Arithmétique

Vidéo ■ partie 1. Division euclidienne et pgcd
Vidéo ■ partie 2. Théorème de Bézout
Vidéo ■ partie 3. Nombres premiers
Vidéo ■ partie 4. Congruences
Fiche d'exercices ♦ Arithmétique dans $\mathbb{Z}$

Préambule

Une motivation : l'arithmétique est au cœur du cryptage des communication. Pour crypter un message on commence par le transformer en un –ou plusieurs– nombres. Le processus de codage et décodage fait appel à plusieurs notions de ce chapitre :

- On choisit deux ***nombres premiers*** p et q que l'on garde secrets et on pose $n = p \times q$. Le principe étant que même connaissant n il est très difficile de retrouver p et q (qui sont des nombres ayant des centaines de chiffres).
- La clé secrète et la clé publique se calculent à l'aide de l'***algorithme d'Euclide*** et des ***coefficients de Bézout***.
- Les calculs de cryptage se feront ***modulo*** n.
- Le décodage fonctionne grâce à une variante du ***petit théorème de Fermat***.

1. Division euclidienne et pgcd

1.1. Divisibilité et division euclidienne

Définition 1.
Soient $a, b \in \mathbb{Z}$. On dit que b ***divise*** a et on note $b|a$ s'il existe $q \in \mathbb{Z}$ tel que

$$\boxed{a = bq.}$$

Exemple 1.

- $7|21$; $6|48$; a est pair si et seulement si $2|a$.
- Pour tout $a \in \mathbb{Z}$ on a $a|0$ et aussi $1|a$.
- Si $a|1$ alors $a = +1$ ou $a = -1$.
- $(a|b \text{ et } b|a) \implies b = \pm a$
- $(a|b \text{ et } b|c) \implies a|c$
- $(a|b \text{ et } a|c) \implies a|b+c$

Théorème 1 (Division euclidienne)**.**
Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N} \setminus \{0\}$. Il **existe** *des entiers $q, r \in \mathbb{Z}$ tels que*

$$\boxed{a = bq + r \qquad et \qquad 0 \leqslant r < b}$$

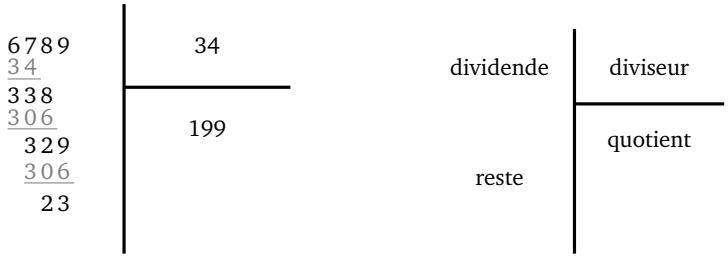
De plus q et r sont **uniques**.

Terminologie : q est le ***quotient*** et r est le ***reste***.
Nous avons donc l'équivalence : $r = 0$ si et seulement si b divise a.

Exemple 2.
Pour calculer q et r on pose la division « classique ». Si $a = 6789$ et $b = 34$ alors

$$6789 = 34 \times 199 + 23$$

On a bien $0 \leqslant 23 < 34$ (sinon c'est que l'on n'a pas été assez loin dans les calculs).



Démonstration.
Existence. On peut supposer $a \geqslant 0$ pour simplifier. Soit $\mathcal{N} = \{n \in \mathbb{N} \mid bn \leqslant a\}$. C'est un ensemble non vide car $n = 0 \in \mathcal{N}$. De plus pour $n \in \mathcal{N}$, on a $n \leqslant a$. Il y a donc un nombre fini d'éléments dans $\mathcal{N}$, notons $q = \max \mathcal{N}$ le plus grand élément.
Alors $qb \leqslant a$ car $q \in \mathcal{N}$, et $(q+1)b > a$ car $q+1 \notin \mathcal{N}$, donc

$$qb \leqslant a < (q+1)b = qb + b.$$

On définit alors $r = a - qb$, r vérifie alors $0 \leqslant r = a - qb < b$.
Unicité. Supposons que q', r' soient deux entiers qui vérifient les conditions du théorème. Tout d'abord $a = bq + r = bq' + r'$ et donc $b(q - q') = r' - r$. D'autre part $0 \leqslant r' < b$ et $0 \leqslant r < b$ donc $-b < r' - r < b$ (notez au passage la manipulation des inégalités). Mais $r' - r = b(q - q')$ donc on obtient $-b < b(q - q') < b$. On peut diviser par $b > 0$ pour avoir $-1 < q - q' < 1$. Comme $q - q'$ est un entier, la seule possibilité est $q - q' = 0$ et donc $q = q'$. Repartant de $r' - r = b(q - q')$ on obtient maintenant $r = r'$.

□

1.2. pgcd de deux entiers

Définition 2.
Soient $a, b \in \mathbb{Z}$ deux entiers, non tous les deux nuls. Le plus grand entier qui divise à la fois a et b s'appelle le ***plus grand diviseur commun*** de a, b et se note $\text{pgcd}(a, b)$.

