}/n\mathbb{Z}$, et c'est l'exemple le plus simple d'anneau qui ne soit pas celui des nombres entiers relatifs. Si n n'est pas premier, il n'est pas intègre (pourquoi ?). Si n est premier, c'est un corps : sauriez vous le démontrer ?

3.8.3 Programmation des algorithmes

Division Euclidienne

La preuve que nous avons donnée de la division euclidienne n'est pas « constructive », en ce sens qu'elle ne nous donne pas un moyen effectif de trouver les quotient et reste dans une division. Nous présentons maintenant un moyen explicite, donc programmable sur ordinateur, de faire cette division euclidienne. Notons ici $q(a,b)$ et $r(a,b)$ le quotient et le reste de la division de a par b. On vérifie que $(q(a,b), r(a,b))$ vaut $(0,a)$ si $a < b$. Si $a > b$, et $a = qb + r$, alors $a - b = (q-1)b + r$. Ceci se traduit par le fait que, si $a \geq b$, alors $\big(q(a,b), r(a,b)\big) = \big(1 + q(a-b,b), r(a-b,b)\big)$.

On voit alors que l'on peut ramener le calcul de la division de a par b à celui de la division de $a-b$ par b. Il ne reste plus qu'à répéter l'opération. Ceci nous donne un algorithme fonctionnel récursif (en style CAML) :

```
let rec diveucl (a,b) =
if a < b then (0,a)
else let (q1,r1) = diveucl(a-b,b) in (1 + q1,r1);;
```

En style impératif-itératif, on procédera plutôt comme suit. On retranche b à a tant que c'est possible ; le nombre de telles soustractions est le quotient q, la valeur finale de a est le reste r. Pour réaliser cela, on déclare deux variables q et r. La première vaut 0 au départ (initialisation) et augmente de 1 à chaque étape (mises à jour). La deuxième vaut a au départ et diminue de b à chaque étape. Voici l'algorithme :

```
(* Division euclidienne de a par b *)
q := 0; r := a;
tant que r >= b faire (q := q + 1; r := r - b);
rendre(q,r);;
```

Nous allons *démontrer* que cet algorithme est correct. Il faut bien entendu supposer pour cela que les données sont valides, autrement dit que $a, b \in \mathbb{N}$ et que $b \neq 0$.

Tout d'abord, on prouve la *terminaison*, autrement dit, que le processus s'arrête un jour ! Comme presque toutes les preuves de terminaison d'algorithmes ou de programmes, celle-ci repose sur l'argument suivant : il y a un certain entier naturel (parfois appelé "compteur") qui diminue strictement à chaque étape. Comme $\mathbb{N}$ est bien ordonné, il ne peut donc y avoir une infinité d'étapes. Ici, le rôle du compteur est tenu par r. Comme on lui retranche $b \geq 1$ à chaque étape, il diminue en effet strictement.

Nous allons ensuite montrer qu'à la fin de l'exécution de l'algorithme, les valeurs rendues q et r vérifient bien les propriétés qui caractérisent le quotient et le reste. La technique repose sur la notion d'*invariant de boucle*, qui s'apparente au principe de récurrence. Notre invariant de boucle est l'affirmation suivante : *À tout moment de l'exécution de l'algorithme, q et r sont des entiers naturels tels que $a = qb + r$.* (Mais attention, comme on n'a pas $r < b$, ceci ne signifie pas que r est le reste et q le quotient).
Comme pour une démonstration par récurrence, il y a une *initialisation*, qui consiste à vérifier l'invariant de boucle au départ. Ici, l'initialisation des variables q et r est `q := 0; r := a;`, et l'on a bien, au départ :

$$qb + r = 0.b + a = a.$$

Il y a ensuite une vérification d'*hérédité*, qui consiste à prouver que, si l'invariant de boucle est satisfait avant une itération, alors il est satisfait après. On voit bien ici que les "variables" des programmeurs ne sont pas comme les variables des mathématicien, elles changent de valeur au cours du temps ! On va exprimer cela en notant q, r les valeurs contenues dans les variables `q,r` avant une itération (ou boucle), et q', r' les valeurs contenues dans les variables `q,r` après. Par définition des affectations qui constituent la boucle : `(q := q + 1; r := r - b)`, on a les relations $q' = q + 1$ et $r' = r - b$. On a donc : $q'b + r' = (q+1)b + (r-b) = qb + r$. Ainsi :

$$a = qb + r \Longrightarrow a = q'b + r'.$$

Si l'invariant de boucle est vérifié avant, il l'est encore après ; et il l'est au départ. Donc il l'est toujours, donc encore à la fin. Les valeurs q,r rendues sont donc telles que $a = qb + r$, et nous avons *presque* fini ...

