# Introduction à l'arithmétique

Benjamin Schraen

Décembre 2003

## Table des matières

L'objectif de ce petit cours est d'introduire les notions les plus simples de l'arithmétique.

Tout d'abord, posons-nous cette question : quels sont les objets mathématiques les plus simples, les plus universellement connus ? Pour moi il s'agit des entiers 0, 1, 2, etc... On note usuellement $\mathbb{N}$ l'ensemble des entiers, c'est à dire : $\mathbb{N} = \{0,1,2,\dots\}$. Mais ces nombres ne seraient rien sans les opérations que l'on peut faire avec eux, il y en a deux très connues : l'addition et la multiplication.

Tout le monde sait que l'on peut additionner les entiers. Ainsi, si on a un ensemble de 3 objets et un autre de 2 objets, en réunissant ces deux ensembles on obtient un ensemble de $3 + 2 = 5$ objets, c'est l'opération d'addition. On peut également revenir en arrière, c'est la soustraction : si on retire 2 objets à un ensemble comportant au départ 3 objets, il reste $3 - 2 = 1$ objet. Mais attention, pour soustraire un entier quelconque $m$ à un autre entier $n$, il faut une condition qui est que $m$ soit plus petit que $n$ (eh oui, il faut pouvoir retirer suffisament d'objets). C'est pour éviter d'avoir toujours à vérifier ce genre de condition que l'on a décidé de considérer de nouveaux entiers représentant des quantités négatives : $-1$, $-2$, ... On considère donc désormais l'ensemble de tous les entiers munis du signe $+$ ou $-$, on note $\mathbb{Z}$ cet ensemble et on appelle ses éléments les entiers relatifs : $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. Les entiers relatifs positifs sont alors juste appelés entiers naturels (c'est l'ensemble $\mathbb{N}$). L'avantage est maintenant que dans $\mathbb{Z}$, l'addition et la soustraction ne sont plus qu'une même opération : soustraire $m$ à $n$ revient à ajouter $-m$ à $n$.

Passons maintenant à la multiplication. Si l'on possède 4 ensembles de 3 objets chacun, la réunion de ces 4 ensembles contiendra $4 \times 3 = 12$ objets, c'est une opération que tout le monde connaît bien. Arrive maintenant le problème de la division, qui est à la multiplication ce que la soustraction est à l'addition. Si l'on possède 10 objets à répartir en paquets de 5 objets, on obtiendra au final $\frac{10}{5} = 2$ paquets de 5 objets. Néanmoins, il n'est pas toujours possible de séparer $n$ objets en paquets de $m$ objets lorsque $n$ et $m$ sont des entiers naturels quelconques. Pour pouvoir parler du nombre $\frac{n}{m}$ pour toutes les valeurs de $n$ et $m$, on s'est décidé à considérer des nombres "rationnels" ou frations, leur ensemble étant noté $\mathbb{Q}$. Ce point de vue est parfois bien utile mais pas lorsqu'il s'agit de partager des objets indivisibles. Il est acceptable de parler de 5 tiers d'une tarte, mais qui aimerait se retrouver avec des tiers de billets de banque à l'issue d'un partage des plus équitables ? C'est ici tout le problème de l'arithmétique : on ne peut pas diviser un entier par n'importe quel autre, et c'est pourquoi il est nécessaire d'effectuer une étude poussée de la divisibilité. Voici donc une première définition de l'arithmétique : l'arithmétique est l'étude des nombres entiers, c'est-à-dire de l'ensemble $\mathbb{Z}$ muni de ses deux opérations : l'addition $+$ et la multiplication $\times$.

Un exemple de problème pouvant rentrer dans le cadre de l'arithmétique, et qui est probablement connu depuis l'antiquité grecque, est le suivant : quels sont les triangles dont les côtés ont un entier pour longueur ? Rappelons déjà le célèbre théorème de Pythagore :

**Théorème 1** *Si $ABC$ est un triangle rectangle en $A$, on a entre les longueurs de ses côtés, la relation $BC^2 = AB^2 + AC^2$.*

Ainsi on peut considérer le problème plus précis de trouver les triangles rectangles dont les côtés sont de longueur entière, problème qui se ramène à trouver tous les triplets d'entiers $(a,b,c)$ vérifiant la relation $a^2 + b^2 = c^2$. Or on a maintenant un problème purement arithmétique.

À la fin de ce cours, nous serons en mesure de résoudre ce problème. Cependant, l'imagination sans bornes des mathématiciens les a conduits à étendre ce problème : si on se fixe un entier naturel non nul $n$, quels sont les triplets d'entiers $(a,b,c)$ tels que $a^n + b^n = c^n$ ? Il est clair que si $a$ est un entier quelconque le triplet $(a,0,a)$ est une solution. Il y a environ 300 ans, Fermat affirmait avoir trouvé une démonstration "merveilleuse" du fait que pour $n \geq 3$, il n'y avait pas

d'autre solutions que celles-ci. Cependant, on n'a jamais trouvé d'écrit de Fermat démontrant ce fait pour $n$ autre que 3 ou 4. Euler démontra ce résultat dans le cas $n = 5$. Et jusqu'à la fin du $XX^e$ siècle, les mathématiciens du monde entier s'attaquèrent au mystérieux "dernier théorème de Fermat", à l'aide d'outils mathématiques toujours plus abstraits et compliqués. Ce n'est qu'en 1994 que le mathématicien américain Andrew Wiles donna une preuve faisant appel aux outils les plus perfectionnés de l'algèbre et de l'arithmétique actuelle.

# 1 La divisibilité.

Comme nous l'avons vu dans l'introduction, on ne peut pas toujours diviser un entier par un autre, pour obtenir un nombre entier. Voici pourquoi on introduit la notion de divisibilité.

**Définition 1** *Soient $a$ et $b$ deux entiers ($(a,b) \in \mathbb{Z}$). On dit que $b$ divise $a$ s'il existe $k \in \mathbb{Z}$ tel que $a = kb$. On dit aussi que $a$ est divisible par $b$, ou que $a$ est un multiple de $b$, ou encore que $b$ est un diviseur de $a$. On notera alors $b|a$.*

Fixons maintenant $b \in \mathbb{Z}$, on va s'intéresser aux multiples de $b$. Par définition ce sont tous les entiers $nb$ où $n \in \mathbb{Z}$. On note donc $\mathbb{Z}b$ l'ensemble des multiples de $b$ : $\mathbb{Z}b = \{nb, n \in \mathbb{Z}\}$.
Remarquons que si l'on prend $b = 0$, alors pour tout $n \in \mathbb{Z}$, $nb = 0$. Ainsi 0 n'a qu'un seul multiple : lui-même. $\mathbb{Z}0 = \{0\}$.
Si maintenant $b \neq 0$, $b$ a une infinité de multiples. C'est clair car si $n$ et $m$ sont deux entiers différents, $nb \neq mb$.

Nous allons maintenant nous intéresser aux diviseurs d'un entier donné. On fixe un élément de $\mathbb{Z}$ que nous noterons $a$ (pour avoir les mêmes notations que dans la définition). Nous allons noter $\mathcal{D}(a)$ l'ensemble des diviseurs de $a$. Ainsi par définition

$$\mathcal{D}(a) = \{n \in \mathbb{Z}, n|a\} = \{n \in \mathbb{Z}, \exists k \in \mathbb{Z}, kn = a\}$$

Comme précédemment commençons par étudier le cas où $a = 0$. Alors tout entier est diviseur de $a$. En effet si $n \in \mathbb{Z}$, $n0 = 0$. D'où $\mathcal{D}(0) = \mathbb{Z}$.
Nous allons maintenant montrer que si $a \neq 0$, l'ensemble $\mathcal{D}(a)$ est fini et son cardinal est inférieur à $2|a|$.
**Théorème 2** *Soit $a \in \mathbb{Z}$, $a \neq 0$. Alors si $b|a$, $|b| \leq |a|$. Ainsi $\mathcal{D}(a)$ est fini de cardinal inférieur à $2|a|$.*
Preuve : Soit $b$ un diviseur de $a$. Par définition, il existe $k \in \mathbb{Z}$ tel que $a = kb$. Comme $a \neq 0$, on a $k \neq 0$ et $b \neq 0$. Ainsi $|k| \geq 1$ puisque $k$ est entier. En multipliant cette inégalité par $|b|$, on a $|a| = |k||b| \geq |b|$.
Ceci implique que $\mathcal{D}(a)$ est fini puisqu'il n'y a qu'un nombre fini d'entiers $b$ tels que $|b| \leq |a|$. En fait il y en a exactement $2|a| + 1$, mais puisque 0 n'est pas un diviseur de $a$, il y a au plus $2|a|$ diviseurs de $a$.