Exemple 3.
- $\text{pgcd}(21, 14) = 7$, $\text{pgcd}(12, 32) = 4$, $\text{pgcd}(21, 26) = 1$.
- $\text{pgcd}(a, ka) = a$, pour tout $k \in \mathbb{Z}$ et $a \geqslant 0$.
- Cas particuliers. Pour tout $a \geqslant 0$: $\text{pgcd}(a, 0) = a$ et $\text{pgcd}(a, 1) = 1$.

1.3. Algorithme d'Euclide

Lemme 1.
Soient $a, b \in \mathbb{N}^*$. Écrivons la division euclidienne $a = bq + r$. Alors

$$\boxed{\text{pgcd}(a, b) = \text{pgcd}(b, r)}$$

En fait on a même $\text{pgcd}(a, b) = \text{pgcd}(b, a - qb)$ pour tout $q \in \mathbb{Z}$. Mais pour optimiser l'algorithme d'Euclide on applique le lemme avec q le quotient.

Démonstration. Nous allons montrer que les diviseurs de a et de b sont exactement les mêmes que les diviseurs de b et r. Cela impliquera le résultat car les plus grands diviseurs seront bien sûr les mêmes.
- Soit d un diviseur de a et de b. Alors d divise b donc aussi bq, en plus d divise a donc d divise $a - bq = r$.

- Soit d un diviseur de b et de r. Alors d divise aussi $bq + r = a$.

□

Algorithme d'Euclide.
On souhaite calculer le pgcd de $a, b \in \mathbb{N}^*$. On peut supposer $a \geqslant b$. On calcule des divisions euclidiennes successives. Le pgcd sera le dernier reste non nul.

- division de a par b, $a = bq_1 + r_1$. Par le lemme 1, $\text{pgcd}(a,b) = \text{pgcd}(b, r_1)$ et si $r_1 = 0$ alors $\text{pgcd}(a,b) = b$ sinon on continue :
- $b = r_1 q_2 + r_2$, $\quad \text{pgcd}(a,b) = \text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2)$,
- $r_1 = r_2 q_3 + r_3$, $\quad \text{pgcd}(a,b) = \text{pgcd}(r_2, r_3)$,
- $\dots$
- $r_{k-2} = r_{k-1} q_k + r_k$, $\text{pgcd}(a,b) = \text{pgcd}(r_{k-1}, r_k)$,
- $r_{k-1} = r_k q_k + 0$. $\text{pgcd}(a,b) = \text{pgcd}(r_k, 0) = r_k$.

Comme à chaque étape le reste est plus petit que le quotient on sait que $0 \leqslant r_{i+1} < r_i$. Ainsi l'algorithme se termine car nous sommes sûrs d'obtenir un reste nul, les restes formant une suite décroissante d'entiers positifs ou nuls : $b > r_1 > r_2 > \cdots \geqslant 0$.

Exemple 4.
Calculons le pgcd de $a = 600$ et $b = 124$.

$$\begin{array}{rcrcrcr} 600 & = & 124 & \times & 4 & + & 104 \\ 124 & = & 104 & \times & 1 & + & 20 \\ 104 & = & 20 & \times & 5 & + & 4 \\ 20 & = & 4 & \times & 5 & + & 0 \end{array}$$

Ainsi $\text{pgcd}(600, 124) = 4$.

Voici un exemple plus compliqué :

Exemple 5.
Calculons $\text{pgcd}(9945, 3003)$.

$$\begin{array}{rcrcrcr} 9945 & = & 3003 & \times & 3 & + & 936 \\ 3003 & = & 936 & \times & 3 & + & 195 \\ 936 & = & 195 & \times & 4 & + & 156 \\ 195 & = & 156 & \times & 1 & + & 39 \\ 156 & = & 39 & \times & 4 & + & 0 \end{array}$$

Ainsi $\text{pgcd}(9945, 3003) = 39$.

1.4. Nombres premiers entre eux

Définition 3.
Deux entiers a, b sont ***premiers entre eux*** si $\text{pgcd}(a,b) = 1$.

Exemple 6.
Pour tout $a \in \mathbb{Z}$, a et $a+1$ sont premiers entre eux. En effet soit d un diviseur commun à a et à $a+1$. Alors d divise aussi $a + 1 - a$. Donc d divise 1 mais alors $d = -1$ ou $d = +1$. Le plus grand diviseur de a et $a+1$ est donc 1. Et donc $\text{pgcd}(a, a+1) = 1$.

Si deux entiers ne sont pas premiers entre eux, on peut s'y ramener en divisant par leur pgcd :

Exemple 7.
Pour deux entiers quelconques $a, b \in \mathbb{Z}$, notons $d = \text{pgcd}(a,b)$. La décomposition suivante est souvent utile :

$$\left\{ \begin{array}{rcl} a & = & a'd \\ b & = & b'd \end{array} \right. \quad \text{avec} \quad a', b' \in \mathbb{Z} \text{ et } \text{pgcd}(a', b') = 1$$

Mini-exercices.

1. Écrire la division euclidienne de 111 111 par $20xx$, où $20xx$ est l'année en cours.
2. Montrer qu'un diviseur positif de 10 008 et de 10 014 appartient nécessairement à $\{1, 2, 3, 6\}$.