Il reste à montrer que l'on a bien (à la fin) $r < b$. Cela repose sur la condition `r >= b` de la *structure de contrôle* `tant que`. Pour que l'itération s'arrête, il faut que cette condition soit fausse (sinon, par définition de cette structure de contrôle, l'itération continuerait). À la fin de l'exécution de l'algorithme, on a donc bien $r < b$.

Exercice 72. Nous n'avons pas prouvé que q,r restaient des entiers naturels. Combler cette lacune.

Écriture en base b

On suppose connus les entiers n et b sous une forme qui permet les calculs nécessaires. Par exemple, ces entiers peuvent être codés en base 10 et les calculs effectués par un humain pour une conversion en base $b = 2$; ou au contraire, ils peuvent être codés en base 2 dans et les calculs effectués par des circuits logiques pour une conversion en base $b = 10$. Dans tous les cas, le calcul fondamental est la division euclidienne par b, que l'on représentera par une fonction auxiliaire `diveucl(a,b)` dont le résultat est le couple `(q,r)` formé du quotient et du reste. Voici une version fonctionnelle récursive :

```
let rec conversion n b = match n with
| 0 -> []
| - -> let (q,r) = diveucl(n,b) in r :: (conversion q b);;
```

Attention ! Cette fonction rend la liste des chiffres à l'envers, *i.e.* avec le chiffre des unités en premier ! On peut la rendre à l'endroit, mais il faut ruser : cherchez ...

Voici une version impérative itérative, qui écrit les chiffres :

```
(* conversion de n en base b *)
a := n;
tant que a > 0 faire ((q,r) := diveucl(a,b); ecrire r; a := q);;
```

Questions : dans quel ordre sortent les chiffres ? Comment justifier cet algorithme ?

Exponentiation rapide

Soient n un entier naturel et a un nombre (entier, réel ou complexe). Le calcul de a^n de manière évidente (par la définition) nécessite $n-1$ multiplication $a^{k+1} = a^k \times a$, $k = 1, \ldots, n-1$. Par « calculer rapidement », nous entendons que le nombre de multiplications utilisées ne doit pas croître linéairement avec n, c'est à dire à une vitesse proportionnelle à n), comme dans l'algorithme évident ci-dessus, mais seulement avec $\log n$ (i.e. la taille de n).

Une méthode d'exponentiation plus rapide, appelée parfois exponentiation chinoise ou indienne ou babylonienne ou dichotomique, est connue depuis fort longtemps. Elle repose sur le principe « diviser pour régner » :

$$a^n := \begin{cases} a^{\frac{n}{2}} \times a^{\frac{n}{2}} & \text{si } n \text{ est pair,} \\ a \times a^{\frac{n-1}{2}} \times a^{\frac{n-1}{2}} & \text{si } n \text{ est impair.} \end{cases}$$

On a ramené le problème (calculer a^n) à deux sous-problèmes (calculer $a^{\frac{n}{2}}$) plus simples, principe qui améliore parfois les performances d'un l'algorithme.

Exemples.
1) $a^{16} = (a^8)^2 = ((a^4)^2)^2 = (((a^2)^2)^2)^2$. On effectue alors 4 multiplications au lieu de 15 : $a^2 = a \times a$, $a^4 = a^2 \times a^2$, $a^8 = a^4 \times a^4$, et $a^{16} = a^8 \times a^8$.
2) $a^{15} = a(a^7)^2 = a(a(a^3)^2)^2 = a(a(aa^2)^2)^2$. On effectue 6 multiplications au lieu de 14 : $a^3 = a \times a \times a$, $a^7 = a \times a^3 \times a^3$, $a^{15} = a \times a^7 \times a^7$.