Exemples : Le théorème nous assure que les diviseurs de 1 sont dans $\{-1,0,1\}$. On peut éliminer 0, et de plus $1 = 1.1 = (-1).(-1)$, ainsi on a $\mathcal{D}(1) = \mathcal{D}(-1) = \{-1,1\}$. En fait 1 et $-1$ sont les seuls entiers ayant exactement deux diviseurs. Tous les autres entiers $a$ non nuls ont au moins 4 diviseurs différents : $-1$, 1, $-a$, $a$.
Cherchons à déterminer tous les diviseurs de 12. Le théorème nous assure tout de suite qu'il suffit de les chercher dans

$$\{-12, -11, -10, \ldots, 10, 11, 12\}$$

Il suffit alors d'examiner si chaque élément de cet ensemble est diviseur de 12 (à ce point, une certaine connaissance de ses tables de multiplication est nécessaire). On trouve alors que

$$\mathcal{D}(12) = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$$

Revenons maintenant aux multiples d'un entier $b$. Ce sont les nombres de la forme $nb$ où $n \in \mathbb{Z}$. Si $n_1 b$ et $n_2 b$ sont deux multiples de $b$, on voit par factorisation que $n_1 b + n_2 n = (n_1 + n_2)b$ est aussi un multiple de $b$ (puisque $n_1 + n_2 \in \mathbb{Z}$). De même si $k \in \mathbb{Z}$, $k(nb) = (kn)b$ est toujours un multiple de $b$. Plus généralement, on a le résultat suivant :

**Théorème 3** *Soit $b \in \mathbb{Z}$. Si $u$ et $v$ sont deux multiples de l'entier $b$, alors pour tous $\lambda \in \mathbb{Z}$ et $\mu \in \mathbb{Z}$, $\lambda u + \mu v$ est un multiple de $b$.*
*Ce résultat se reformule aussi : si $b$ divise $u$ et $b$ divise $v$, alors dès que $\lambda \in \mathbb{Z}$ et $\mu \in \mathbb{Z}$, $b$ divise $\lambda u + \mu v$.*

$$(b|u \text{ et } b|v) \Rightarrow (\forall(\lambda,\mu) \in \mathbb{Z}^2,\ b|(\lambda u + \mu v)$$

En particulier :

$$\begin{aligned} b|(u+v) &\quad (\lambda = \mu = 1) \\ b|(u-v) &\quad (\lambda = 1, \mu = -1) \\ b|(ku) \text{ pour } k \in \mathbb{Z} &\quad (\lambda = k, \mu = 0) \end{aligned}$$

Preuve : $u$ et $v$ sont des multiples de $b$, donc il existe des éléments $n_1$ et $n_2$ de $\mathbb{Z}$ tels que $u = n_1 b$ et $v = n_2 b$. Ainsi si $\lambda$ et $\mu$ sont dans $\mathbb{Z}$,

$$\lambda u + \mu v = \lambda n_1 b + \mu n_2 b = (\lambda n_1 + \mu n_2)b$$

Et comme $\lambda n_1 + \mu n_2 \in \mathbb{Z}$, $\lambda u + \mu v$ est un multiple de $b$. Le reste s'en déduit.

Ce théorème, a priori très banal, est très utile car il permet d'étudier la divisibilité d'un entier en se ramenant à un cas plus simple. Prenons l'exemple suivant : "Quels sont les entiers $n$ tels que $n+2|7n+3$ ? "
Le théorème va nous permettre de faire disparaître le $n$ dans $7n+3$ par combinaison linéaire : on sait que $n+2|n+2$, donc si $n+2|7n+3$, on a $n+2|(7n+3-7(n+2))$ ce qui donne $n+2|-11$. On se ramène donc à chercher les diviseurs de $-11$. On obtient : $n+2 \in \mathcal{D}(-11) = \{-11, -1, 1, 11\}$, et donc $n \in \{-13, -3, -1, 9\}$. Cependant à ce stade, on n'a pas encore résolu le problème : on a montré que si $n$ est solution, il est dans l'ensemble $\{-13, -3, -1, 9\}$. Mais est-ce que tous les éléments de cet ensemble sont des solutions ? On pourrait bien sûr vérifier que ces éléments sont tous solution un par un (il n'y a que quatre vérifications à faire), mais dans un cas où il y a plus de possibilités ce serait fastidieux. Il s'avère en fait qu'ici on peut refaire le raisonnement à l'envers. En effet, si $n$ est dans cet ensemble, $n+2|-11$, donc $n+2|-11+7(n+2) = 7n+3$ et donc $n$ est solution. Finalement on peut bien conclure que l'ensemble des solutions est $\{-13, -3, -1, 9\}$.

# 2 Congruences.

Nous avons vu que pour montrer qu'un nombre est divisible par un entier $n$, on peut se ramener par combinaisons linéaires à étudier la divisibilité par $n$ d'entiers plus petits, et donc à un problème plus simple. Essentiellement, si on considère un entier $a$, il est équivalent de dire

que $n|a$ ou que $n|a+n$, ou encore que $a|a+2n$ ... Plus généralement $n|a$ si et seulement si il existe un entier $k$ tel que $n|a+kn$, et dans ce cas $n|a+k'n$ pour tout entier $k'$. Ceci nous montre que tous les entiers $a, a+n, \ldots a+kn, \ldots$ ont les mêmes propriétés lorsqu'on étudie la divisibilité par $n$. Voilà pourquoi la notion suivante est très utile.

**Définition 2** *Soit $n \in \mathbb{N}^*$, on dit que deux entiers $a$ et $b$ sont congrus modulo $n$ si $n|(a-b)$ et on note alors $a \equiv b\,[n]$.*

Vérifions tout de suite quelques propriétés du symbole de congruence, fixons donc un entier $n \in \mathbb{N}^*$.
Pour tout entier $a$, $a \equiv a\,[n]$, car on toujours $n|a-a=0$.
Si $a$ et $b$ sont deux entiers, $n|a-b$ si et seulement si $n|b-a$. Il est donc équivalent de dire que $a \equiv b\,[n]$ ou que $b \equiv a\,[n]$.
Si $a$, $b$, $c$ sont trois entiers tels que $a \equiv b\,[n]$ et $b \equiv c\,[n]$, alors $n|a-b$ et $n|b-c$. D'où $n|(a-b)+(b-c)=a-c$ et donc $a \equiv c\,[n]$.
Ces quelques propriétés montrent déjà que le symbole de congruence est une relation assez souple, passons maintenant aux propriétés les plus importantes de ce symbole.

**Théorème 4** *Soit $n \in \mathbb{N}^*$ et $a$, $b$, $c$, $d$ quatre entiers. Alors*

$$a \equiv b\,[n] \text{ et } c \equiv d\,[n] \Rightarrow a+c \equiv b+d\,[n] \text{ et } ac \equiv bd\,[n]$$

Ce résultat peut se traduire par la phrase suivante : "la relation de congruence se préserve par addition et multiplication". Et ceci est très important, nous verrons pourquoi au fur et à mesure. Bien sûr il est aussi vrai que la congruence préserve les combinaisons linéaire, c'est d'ailleurs un cas particulier de ce théorème : soient $a \equiv b\,[n]$, $c \equiv d\,[n]$ et $\lambda$ et $\mu$ deux entiers. Comme $\lambda \equiv \lambda\,[n]$, on a $\lambda a \equiv \lambda b\,[n]$. De même $\mu c \equiv \mu d\,[n]$, et donc $\lambda a + \mu c \equiv \lambda b + \mu d\,[n]$.
Nous allons maintenant donner la preuve (très simple) de ce théorème.
Preuve : On a $n|b-a$ et $n|d-c$, donc d'après le théorème 3, $n|b-a+d-c=(b+d)-(a+c)$ et donc $a+c \equiv b+d\,[n]$. De même $bd-ac=b(d-c)+(b-a)c$. Comme $n|b-a$ et $n|d-c$, on a bien $n|bd-ac$, d'où $ac \equiv bd\,[n]$.

Pour terminer cette partie sur les congruences, nous allons montrer l'utilité des congruences sur un exemple bien connu : le critère de divibilité par 3. Il est en général bien connu qu'un entier est divisible par 3 si et seulement la somme des chiffres de son écriture en base 10 est un multiple de 3. Par exemple 135681 est divisible par 3 car $1+3+5+6+8+1=24$ qui est divisible par 3. Nous allons montrer d'où vient ce critère.
Soit $n$ un entier naturel. L'écriture de $n$ en base 10 est la donnée d'entiers $a_0$, ...,$a_d$ compris entre 0 et 9 tels que $n = a_d 10^d + a_{d-1}10^{d-1} + \cdots + a_0$. Voyons ce que donne cette égalité modulo 3. On a $10 = 3 \times 3 + 1$ donc $10 \equiv 1\,[3]$. Il en découle que $10^2 \equiv 1 \times 1 = 1\,[3]$ et donc, en itérant, pour tout $k \in \mathbb{N}^*$, $10^k \equiv 1\,[3]$. Il faut remarquer que pour écrire tout cela, on doit appliquer le théorème 4 dans le cas multiplicatif. En appliquant maintenant à nouveau le théorème 4 dans le cadre additif, on a $n \equiv a_d + a_{d-1} + \cdots + a_0\,[3]$. On a donc montré que pour étudier la divisibilité par 3 d'un entier, il suffit d'étudier la divisibilité par 3 de la somme des chiffres de son écriture décimale, en particulier un entier est divisible par 3 si et seulement si la somme des chiffres de son écriture décimale est divisible par 3. Comme $10 \equiv 1\,[9]$ le même raisonnement nous donne un critère de divisibilité par 9.

# 3 La division euclidienne.

On a vu que la notion de congruence permet de simplifier l'étude de la divisibilité d'un entier en se ramenant à étudier des entiers plus petits. Cependant on ne sait pas encore quelles sont les limites de cette méthode : ne peut-on pas donner un sens plus précis à "petit" ? La division euclidienne répond à cette question. En fait, quand on étudie la divisibilité par un entier $n$, on peut toujours se ramener à étudier ce qui se passe pour des nombres compris entre 0 et $n$, c'est l'objet de paragraphe.

**Théorème 5** *Étant donné un entier $a$ et un entier $b$ strictement positif, il existe un unique couple $(q,r)$ où $q \in \mathbb{Z}$ et $0 \leq r \leq b-1$ tel que*

$$a = bq + r$$

Chercher ces entiers $q$ et $r$ consiste à effectuer "la division euclidienne" de $a$ par $b$. On appelle $q$ le quotient de la division euclidienne et $r$ le reste.

En terme de congruences, ce théorème peut se reformuler ainsi : tout entier relatif est congru modulo $b$ à un unique entier compris entre 0 et $b-1$.

Commençons par démontrer ce résultat, nous verrons ensuite quelle est son utilité.
Preuve : Comme $b \geq 1$, il existe un entier $k$ tel que $kb \geq a$, donc l'ensemble des multiples de $b$ qui sont inférieurs à $a$ est majoré, il existe donc dans cet ensemble un plus grand élément : $qb$, où $q$ est un entier. Alors $(q+1)b = qb+b > qb$, donc par définition de $q$, $qb+b > a$. Posons alors $r = a - qb$. Comme $a \geq qb$, on a $r \geq 0$ et comme $qb + b > a$, on a $r = a - qb < b$. $r$ étant entier, $r \leq b-1$. On a donc démontré l'existence des entiers $q$ et $r$.
Montrons maintenant qu'ils sont uniques, c'est à dire que si $a = bq + r$ et $a = q'b + r'$ où $q$, $q'$, $r$ et $r'$ sont des entiers avec $0 \leq r \leq b-1$ et $0 \leq r' \leq b-1$, alors $q = q'$ et $r = r'$. Pour ce faire, commençons par écrire $qb + r = a = q'b + r'$, donc $r - r' = (q' - q)b$. Ainsi, comme $q - q'$ est un entier, $r - r'$ est un multiple de $b$. Or on a vu que si $a$ est un multiple non nul de $b$, alors $|a| \geq |b|$, donc si $r - r'$ était non nul, on aurait $|r - r'| \geq |b| = b$. Cependant comme $0 \leq r \leq b-1$ et $0 \leq r' \leq b-1$, on a $-(b-1) \leq r - r' \leq b-1$, donc $|r - r'| \leq b-1$, ce qui donne une contradiction si $r - r'$ est non nul. On peut donc conclure que $r - r' = 0$, donc $r = r'$. On obtient alors $qb = q'b$ et comme $b$ est non nul, $q = q'$, ce qui achève la preuve de l'unicité.

Le théorème donne donc une réponse positive à la question : pourra-t-on toujours simplifier l'étude de la congruence d'un entier ? Oui car tout entier est congru modulo $n$ à un unique entier compris entre 0 et $n-1$. Ce qui est très intéressant dans ce résultat, c'est que pour un entier $n$ strictement positif : "il n'y a qu'un nombre fini de congruences modulo $n$". Si $a$ est un entier, on peut noter $C(a)$ l'ensemble des entiers congru à $a$ modulo $n$. Effectuons la division euclidienne de $a$ par $n$, on obtient un reste $r$ compris entre 0 et $n-1$. On déduit alors facilement des propriétés de la relation de congruence que $C(a) = C(r)$. De plus si $r$ et $s$ sont deux entiers compris entre 0 et $n-1$ tels que $r \neq s$, l'unicité du reste de la division euclidienne montre que $C(r)$ et $C(s)$ sont deux ensembles disjoints (en effet si un entier $a$ apartenait à ces deux ensembles à la fois, $r$ et $s$ seraient deux restes de la division euclidienne de $a$ par $n$, et donc $r = s$). $C(a)$ s'appelle la classe de congruence de $a$ modulo $n$. Finalement le théorème précédent peut se reformuler sous la forme :

**Théorème 6** *Il y a exactement $n$ classes de congruences modulo $n$ qui sont les ensembles $C(k)$ pour $k$ compris entre 0 et $n-1$.*

Voyons maintenant à quoi peut servir ce résultat. Supposons que nous voulions démontrer que pour tout entier naturel $n$, le nombre $n(n+1)(n+2)$ est divisible par 3.
Le théorème nous assure que $n$ est congru à 0, 1 ou 2 modulo 3 : il n'y a donc que 3 cas à étudier.

- Premier cas : $n \equiv 0\,[3]$, cela signifie exactement que $n$ est divisible par 3. Comme $(n+1)(n+2)$ est entier, $n(n+1)(n+2)$ est divisible par 3.
- Deuxième cas : $n \equiv 1\,[3]$. Alors $n+2 \equiv 3 \equiv 0\,[3]$, donc $n+2$ est divisible par 3, et donc $n(n+1)(n+2)$ aussi.
- Troisième cas : $n \equiv 2\,[3]$. Alors $n+1 \equiv 0\,[3]$, et de même $n(n+1)(n+2)$ est divisible par 3.

Tous les cas ont été traités, donc pour tout $n$ entier, $n(n+1)(n+2)$ est divisible par 3. Ici le théorème nous a donc permis de nous ramener à étudier seulement 3 cas.

Voici un autre exemple, celui du problème dit "des deux carrés". Étant donné un entier $n$, peut-on l'écrire sous la forme $n = a^2 + b^2$ où $a$ et $b$ sont deux entiers ? Nous allons voir que ceci n'est pas toujours possible, l'idée est de regarder les classes de conjugaison modulo 4. Si $a \in \mathbb{Z}$, $a$ est congru à 0, 1, 2 ou 3 modulo 4. Quelle est alors la classe de conjugaison de $a^2$ ? On sait que $a \equiv r\,[4]$ où $r \in \{0,1,2,3\}$. Alors $a^2 \equiv r^2\,[4]$. Il y a ainsi 4 cas à étudier :

- $r = 0$, $r^2 \equiv 0\,[4]$.
- $r = 1$, $r^2 \equiv 1\,[4]$.
- $r = 2$, $r^2 = 4 \equiv 0\,[4]$.
- $r = 3$, $r^2 = 9 = 8 + 1 \equiv 1\,[4]$.