Avec l'écriture en base 2 de $n = (c_k c_{k-1} \cdots c_0)_2 = c_0 + c_1 \cdot 2 + \cdots + c_k \cdot 2^k$, où $c_i \in \{0, 1\}$, on voit que $a^n = a^{c_0}(a^2)^{c_1}(a^{2^2})^{c_2} \cdots (a^{2^k})^{c_k}$. On a besoin au plus de k multiplications pour calculer tous les a^{2^i} $(1 \leq i \leq k)$, puis k multiplications pour former le produit des $(a^{2^i})^{c_i}$ $(1 \leq i \leq k)$. Le nombre total de multiplications est $2k = 2\lfloor \log_2 n \rfloor = O(\log n)$. Voici un algorithme basé sur cette idée :

```
(* Calcul de a puissance n *)
r := 1; x := a; p := n;
tant que p >0 faire (si p impair alors r := x * r; p := p div 2; x := x * r);
rendre r;;
```

Exercice 73. Vérifier la terminaison, la correction de l'algorithme.

Calcul du PGDC

Forme fonctionnelle récursive :

```
let rec pgcd a b = match b with
| 0 -> a
| - -> let (q,r) = diveucl(n,b) in (pgcd b r);;
```

Forme impérative itérative.

Comme d'habitude, le principe est de déclarer des variables globales qui prendront successivement les valeurs r_i.

```
(* calcul du pgcd de a et b *)
x := a; y := b;
tant que y > 0 faire ((q,r) := diveucl(x,y); x := y; y := r);;
rendre x;;
```

Coefficients de Bézout

Outre les variables `x` et `y` de l'algorithme d'Euclide "simple", nous entretenons quatre nouvelles variables destinées à exprimer les valeurs successives de `x` et `y` en fonction de a et b.

```
(* calcul du pgcd de a et b et des coefficients de Bezout u et v *)
x := a; y := b; u := 1; v := 0; s := 0; t := 1;
tant que y > 0 faire
  ((q,r) := diveucl(x,y);
   x := y;
   y := r
   (u,s) := (s,u - q s);            (* affectations simultanees *)
   (v,t) := (t,v - q t));;
rendre (x,u,v);;
```

Exercice.
Justifier l'algorithme étendu (terminaison, correction). (Utiliser l'invariant de boucle : $x = ua + vb$ et $y = sa + tb$.)

Exercices sur le chapitre 3

Exercice 74. $\{x \in \mathbb{Z}, x^2 \leq 100\}$ est elle majorée, minorée ? Si oui, donnez le cas échéant son plus petit et plus grand élément. Même question pour $\{x \in \mathbb{Z}, x \leq 100\}$.

Exercice 75. Quels sont les "éléments inversibles" de $\mathbb{Z}$, *i.e.* les $a \in \mathbb{Z}$ tels qu'il existe $b \in \mathbb{Z}$ tel que $ab = 1$?

Exercice 76. Est-ce que toute partie non vide de $\mathbb{Z}$ admet un plus petit élément ?

Exercice 77. On suppose que a et b sont premiers entre eux. Montrer que a et $b - a$ sont premiers entre eux.

Exercice 78. (*) Déterminez les couples d'entiers naturels (a, b) tels que $a + b = 1008$ et $\text{pgcd}(a, b) = 24$.

Exercice 79. Montrez que $\max(a, b) = \dfrac{a + b + |a - b|}{2}$·. Donnez une expression similaire pour $\min(a, b)$.

Exercice 80. (*) Pour a, b, c dans $\mathbb{Z}$, montrez que $\text{pgcd}(\text{pgcd}(a, b), c)) = \text{pgcd}(a, \text{pgcd}(b, c))$. (On pourra faire intervenir $D(a) \cap D(b) \cap D(c)$.)

Exercice 81. (*) Montrez que $11^{100} - 1$ est divisible par 1000 (Indication : écrire $11 = 10 + 1$ et utilisez la formule du binôme).

Exercice 82. Quel est le reste de la division de 812231 par 99 ? Par 97 ? (Sans faire la division explicitement, et bien sûr sans utiliser de calculette !)

Exercice 83. Ecrire 13 en base 2, en base 3, et en base 7.