Donc finalement un carré est congru à 0 ou 1 modulo 4. Ainsi si $a$ est une somme de deux carrés, $a$ est congru à 0, 1 ou 2 modulo 4. L'unicité du reste de la division euclidienne prouve alors bien qu'un entier congru à 3 modulo 4 ne peut pas s'écrire comme somme de deux carrés. Par exemple 40003 n'est pas une somme de deux carrés (n'est-ce pas plus facile ainsi que de le vérifier à la main ?).
Le problème de savoir quels sont exactement les entiers qui sont somme de deux carrés est plus difficile.

# 4 PGCD et équations linéaires à coefficients entiers.

Un nouveau problème qui apparaît souvent en arithmétique est de comparer deux entiers, mais d'une façon particulière : en regardant leurs diviseurs. On peut se poser cette question : si l'on prend deux entiers $a$ et $b$, quels sont les diviseurs que ces deux nombres ont en commun ? Il s'agit de l'ensemble $\mathcal{D}(a) \cap \mathcal{D}(b)$. Si $a$ ou $b$ est non nul, cet ensemble est évidemment fini, il admet donc un plus grand élément que l'on appelle le PGCD de $a$ et $b$ (PGCD signifie Plus Grand Commun Diviseur). Nous allons voir que cet élément a des propriétés très intéressantes qui font qu'il caractérise à lui tout seul tous les diviseurs communs à $a$ et $b$. En fait, un des but de ce chapitre sera de montrer qu'un entier divise à la fois $a$ et $b$ si et seulement si il divise PGCD($a$,$b$). PGCD($a$,$b$) permet donc à lui seul de connaître tous les diviseurs communs à $a$ et $b$, puisque ce sont exactement les diviseurs de PGCD($a$,$b$). On peut encore réécrire ceci de cette façon : $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(\text{PGCD}(a,b))$.

Nous allons aussi étudier un autre type de problème auquel le PGCD est fortement lié : les équations linéaires à coefficients entiers. Il s'agit d'équations de la forme $am + bn = c$ où $a$, $b$ et $c$ sont des entiers fixés, et où on cherche des solutions $(m,n)$ telles que $m$ et $n$ soient des entiers. Voici typiquement le type de problème faisant intervenir ce genre d'équation :
On dispose de billets de 20 et 50 euros. Combien y a-t-il de façons, et quelles sont-elles, de réunir

la somme de 240 euros ? Cela revient en effet à trouver des entiers naturels $m$ et $n$ tels que $20m + 50n = 240$.
On peut aussi voir ces équations plus géométriquement : si on considère la droite affine d'équation $ax+by = c$. Les solutions $(m,n)$ de l'équation qui sont entières, représentent exactement les points à coordonnées entières qui sont sur la droite.

Donnons tout d'abord quelques exemples simples de PGCD. Si $a$ et $b$ sont deux entiers tels que $b|a$, alors $\text{PGCD}(a,b) = |b|$. En effet le PGCD de $a$ et $b$ est le plus grand diviseur commun à $a$ et $b$. En particulier, il divise $b$. Donc d'après le théorème 2, $\text{PGCD}(a,b) \leq |b|$. Mais $|b|$ est un diviseur de $b$. Et comme $b$ divise $a$, $|b|$ aussi. Ainsi $|b|$ est un diviseur commu à $a$ et $b$, et c'est bien le plus grand.
On peut aussi remarquer que si $a$ est un entier, alors $\text{PGCD}(a,1) = 1$.

Revenons maintenant à l'étude des équations $am + bn = c$ où $a$, $b$ et $c$ sont des entiers. Supposons que nous ayons une solution $(m,n)$ à l'équation $am + bn = c$, et posons $d = \text{PGCD}(a,b)$. Par définition $d|a$ et $d|b$, donc $d|c$. Ainsi une condition nécessaire pour que l'équation ait des solutions est que $c$ soit un multiple du PGCD de $a$ et $b$. Le résultat important est que si tel est le cas, l'équation a effectivement des solutions.

**Théorème 7** *Soient $a$ et $b$ deux entiers relatifs tels que $a$ ou $b$ soit non nul et $d = PGCD(a,b)$. L'équation $am + bn = c$ a des solutions entières si et seulement si $d|c$.*

Remarque : Le théorème nous donne uniquement une condition pour qu'il existe des solutions, il ne nous donne pas toutes les solutions de l'équation. Nous verrons cependant plus loin que l'on peut déterminer l'ensemble des solutions.

Preuve : Nous avons déjà vu que pour qu'il y ait des solutions, il est nécessaire que $d|c$. Réciproquement, nous allons monter que si $d|c$, il y a des solutions à cette équation.
Montrons d'abord que l'équation $am + bn = \text{PGCD}(a,b)$ a des solutions. Pour cela, l'idée est de considérer toutes les combinaisons entières possibles de $a$ et $b$, c'est à dire l'ensemble $\mathbb{Z}a + \mathbb{Z}b = \{am + bn,\ m \in \mathbb{Z}, n \in \mathbb{Z}\}$ et de montrer que $\text{PGCD}(a,b) \in \mathbb{Z}a + \mathbb{Z}b$. Comme $a$ et $b$ ne sont pas nuls tous les deux, cet ensemble contient un entier non nul. De plus, si $u \in \mathbb{Z}a + \mathbb{Z}b$, $-u \in \mathbb{Z}a + \mathbb{Z}b$, on voit donc que cet ensemble contient nécessairement un entier strictement positif. Appelons alors $h$ le plus petit entier strictement positif appartenant à cet ensemble. Nous allons montrer que $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}h = \{kh, k \in \mathbb{Z}\}$. En effet, supposons que $x \in \mathbb{Z}a + \mathbb{Z}b$, effectuons la division euclidienne de $x$ par $h$. On obtient $x = qh + r$ où $q$ est entier et $0 \leq r < h$. Comme $x$ et $h$ sont dans $\mathbb{Z}a + \mathbb{Z}b$, on voit que $x - qh$ y est aussi. Ainsi $r$ est un élément de $\mathbb{Z}a + \mathbb{Z}b$. Mais n'oublions pas que l'on a supposé que $h$ est le plus petit élément de $\mathbb{Z}a + \mathbb{Z}b$ qui est strictement positif. Donc si $r \neq 0$, alors par définition de $h$, on doit avoir $r \geq h$. Mais ceci est absurde vu que l'on sait que $r < h$. Ainsi $r = 0$, ce qui prouve que $x = qh$. Réciproquement il est facile de vérifier que tous les multiples de $h$ sont dans $\mathbb{Z}a + \mathbb{Z}b$. On a donc montré que $\mathbb{Z}a + \mathbb{Z}b$ est en fait constitué de tous les multiples de $h$.
Or $a$ et $b$ sont des éléments de $\mathbb{Z}a + \mathbb{Z}b$, donc d'après ce que l'on vient de démontrer, il existe des entiers $u$ et $v$ tels que $a = uh$ et $b = vh$. $h$ est ainsi un diviseur commun à $a$ et $b$. Par définition du PGCD de $a$ et $b$, on a donc $h \leq \text{PGCD}(a,b)$. D'un autre côté, on sait par définition qu'il existe des entiers $m$ et $n$ tels que $h = am + bn$, donc le PGCD de $a$ et $b$ divise $h$. Ainsi $|\text{PGCD}(a,b)| \leq |h|$ et comme tous ces nombres sont positifs, ceci donne $\text{PGCD}(a,b) \leq h$. Finalement on a montré $\text{PGCD}(a,b) \leq h$ et $h \leq \text{PGCD}(a,b)$, d'où $h = \text{PGCD}(a,b)$. Il existe donc bien des entiers $m$ et $n$ tels que $am+bn = \text{PGCD}(a,b)$, et donc l'équation $am+bn = \text{PGCD}(a,b)$

a des solutions.
Nous pouvons maintenant enfin conclure : si PGCD$(a,b)|c$, on peut écrire $c = \text{PGCD}(a,b)k$. Soient $m$ et $n$ tels que $am + bn = \text{PGCD}(a,b)$ (ils existent d'après ce qui précède), alors $a(km) + b(kn) = k\text{PGCD}(a,b) = c$, ce qui prouve que l'équation $am + bn = c$ a des solutions, et achève enfin la preuve du théorème.

Remarque : On peut remarquer que dans la preuve ci-dessus, on a en fait montré que $\mathbb{Z}a + \mathbb{Z}b = \text{PGCD}(a,b)\mathbb{Z}$.

Nous allons maintenant revenir vers des propriétés plus spécifiques du PGCD et démontrer le résultat dont nous parlions plus haut :

**Théorème 8** *Soient $a$ et $b$ deux entiers. Alors $d$ est un diviseur commun à $a$ et $b$ si et seulement si $d$ divise PGCD$(a,b)$.*

Preuve : Si $d$ divise PGCD$(a,b)$, comme PGCD$(a,b)$ divise $a$ et $b$, on voit que $d$ doit également diviser $a$ et $b$. C'est la partie réciproque qui est moins évidente, mais avec le théorème 7, cela devient plus facile. Supposons que $d$ divise à la fois $a$ et $b$. On sait qu'il existe des entiers $m$ et $n$ tels que $am + bn = \text{PGCD}(a,b)$. Alors, comme $d|a$ et $d|b$, on a $d|\text{PGCD}(a,b)$ et la preuve est terminée !

# 5 Entiers premiers entre eux, théorèmes de Bezout et Gauss.

**Définition 3** *Soient $a$ et $b$ deux entiers, on dit qu'ils sont premiers entre eux si leur PGCD vaut 1.*

Dire que deux entiers sont premiers entre eux revient à dire que leurs seuls diviseurs communs sont 1 et $-1$, c'est à dire qu'au niveau arithmétique, ils sont le plus différent possible.
Le théorème de Bezout donne une caractérisation des entiers premiers eux.

**Théorème 9 (Théorème de Bezout)** *Deux entiers $a$ et $b$ sont premiers entre eux si et seulements si, il existe des entiers $m$ et $n$ tels que $am + bn = 1$.*

Preuve : La preuve a essentiellement déjà été faite : supposons que $a$ et $b$ soient premiers entre eux. D'après le théorème 7, il existe des entiers $m$ et $n$ tels que $am + bn = \text{PGCD}(a,b) = 1$. Réciproquement s'il existe $m$ et $n$ tels que $am+bn = 1$, alors PGCD$(a,b)|1$, donc PGCD$(a,b) = 1$, ce qui signifie que $a$ et $b$ sont premiers entre eux.

Remarque : on doit cependant remarquer que ce théorème donne plus d'information que le théorème 7, car ici on a une condition nécessaire et suffisante. Si $am + bn = c$, tout ce qu'on peut dire c'est que le PGCD de $a$ et $b$ divise $c$. Mais si $c = 1$, on peut affirmer qu'il y a égalité.
On a aussi le résultat suivant, conséquence immédiate du théorème :

**Corollaire 1** *Si $a$ et $b$ sont deux entiers premiers entre eux :*

$$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}$$

Autrement dit, tout entier peut d'écrire comme combinaison entières de deux entiers premiers entre eux choisis arbitrairement.

Nous allons maintenant passer à un autre théorème très important. Voici le problème : supposons que l'on sache qu'un entier $d$ divise un produit $ab$ de deux entiers. On ne peut a priori pas dire que $d$ divise $a$ ou que $d$ divise $b$. $d$ peut même ne diviser ni $a$ ni $b$, comme on le voit en prenant $d = 6$, $a = 3$ et $b = 4$. Supposons cependant que $d$ et $a$ soient premiers entre eux, cela signifie que $a$ et $d$ n'ont aucun diviseur en commun (ce n'est pas le cas dans l'exemple précédent où $a$ et $d$ ont 3 comme diviseur commun), alors on peut s'attendre à ce que $d$ divise $b$, c'est l'objet du théorème suivant :

**Théorème 10 (Théorème de Gauss)** *Soient $a$, $b$ et $d$ trois entiers tels que $a$ et $d$ soient premiers entre eux. Alors $d|b$.*

Preuve : Comme $a$ et $d$ sont premiers entre eux, il existe, d'après le théorème de Bezout, deux entiers $u$ et $v$ tels que $au + dv = 1$. En multipliant cette expression par $b$, on a $abu + dbv = b$. Or comme $d|ab$, on obtient alors bien $d|(abu + dbv)$, c'est à dire $d|b$.

Ce théorème est très utile, car il permet souvent de simplifier certaines situations. Par exemple si on sait que $3|2n$, alors on peut en conclure que $3|n$. Voici d'autres exemples parfois bien utiles :

**Corollaire 2** *Soient $a$, $b$, $c$ trois entiers tels que $a$ est premier à $c$ et $b$ est premier à $c$. Alors $ab$ est premier à $c$.*

Preuve : En effet, soit $d$ le PGCD de $ab$ et de $c$. Comme $d$ divise $c$ et que $c$ est premier à $a$, alors $d$ est premier à $a$ (ceci nécessite une petite vérification laissée au lecteur). Ainsi comme $d|ab$, d'après le théorème de Gauss, $d|b$. Or on sait par hypothèse que $d$ divise aussi $c$. Comme $c$ et $b$ sont premiers entre eux, $d = 1$.

**Corollaire 3** *Si $a$ et $b$ sont deux entiers premiers entre eux divisant un entier $c$, alors $ab$ divise $c$.*

Preuve : En effet on peut écrire $c = ak$ où $k$ est un entier. Comme $b$ divise $c$ et que $a$ et $b$ sont premiers entre eux, d'après le théorème de Gauss, $b$ divise $k$. On peut donc bien en conclure que $ab$ divise $c = ak$.

Remarque : Ce dernier résultat est encore une fois très intuitif : si $a$ et $b$ divisent $c$, une raison pour laquelle $ab$ ne doit pas forcément diviser $c$ est que $a$ et $b$ auront peut-être des diviseurs en communs, et le produit $ab$ peut être "trop gros" pour diviser $c$ (par exemple 6 et 3 divisent 12, mais $18 = 3 \times 6$ non). Mais si on suppose $a$ et $b$ premiers entre eux, ils n'ont par définition, aucun diviseur en commun, et on s'attend alors bien à ce que $ab$ divise $c$.

Revenons un instant dans le cas général où $a$ et $b$ sont deux entiers quelconques, non nécessairement premiers entre eux. Soit $d$ leur PGCD. On peut alors écrire $a = da'$ et $b = db'$ où $a'$ et $b'$ sont deux entiers. Que dire alors de $a'$ et $b'$ ? Souvenons-nous que le PGCD de deux entiers représente tout ce que ces entiers ont en commun d'un point de vue arithmétique. On doit donc s'attendre à ce que $a'$ et $b'$ soient premiers entre eux. Et c'est bien le cas. En effet, d'après le théorème 7, on peut trouver des entiers $m$ et $n$ tels que $am + bn = d$. Mais en écrivant $a = da'$ et $b = db'$, on voit que $a'm + b'n = 1$. D'après le théorème de Bezout, $a'$ et $b'$ sont bien premiers entre eux.

Pour conclure ce chapitre, nous allons achever l'étude des équation linéaires à coefficients entiers que nous avions commencée dans le chapitre précédent, en déterminant toutes les solutions

d'une telle équation.