Exercice 84. (*) On écrit les nombres entiers a et c en base b : $a = \sum_{i=1}^{N} a_i b^i$ et $c = \sum_{i=1}^{N} c_i b^i$. On appelle $i_0 = \max\{i,\ a_i < c_i\}$. Montrez que $a < c$ si et seulement si $a_{i_0} < c_{i_0}$.

Exercice 85.

(i) Un nombre s' écrit 6142 en base 7. Est-il pair (i.e. multiple de 2) ?

(ii) Montrez qu'en base 7, un nombre est pair si et seulement si la somme de ses chiffres est paire.

(iii) (*) Donnez un critère général de parité en base b, en distinguant les cas b pair et b impair.

Exercice 86. (**) [Le jeu de Marienbad] Ce jeu se joue à deux joueurs, et se pratique de la façon suivante : on a des allumettes disposées en rangées plus ou moins longues. A chaque étape, tant qu'il reste des allumettes, un joueur doit choisir une rangée, et peut enlever dans cette rangée autant d'allumettes qu'il veut. Le joueur qui prend la dernière allumette a perdu. Dans ce jeu, le joueur qui commence a une stratégie pour gagner à coup sûr, selon la condition initiale. Nous allons la décrire et le démontrer.

Appelons N le nombre de rangées, et a_n le nombre d'allumettes dans la rangée n (et on suppose $n \geq 1$) : on écrit a_n en base 2

$$a_n = \sum_{i=0}^{K} \epsilon_{i,n} 2^i,$$

avec $\epsilon_i = 0$ ou 1. K est un entier tels que tous les a_n soient inférieurs à 2^K. On pose, pour $i = 0 \dots K$

$$A_i = \sum_{n=1}^{N} \epsilon_{i,n}$$

et définit $\eta_i \in \{0, 1\}$ par

$$A_i \equiv \eta_i \pmod 2.$$

La question de savoir si on perd ou gagne revient au fait de savoir si tous les η_i sont nuls ou non.

(i) Supposons que le joueur qui joue enlève $c = \sum_{i=0} c_i 2^i$ allumettes à la rangée n ($c_i \in \{0, 1\}$), et appelons i_0 le plus grand indice i tel que $c_{i_0} \neq 0$. Montrez que, si avant de jouer, $\eta_{i_0} = 0$, alors après le jeu, $\eta_{i_0} = 1$.

(ii) On suppose que les η_i ne sont pas tous nuls. Soit $J = \{i, \eta_i = 1\}$ et $i_0 = \max J$.

(a) Montrez qu'il existe k tel que $\epsilon_{i_0,k} = 1$. Nous fixons ce k dans la suite.

(b) Montrez que si on pose $m_1 = \sum_{i \in J} \epsilon_{i,k} 2^i$ et $m_2 = \sum_{i \in J} (1 - \epsilon_{i,k}) 2^i$, on a

$$m_1 \geq 2^{i_0},\ m_2 \leq 2^{i_0} - 1,\ m_1 \leq n_k.$$

(c) Montrez que si, à la rangée k, on enlève $m_1 - m_2$ allumettes, alors après le jeu, tous les η_i sont nuls (on aura intérêt à écrire le reste $n_k - n_2'$ en base 2, et faire le bilan de changement des η_i pour chaque indice i, en séparant ceux qui sont dans J et les autres).

(iii) Montrez que si, à l'instant initial, tous les η_i sont nuls, alors celui qui joue en premier perd face à un joueur qui sait jouer.

(iv) Montrez que si à l'instant initial, l'un des η_i est non nul, celui qui commence gagne.

Suggestion : entraînez vous à jouer à ce jeu (sans papier) avec vos amis.

Exercice 87.

(i) Quels sont les entiers naturels qui divisent 0 ? 1 ? 2 ?

(ii) Quels sont les entiers relatifs que divisent 0 ? 1 ? 2 ?

(iii) Quels sont les diviseurs de 15, de 100 ?

Exercice 88. Montrer que la relation "a divise b" sur $\mathbb{N}$ est une relation d'ordre (non total).

Exercice 89. Calculer $\text{pgcd}(9000, 1575)$ et $\text{pgcd}(1480, 324)$.