**Théorème 11** *Soient a, b et c des entiers. L'équation $ax + by = c$ a des solutions entières si et seulement si le PGCD de a et b divise c. De plus si cette condition est vérifiée, soit $(x_0,y_0)$ une solution particulière de l'équation et $a'$ et $b'$ tels que $a = PGCD(a,b)a'$ et $b = PGCD(a,b)b'$. Alors l'ensemble des solutions est :*

$$\{(x_0 + b'k,y_0 - a'k), k \in \mathbb{Z}\}$$

Preuve : Nous supposerons tout le temps ici que $a \neq 0$. Soit $(x,y)$ une solution entière de cette équation. Alors $ax + by = c$. Or on sait que $c = ax_0 + by_0$, donc $ax + by = ax_0 + by_0$, donc $a(x - x_0) = b(y_0 - y)$. En simplifiant cette égalité par le PGCD de $a$ et $b$, on obtient $a'(x - x_0) = b'(y_0 - y)$. Or $a'$ et $b'$ sont maintenant premiers entre eux (voir plus haut), et $a'$ divise $b'(y_0 - y)$. Donc d'après le théorème de Gauss, $a'$ divise $y_0 - y$. On pose alors $y - y_0 = -a'k$ avec $k \in \mathbb{Z}$. On a alors $a'(x - x_0) = b'a'k$ d'où $x - x_0 = b'k$ puisque, $a$ étant non nul, $a'$ est non nul. Ainsi toute solution de l'équation est de la forme annoncée. Vérifions réciproquement que tous les éléments de cet ensemble sont solutions de l'équation.
En effet si $k \in \mathbb{Z}$, $a(x_0 + b'k) + b(y_0 - a'k) = (ax_0 + by_0) + k(ab' - ba') = c + k(ab' - ba') = c$ car $\text{PGCD}(a,b)(ab' - ba') = ab - ba = 0$, et $ab' - ba' = 0$.
Remarque : L'hypothèse $a \neq 0$ dans la démonstration n'est pas restrictive, puisque si $a = b = 0$, les solutions sont faciles à déterminer, et dans le cas contraire, on peut toujours se ramener à $a \neq 0$, quitte à inverser les rôles de $a$ et $b$.
Si on applique ce résultat au problème de trouver comment réunir 240 euros avec des billets de 20 et 50 euros, il ne faudra retenir que les solutions positives de cet ensemble (il y a alors une condition sur $k$).

# 6 PPCM.

Dans ce très court chapitre, nous allons étudier le PPCM, de deux entiers, notion très proche du PGCD.

**Définition 4** *Soient a et b deux entiers. On appelle PPCM de a et b (Plus Petit Commun Multiple), le plus petit entier strictement positifs PPCM(a,b) qui soit à la fois un multiple de a et un multiple de b.*

Supposons désormais $a$ et $b$ positifs (on peut toujours se ramener à ce cas en multiplicant par $-1$). Il est déjà clair que $ab$ est toujours un multiple commun à $a$ et $b$, ce n'est cependant pas toujours le PPCM, il existe souvent des multiples communs à $a$ et $b$ plus petits. Soit en effet $d$ le PGCD de $a$ et $b$. On peut écrire $a = da'$ et $b = db'$ où $a'$ et $b'$ sont premiers entre eux. Alors $da'b'$ est toujours un multiple de $a$, car il s'agit de $ab'$. Mais c'est aussi toujours un multiple de $b$ puisqu'on peut aussi l'écrire $ba'$. C'est donc un multiple commun à $a$ et $b$. Or on voit bien qu'il est plus petit que $ab$ vu que $ab = d^2a'b'$. En fait on montre que $da'b'$ est le PPCM de $a$ et $b$.

**Théorème 12** *Soient a et b deux entiers positifs non tous les deux nuls. On pose $a = PGCD(a,b)a'$ et $b = PGCD(a,b)b'$. Alors le PPCM de a et b est $PGCD(a,b)a'b'$.*

Preuve : En effet soit $m$ le PPCM de $a$ et $b$. On sait que $a$ divise $m$, donc $m = ak = \text{PGCD}(a,b)a'k$ où $k$ est un entier. Or $b = \text{PGCD}(a,b)b'$ divise aussi $m$, donc on peut affirmer que $b'$ divise $a'k$. Comme $a'$ et $b'$ sont premiers entre eux, le théorème de Gauss nous assure que $b'$ divise $k$. Ainsi $k = b'k'$ où $k'$ est un entier. Donc $\text{PGCD}(a,b)a'b'$ divise $m$. Or $\text{PGCD}(a,b)a'b'$ est un multiple commun à $a$ et $b$ comme on l'a vu plus haut. Comme $m$ est le plus petit de ces multiples, on a bien $m = \text{PGCD}(a,b)a'b'$, ce qui achève la démonstration.

Remarque : Comme $ab = \text{PGCD}(a,b)^2 a'b'$, on peut en conclure que $ab$ est le PPCM de $a$ et $b$ si et seulement si $a$ et $b$ sont premiers entre eux. Plus généralement on a la formule suivante :

**Corollaire 4** *Si $a$ et $b$ sont deux entiers positifs non nuls, on a*

$$PGCD(a,b)PPCM(a,b) = ab$$

# 7 Les nombres premiers et le théorème fondamental de l'arithmétique.

Dans notre étude des diviseurs des nombres entiers, on peut observer que certains nombres ont un statut bien particulier : ils ont très peu de diviseurs. On a déjà vu qu'un entier $n$ a au moins pour diviseurs 1, $-1$, $n$ et $-n$. Il existe des entiers qui n'ont aucun autre diviseur : par exemple 2, 3, 5 ... Mais 6 par exemple en a plus : il y a aussi 2, 3, $-2$ et $-3$. Les entiers ayant cette particularité d'avoir si peu de diviseurs sont appelés nombres premiers.

**Définition 5** *On appelle nombre premier un nombre entier naturel $p$ ayant exactement 4 diviseurs, à savoir 1, $-1$, $p$ et $-p$.*

On peut tout de suite remarquer qu'avec cette définition, 1 n'est pas considéré comme un nombre premier. En effet, il n'a que 2 diviseurs : 1 et $-1$. C'est une convention, nous verrons plus loin pourquoi le théorème fondamental de l'arithmétique rend cette convention compréhensible.

Remarquons aussi que si $p$ est un nombre premier et $n$ un entier, soit $p$ divise $n$, soit $p$ et $n$ sont premiers entre eux (en effet le pgcd de $p$ et $n$ est un diviseur de $p$, donc est soit 1 soit $p$).

Donnons quelques exemples de nombres premiers. Nous avons 2, 3, 5, 7, 11, 13 ... (essayez de trouver tous les nombres premiers jusqu'à 50). En fait les nombres premiers sont fondamentaux car ils permettent à eux seuls de retrouver tous les autres entiers. Par exemple on peut écrire $60 = 2 \times 2 \times 3 \times 5$. C'est un produit de nombres premiers. En fait tout entier peut s'écrire comme un tel produit de nombres premiers, et mieux : cette décomposition est unique. Dans notre exemple cela signifie que tout produit d'une séquence de nombres premiers autre que 2, 2, 3, 5, donnerait un autre résultat que 60. Il s'agit de ce qu'on appelle le théorème fondamental de l'arithmétique.

**Théorème 13 (Théorème fondamental de l'arithmétique)** *Soit $n$ un entier naturel non nul. Il existe des nombres premiers $p_1, \ldots, p_r$ et des entiers naturels $\alpha_1, \ldots, \alpha_r$ tels que $n = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$. De plus cette décomposition est unique, c'est à dire que si $n = q_1^{\beta_1} \times \cdots \times q_s^{\beta_s}$ où $q_1, \ldots, q_s$ sont des nombres premiers, alors pour tout $1 \leq i \leq s$, il existe un $1 \leq j \leq r$ tel que $q_i = p_j$ et $\alpha_j = \beta_i$.*

Preuve : Nous allons d'abord démontrer l'existence d'une telle décomposition. Notons $E$ l'ensemble des entiers naturels qui s'écrivent comme un produit de nombres premiers. Ce que l'on veut montrer, c'est que $E = \mathbb{N}^*$. Supposons donc le contraire, et soit $n$ le plus petit entier qui ne soit pas dans $E$. Alors $n$ n'est pas premier, car sinon $n$ serait dans $E$. $n$ a donc un diviseur $d$ tel que $1 < d < n$. Par définition de $n$, $d$ est dans $E$. Ainsi $d$ est un produit de nombres premiers, et il existe donc un nombre premier $p$ qui divise $d$. $p$ divise alors aussi $n$. On peut donc écrire $n = pk$ où $k$ est un entier. Mais comme $p$ est premier, $p \geq 2$, ainsi $k < n$. Par définition de $n$, $k$ est dans $E$, donc $k$ est un produit de nombres premiers. Ainsi $pk = n$ est aussi un produit de nombres premiers. C'est absurde puisque l'on a supposé que $n$ n'appartient pas à $E$. Notre hypothèse était donc fausse et on a bien $E = \mathbb{N}^*$.

Démontrons maintenant l'unicité de la décomposition. Soient $p_1, \ldots, p_r$ les nombres premiers

divisant $n$ (il n'y en a qu'un nombre fini, car ce sont tous des entiers compris entre 2 et $n$). Supposons les deux à deux distincts (si $i$ est différent de $j$ alors $p_i$ est différent de $p_j$). Posons de plus $\alpha_i$ le plus grand entier tel que $p_i^{\alpha_i}$ divise $n$. Nous aurons besoin ici du résultat suivant :

**Lemme 1** *Si $p$ et $q$ sont deux nombres premiers distincts, $m$ et $n$ deux entiers naturels supérieurs ou égaux à 1, alors $p^n$ et $q^m$ sont premiers entre eux.*

Preuve du lemme : En effet soit $d$ leur pgcd. Supposons $d$ différent de 1 et soit $l$ un diviseur premier de $d$. Alors $l$ divise $p^n$. Si $l$ est différent de $p$, alors $l$ est premier avec $p$ et d'après le théorème de Gauss, $l$ divise $p^{n-1}$. En continuant ainsi, on arrive à $l$ divise $p$, et comme $p$ est premier, $l = p$. C'est absurde. On peut donc finalement en conclure que $l = p$. Mais de la même façon on peut montrer que $l = q$, et donc $p = q$, c'est absurde aussi. Ainsi $p^n$ et $q^m$ sont premiers entre eux.

Retour à la preuve du théorème : En appliquant le lemme, on obtient que $p_1^{\alpha_1}$ et $p_2^{\alpha_2}$ sont premiers entre eux, donc $p_1^{\alpha_1}p_2^{\alpha_2}$ divise $n$. De plus $p_3^{\alpha_3}$ est premier avec $p_1^{\alpha_1}$ et avec $p_2^{\alpha_2}$, donc avec $p_1^{\alpha_1}p_2^{\alpha_2}$ d'après le corollaire 3. Ceci nous permet encore de conclure que $p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}$ divise $n$. En continuant ainsi on trouve que $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$ divise $n$. On peut donc écrire $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}k$ avec $k$ entier. Supposons $k$ différent de 1, alors il existe un nombre premier $p$ divisant $k$. Mais alors $p$ divise aussi $n$, et donc il existe $1 \leq i \leq r$ tel que $p = p_i$. On aura alors $p_i^{\alpha_i+1}$ divise $n$. Mais ceci est impossible puisque $\alpha_i$ est le plus grand entier tel que $p_i^{\alpha_i+1}$ divise $n$. On en conclut donc que $k = 1$ et que $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$. Supposons maintenant que $n = q_1^{\beta_1} \times \dots \times q_s^{\beta_s}$. Si $1 \leq j \leq s$, $q_j$ divise $n$, il existe donc $1 \leq i \leq r$ tel que $q_j = p_i$. De plus $q_j^{\beta_j}$ divise $n$, donc par définition, $\beta_j \leq \alpha_i$. Notons donc $q_j = p_{i(j)}$. On a $n = q_1^{\beta_1} \times \dots \times q_s^{\beta_s}$, donc $1 = q_1^{\alpha_{i(1)}-\beta_1} \times \dots \times q_s^{\alpha_{i(s)}-\beta s}$. Ceci impose que $\alpha_{i(j)} - \beta_j = 0$ pour tout $1 \leq j \leq s$, donc que $\alpha_{i(j)} = \beta_j$, ce qui achève la démonstration de l'unicité de la décomposition.

Ce théorème s'appelle le théorème fondamental de l'arithmétique car la structure arithmétique d'un entier dépend uniquement de sa décomposition en produit de nombres premiers. Les nombres premiers sont ainsi les briques qui permettent d'étudier l'arithmétique des entiers. 1 n'est pas en général considéré comme premier, car multiplier un entier par 1 ne change rien, il n'est donc pas considéré comme une "brique" de construction.

Soit $n$ un entier naturel. On a vu au cours de la preuve du théorème que si $p$ est un nombre premier divisant $n$ et si l'on note $v_p(n)$ l'exposant de la plus grande puissance de $p$ divisant $n$, que $n$ est le produit des $p^{v_p(n)}$ pour $p$ premier divisant $n$. Si $p$ divise $n$, $v_p(n)$ est donc un entier supérieur ou égal à 1. Posons alors $v_p(n) = 0$ si $p$ est un nombre premier ne divisant pas $n$. On a ainsi défini $v_p(n)$ pour tout nombre premier $p$ et tout entier naturel $n$. On dit que $v_p(n)$ est la valuation de $n$ en $p$. L'unicité de la décomposition en produit de facteurs premiers nous donne ceci :

**Corollaire 5** *Si $p$ est nombre premier, et si $n$ et $m$ sont deux entiers naturels, alors $v_p(nm) = v_p(n) + v_p(m)$.*

Preuve : En effet, on en décomposant $n$ et $m$ en produit de facteurs premier, on voit que l'exposant de $p$ dans la décomposition de $nm$ est $v_p(n) + v_p(m)$.

Les nombre premiers nous permettent alors de déterminer les diviseurs d'un entier $n$ :

**Théorème 14** *Soient $n$ et $d$ deux entiers. $d$ divise $n$ si et seulement si pour tout nombre premier $p$, $v_p(d) \leq v_p(n)$.*

Preuve : Si $d$ divise $n$, on peut écrire $n = dk$ où $k$ est un entier, et la formule $v_p(n) = v_p(d) + v_p(k)$ pour tout nombre premier $p$ nous montre que $v_p(d) \leq v_p(n)$. Réciproquement si pour tout nombre

premier $p$, $v_p(d) \leq v_p(n)$, définissons $k$ comme étant le produit des $p^{v_p(n)-v_p(d)}$ pour $p$ nombre premier divisant $n$. On voit en décomposant $n$, $d$ et $k$ en produits de facteurs premiers que $n = dk$.

**Corollaire 6** *Si $n$ et $m$ sont deux entiers naturels $v_p(PGCD(n,m)) = \min(v_p(n),v_p(m)$ et $v_p(PPCM(n,m)) = \max(v_p(n),v_p(m))$ pour tout nombre premier $p$.*

Preuve : En effet, soit $a$ l'entier défini par $v_p(a) = \min(v_p(n),v_p(m))$ pour tout $p$ premier. Alors $v_p(a) \leq v_p(n)$ et $v_p(a) \leq v_p(m)$ pour tout nombre premier $p$, donc $a$ est un diviseur commun à $m$ et à $n$. Mais si $d$ est un diviseur commun à $n$ et à $m$, $v_p(d) \leq v_p(n)$ et $v_p(d) \leq v_p(m)$, donc $v_p(d) \leq \min(v_p(n),v_p(m))$, et ceci pour tout premier $p$. Ainsi $d$ divise $a$. On peut bien en conclure que $a$ est le PGCD de $n$ et $m$. La formule pour le PPCM est laissée en exercice au lecteur.

On peut remarquer aussi que se donner un diviseur positif de $n$, c'est se donner, pour chaque nombre premier $p$, un entier $v_p(d)$ compris entre 0 et $v_p(n)$. Le nombre de diviseurs positifs de $n$ est donc le produit des $v_p(n)+1$ pour $p$ divisant $n$. Par exemple $60 = 2^2 \times 3 \times 5$, donc $v_2(60) = 2$, $v_3(60) = v_5(60) = 1$. Ainsi 60 a $3 \times 2 \times 2 = 12$ diviseurs positifs. En comptant les diviseurs négatifs, 60 a en tout 24 diviseurs.