Exercice 90. (*) Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0, 0)\}$.
1) Soit $d = \text{pgcd}(a, b)$. Montrer que $\text{pgcd}(\frac{a}{d}, \frac{b}{d}) = 1$.
2) Montrer que pour tout entier $n \geq 1$, on a $\text{pgcd}(na, nb) = n \,\text{pgcd}(a, b)$.

Exercice 91. (*) Soit $r \in \mathbb{Q}_+$. Montrer qu'il existe un unique couple $(u, v) \in \mathbb{N} \times \mathbb{N}^*$ tel que $r = \frac{u}{v}$ et $\text{pgcd}(u, v) = 1$ ("forme réduite" ou "irréductible" du rationnel r).

Exercice 92. (**) On considère n nombres entiers $a_1, \dots, a_n$, et les sommes $s_1 = a_1$, $s_2 = a_1 + a_2, \dots, s_n = a_1 + \dots a_n$.

(1) Montrez que, si aucun des s_i n'est congru à 0 modulo n, alors il y en a deux qui sont congrus entre eux.

(2) En déduire dans une liste de n entiers rangés dans n'importe quel ordre, on peut en trouver k consécutifs dont la somme est multiple de n.

Exercice 93. En utilisant la formule (3.1) page 43, donnez le résultat de la division euclidienne de b^n par $b-1$. Et celui de de 10^{100} par 9.

Exercice 94. (*) Montrez que l'équation en nombre entiers $y^2 = x(x+1)$ n'a pas de solutions autres que $x = y = 0$.

En déduire que l'équation $x^2 = y^2+1$ n'a pas d'autres solutions que $x = 1, y = 0$. (Indication : on pourra raisonner sur la parité de x et y et se ramener au cas précédent).

Exercice 95. (*) On a vu dans l'exercice 94 , pour x entier non nul, $x(x+1)$ n'est jamais un carré.

Montrez que si x est un entier non nul, $x(x+1)(x+2)$ n'est jamais un carré. (Indication : considérez les facteurs premiers de $x, x+1$ ou $x+2$ en distinguant les facteurs premiers supérieurs à 3 du facteur 2).

Même question pour $x(x+1)(x+2)(x+3)$.

Exercice 96. En notant $a = \prod_i p_i^{e_i}$ et $b = \prod_i p_i^{f_i}$, où p_i est la liste des nombres premiers, en appelant $\text{ppcm}(a,b)$ le plus petit multiple commun à a et b,

(i) montrer que $\text{pgcd}(a,b) = \prod_{i\geq 1} p_i^{\max(e_i,f_i)}$;

(ii) donnez une formule analogue pour $\text{ppcm}(a,b)$;

(iii) montrez que les multiples communs à a et b sont les multiples de $\text{ppcm}(a,b)$;

(iv) démontrez que $\text{ppcm}(a,b)\text{pgcd}(a,b) = ab$.

Exercice 97.

(i) Énumérer les facteurs premiers de 15!. Pour chacun d'entre eux, préciser son exposant dans la décomposition de 15! en produits de facteurs premiers.

(ii) Écrire la décomposition de 15! en produits de facteurs premiers.

(iii) Déterminer le nombre de diviseurs de 15!.

Exercice 98.

(1) Soit p un nombre premier, montrez que si $x^2 \equiv 1 \pmod p$, alors $x \equiv \pm 1 \pmod p$. Est-ce vrai pour $p = 8$?

(2) (*) Soit p un nombre premier et n non divisible par p. Montrez qu'il existe un unique entier $m \in \{1, \ldots, p-1\}$ tel que $mn \equiv 1 \pmod p$. On pourra commencer par montrer l'existence d'un entier (pas forcément inférieur à $p-1$) vérifiant $mn \equiv 1 \pmod p$ en utilisant la propriété de Bézout, puis utiliser les propriétés de la congruence modulo p.

(3) (**) En se servant des deux questions précédentes, montrez que, si p est premier $(p-1)! \equiv -1 \pmod p$.

(4) (*) Montrez que si $(p-1)! \equiv -1 \pmod p$, alors p est premier. (Indication : utilisez l'identité de Bézout !)