On peut encore se poser une question sur les nombres premiers : y en a-t-il une infinité ? Il semble bien que oui, en essayant de déterminer "à la main" les nombres premiers, il nous semble que l'on puisse trouver des nombres premiers aussi grand que l'on veut. Cependant cette simple observation ne constitue pas une véritable démonstration mathématique. Une démonstration très élégante du fait qu'il existe une infinité de nombres premiers est connu depuis Euclide, la voici :

**Théorème 15** *Il existe une infinité de nombres premiers.*

Preuve : Supposons par l'absurde qu'il n'y ait qu'un nombre fini de nombres premiers. Notons les $p_1, \ldots, p_r$. Posons alors $N = p_1 \times \cdots \times p_r + 1$. $N$ est un entier naturel non nul et strictement supérieur à 1, donc d'après le théorème fondamental de l'arithmétique, il est divisible par un nombre premier $p$. $p$ fait donc partie de la liste $p_1, \ldots, p_r$. Ainsi $p$ divise $p_1 \times \cdots \times p_r$. Comme $p$ divise aussi $N$, on obtient que $p$ divise 1, mais ceci est bien entendu absurde. Notre hypothèse était fausse : il existe bien une infinité de nombres premiers.

# 8 Exemple : l'équation de Pythagore.

Nous allons ici étudier en tant qu'exemple d'application de tout ce qui précède, l'équation de Pythagore, c'est à dire que nous allons chercher quels sont les triplets $(x,y,z)$ de nombres entiers vérifiant $x^2 + y^2 = z^2$. Le théorème de Pythagore nous dit que géométriquement cela revient à chercher les triangles rectangles dont tous les côtés sont de longueur entière. Dans la recherche de ces solutions, on peut déjà remarquer qu'on peut supposer $x$ et $y$ premiers entre eux. En effet si $d$ est leur pgcd, on peut écrire $x = dx'$ et $y = dy'$ où $x'$ et $y'$ sont premiers entre eux. Alors $d^2(x'^2+y'^2) = z^2$. Ainsi $d$ divise $z$ et on s'est ramené à l'équation $x'^2+y'^2 = z'^2$ où $x'$, $y'$ et $z'$ sont deux à deux premiers entre eux. Ainsi $x'$ et $y'$ ne peuvent pas être tous les deux pairs. De plus, ils ne peuvent pas être tous les deux impairs. En effet, dans ce cas on aurait $x'^2+y'^2 \equiv 2\,[4]$ alors que $z'^2$ est un carré et ne peut donc être congru à 2 modulo 4. Finalement on peut se ramener à chercher des solutions sous la forme $(x,y,z)$ où $x$, $y$ et $z$ sont deux à deux premiers entre eux, $x$ est impair et $y$ est pair (et dans ce cas $z$ est également impair). Le problème est donc ramené

à ce dernier cas :

**Théorème 16** *Si (x,y,z) est une solution entière à l'équation de Pythagore, ave x, y et z premiers entre eux deux à deux, x impair et y pair, il existe r et s deux entiers tels que* $x = r^2 - s^2$, $y = 2rs$ *et* $z = r^2 + s^2$.

Preuve : On a $x^2 + y^2 = z^2$ et on sait que $z^2 - x^2 = (z - x)(z + x)$, donc $y^2 = (z - x)(z + x)$. Or comme $x$ est impair et $y$ pair, $z$ est impair, et donc $z - x$ et $z + x$ sont pairs tous les deux. Posons donc $z - x = 2l$ et $z + x = 2q$ avec $l$ et $q$ entiers. Comme $y$ est pair on peut aussi l'écrire $y = 2y'$ avec $y'$ entier. L'équation devient donc $y'^2 = lq$. Cette dernière équation doit pouvoir nous apprendre des choses sur $l$ et $q$, cependant on en connaît trop peu sur eux. Ils serait par exemple intéressant de voir s'ils sont premiers entre eux. Or on a $2z = (z - x) + (z + x)$ et $2x = (z + x) - (z - x)$, donc $x = q - l$ et $z = l + q$. Le pgcd de $l$ et $q$ divise donc à la fois $x$ et $y$. Comme $x$ et $y$ sont premiers entre eux, ce pgcd vaut 1 et donc $l$ et $q$ sont premiers entre eux.
Nous allons maintenant avoir besoin d'un résultat intermédiaire :

**Lemme 2** *Soient l et q deux entiers premier entre eux. Si lq est un carré, alors l et q sont tous les deux des carrés.*

Preuve du lemme : C'est presque immédiat en regardant les décomposition en facteurs premiers. En effet, un entier est un carré si et seulement si sa valuation en chaque nombre premier est paire. Or comme $l$ et $q$ sont premiers entre eux, tout nombre premier divisant $l$ ne divise pas $q$ et réciproquement. Cela signifie que si $p$ est un nombre premier divisant $n$, on a soit $v_p(l) = v_p(n)$, soit $v_p(q) = v_p(n)$. Ainsi la valuation de $l$ en chaque nombre premier est soit nulle, soit paire, et de même pour $q$. $l$ et $q$ sont donc des carrés.
Remarque : Ce résultat n'est plus vrai si $l$ et $q$ ne sont plus supposés premiers entre eux (prendre $l = 6$ et $q = 6$ par exemple).

Retour à la preuve du théorème : On peut donc écrire $l = s^2$ et $q = r^2$, et on a bien $x = r^2 - s^2$, $y = 2rs$ et $z = r^2 + s^2$.

On peut vérifier réciproquement que tous les triplets de la forme donnée dans le théorème sont solutions de l'équation de Pythagore, et que si $(x,y,z)$ est une solution, alors $(kx,ky,kz)$ est une solution pour tout $k$ entier. On peut donc conclure :

**Corollaire 7** *L'ensemble des solutions de l'équation* $x^2 + y^2 = z^2$ *est*

$$\{(k(r^2 - s^2), 2krs, k(r^2 + s^2),\ (2krs, k(r^2 - s^2), k(r^2 + s^2),\ (k,r,s) \in \mathbb{Z}^3\}$$

On sait donc entièrement résoudre l'équation de Pythagore, on voit qu'il y a une infinité de solutions et ce résultat nous permet d'en fabriquer de très grandes très facilement. Prenons par exemple $r = 20$ et $s = 15$, on a une solution : $x = 175$, $y = 600$ et $z = 625$.

C'est cette équation avec $n$ quelconque au lieu de 2 : $x^n + y^n = z^n$ qui a occupé les mathématiciens jusqu'à nos jours. On sait depuis peu que pour $n \geq 3$ cette équation n'a pas de solution ave $x$, $y$ et $z$ tous non nuls. Il s'agit du théorème de Fermat-Wiles.

# 9 Conclusion.

Nous avons ici décrit les principaux objets de l'arithmétique, à savoir les congruences et les nombres premiers. Beaucoup de questions en arithmétique portent sur les nombres premiers. Deux théorèmes difficiles, démontrés au $XIX^e$ siècle précisent la répartition des nombres premiers. On a par exemple montré qu'il y a une infinité de nombre premiers, mais on pourrait très

bien se demander comment sont répartis ces nombres premiers dans des classes de congruences modulo un entier $n$. Le théorème de la progression arithmétique de Dirichlet nous dit que si $a$ et $n$ sont deux entiers premiers entre eux, il y a une infinité de nombres premiers congrus à $a$ modulo $n$. On peut aussi se demander si cette infinité de nombres premiers est "grande". Le "théorème des nombres premiers", démontré simultanément par Hadamard et La Vallée Poussin dit que si on note $N(n)$ le nombre de nombres premiers compris entre 1 et $n$, $N(n)$ est équivalent à $\frac{n}{\ln(n)}$ quand $n$ tend vers l'infini.

Par la suite, il est aussi intéressant d'étudier d'autres ensembles de nombres que les entiers. Par exemple si on pousse l'étude du problème des deux carrés : chercher les nombre entiers $n$ qui s'écrivent $a^2 + b^2$ avec $a$ et $b$ entiers. Il est alors tentant d'écrire $n = (a + ib)(a - ib)$ où $i$ est un nombre complexe vérifiant $i^2 = -1$. On se ramène alors à un problème de divisibilité dans l'ensemble des nombres complexes de la forme $a + ib$ avec $a$ et $b$ entiers. En fait cet ensemble a des propriétés tout à fait analogues à celles de $\mathbb{Z}$, et les théorèmes de Gauss et Bezout y sont vrais dans un contexte plus général. L'étude du théorème de Fermat demande aussi d'étudier des structures toujours plus générales : anneaux principaux, factoriels, de Dedekind etc ...