Exercice 99. Soient $a, b, c \in \mathbb{Z}$. Démontrer l'équivalence :

$$(\exists x, y \in \mathbb{Z} \ : \ ax + by = c) \iff \text{pgcd}(a,b) | c.$$

Exercice 100. (*)

(i) En utilisant la formule (3.1) page 43, montrez que, si $b \mid a$, alors $x^b - 1 \mid x^a - 1$.

(ii) On suppose que $a = bq + r$. Montrez que, pour tout $x \in \mathbb{N}$, le reste de la division de $x^a - 1$ par $x^b - 1$ est $x^r - 1$.

(iii) (*) En utilisant l'algorithme d'Euclide à la fois sur le couple (a, b) et $(x^a - 1, x^b - 1)$, montrez que le pgcd de $x^a - 1$ et $x^b - 1$ est $x^{\mathrm{pgcd}(a,b)} - 1$.

Exercice 101. (*) Soient a et b dans $\mathbb{N}$ tels que $\mathrm{pgcd}(a, b) = 1$. Démontrer que $\mathrm{pgcd}(a+b, ab) = 1$ (Indication : utilisez la propriété de Bézout).

Exercice 102.

(i) Montrez que, si p est premier, $a^{p^2} \equiv a \pmod{p}$.

(ii) Montrez que si p est premier, $a^{pq+r} \equiv a^{q+r} \pmod{p}$.

(iii) Montrez que si p est premier et que n s'écrit $c_k \dots c_0$ en base p, alors $a^n \equiv a^{c_k + \dots + c_0} \pmod{p}$.

Exercice 103. Quel est le reste de la division de 5^{22} par 3 ?

Exercice 104. (**) Décomposer 561 en facteurs premiers. Démontrer, pour tout $a \in \mathbb{Z}$, la congruence : $a^{561} \equiv a \pmod{561}$. Indication : on pourra utiliser le théorème de Fermat avec les facteurs premiers de 561, la méthode décrite dans l'exercice 102 ainsi que la proposition 10.

Exercice 105. (***) Trouvez un autre entier non premier pour lequel la propriété de 561 décrite dans l'exercice 104 est encore vraie.

Exercice 106. (*) Pour $n \in \mathbb{N}$ on définit $a_n := 11n + 6$ et $b_n := 3n + 4$.

1. Calculer le reste de la division euclidienne de a_1 par b_1, puis de a_2 par b_2.
2. Pour $n \geq 3$, calculer $a_n - 3b_n$ et déterminer le reste de la division euclidienne de a_n par b_n.
3. Pour quelles valeurs de n le nombre b_n divise-t-il a_n ?

Exercice 107. (*)

1. Résoudre dans $\mathbb{Z}^2$ l'équation $(x - 3)(y - 2) = 6$.
2. Résoudre dans $\mathbb{Z}^2$ l'équation $xy = 2x + 3y$.

Exercice 108. (*) Résoudre les équations suivantes dans $\mathbb{Z}^2$:

1. $28x + 76y = 20$,
2. $323x - 391y = 612$.

Exercice 109. (**) Soient a, b, c des entiers naturels non nuls tels que a et b sont premiers entre eux et $c > ab$. Montrer qu'il existe au moins un couple $(x, y) \in \mathbb{N}^2$ tel que $ax + by = c$.

Exercice 110. (*) Soit $k \in \mathbb{N}$ et $a_0, a_1, \dots, a_k$ des entiers relatifs. Montrer que si un nombre rationnel x satisfait l'équation

$$x^{k+1} + \sum_{j=0}^{k} a_j x^j = 0$$

alors $x \in \mathbb{Z}$. Indication : écrire $x = p/q$ avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ et p, q premiers entre eux.

Exercice 111. (*) Soit $n \in \mathbb{N}$. Montrer que l'équation $x^2 = n$ n'admet de solution rationnelle que si n est le carré d'un entier.

Exercice 112. (*) Montrer que l'équation $x^6 - 7x + 1 = 0$ n'admet pas de solution rationnelle.

Exercice 113. (*) Montrer que l'équation $x^2 - 5y^2 = 3$ n'a pas de solution dans $\mathbb{Z}^2$. Indication : considérer les congruences modulo un entier bien choisi.