3. Calculer $\text{pgcd}(560, 133)$, $\text{pgcd}(12\,121, 789)$, $\text{pgcd}(99\,999, 1110)$.
4. Trouver tous les entiers $1 \leqslant a \leqslant 50$ tels que a et 50 soient premiers entre eux. Même question avec 52.

2. Théorème de Bézout

2.1. Théorème de Bézout

Théorème 2 (Théorème de Bézout)**.**
Soient a, b des entiers. Il existe des entiers $u, v \in \mathbb{Z}$ tels que

$$\boxed{au + bv = \text{pgcd}(a, b)}$$

La preuve découle de l'algorithme d'Euclide. Les entiers u, v ne sont pas uniques. Les entiers u, v sont des ***coefficients de Bézout***. Ils s'obtiennent en « remontant » l'algorithme d'Euclide.

Exemple 8.
Calculons les coefficients de Bézout pour $a = 600$ et $b = 124$. Nous reprenons les calculs effectués pour trouver $\text{pgcd}(600, 124) = 4$. La partie gauche est l'algorithme d'Euclide. La partie droite s'obtient de *bas en haut*. On exprime le pgcd à l'aide de la dernière ligne où le reste est non nul. Puis on remplace le reste de la ligne précédente, et ainsi de suite jusqu'à arriver à la première ligne.

$$\begin{array}{rcl} 600 = 124 \times 4 + 104 & & 4 = \left[\begin{array}{l} 600 \times 6 + 124 \times (-29) \\ 124 \times (-5) + (600 - 124 \times 4) \times 6 \end{array}\right. \\ 124 = 104 \times 1 + 20 & & 4 = \left[\begin{array}{l} 124 \times (-5) + 104 \times 6 \\ 104 - (124 - 104 \times 1) \times 5 \end{array}\right. \\ 104 = 20 \times 5 + 4 & & 4 = \left[\begin{array}{l} 104 - 20 \times 5 \end{array}\right. \\ 20 = 4 \times 5 + 0 & & \end{array}$$

Ainsi pour $u = 6$ et $v = -29$ alors $600 \times 6 + 124 \times (-29) = 4$.

Remarque.
- Soignez vos calculs et leur présentation. C'est un algorithme : vous devez aboutir au bon résultat ! Dans la partie droite, il faut à chaque ligne bien la reformater. Par exemple $104-(124-104\times1)\times5$ se réécrit en $124\times(-5)+104\times6$ afin de pouvoir remplacer ensuite 104.
- N'oubliez pas de vérifier vos calculs ! C'est rapide et vous serez certains que vos calculs sont exacts. Ici on vérifie à la fin que $600 \times 6 + 124 \times (-29) = 4$.

Exemple 9.
Calculons les coefficients de Bézout correspondant à $\text{pgcd}(9945, 3003) = 39$.

$$\begin{array}{rcl} 9945 = 3003 \times 3 + 936 & & 39 = 9945 \times (-16) + 3003 \times 53 \\ 3003 = 936 \times 3 + 195 & & 39 = \cdots \\ 936 = 195 \times 4 + 156 & & 39 = \cdots \\ 195 = 156 \times 1 + 39 & & 39 = 195 - 156 \times 1 \\ 156 = 39 \times 4 + 0 & & \end{array}$$

À vous de finir les calculs. On obtient $9945 \times (-16) + 3003 \times 53 = 39$.

2.2. Corollaires du théorème de Bézout

Corollaire 1.
Si $d|a$ et $d|b$ alors $d|\text{pgcd}(a, b)$.

Exemple : $4|16$ et $4|24$ donc 4 doit diviser $\text{pgcd}(16, 24)$ qui effectivement vaut 8.

Démonstration. Comme $d|au$ et $d|bv$ donc $d|au+bv$. Par le théorème de Bézout $d|\text{pgcd}(a,b)$. □

Corollaire 2.
*Soient a,b deux entiers. a et b sont premiers entre eux **si et seulement si** il existe $u,v\in\mathbb{Z}$ tels que*

$$\boxed{au+bv=1}$$

Démonstration. Le sens ⇒ est une conséquence du théorème de Bézout.
Pour le sens ⇐ on suppose qu'il existe u,v tels que $au+bv=1$. Comme $\text{pgcd}(a,b)|a$ alors $\text{pgcd}(a,b)|au$. De même $\text{pgcd}(a,b)|bv$. Donc $\text{pgcd}(a,b)|au+bv=1$. Donc $\text{pgcd}(a,b)=1$. □

Remarque.
Si on trouve deux entiers u',v' tels que $au'+bv'=d$, cela n'implique **pas** que $d=\text{pgcd}(a,b)$. On sait seulement alors que $\text{pgcd}(a,b)|d$. Par exemple $a=12$, $b=8$; $12\times1+8\times3=36$ et $\text{pgcd}(a,b)=4$.

Corollaire 3 (Lemme de Gauss)**.**
Soient $a,b,c\in\mathbb{Z}$.

$$\boxed{\textit{Si}\quad a|bc\quad\textit{et}\quad \text{pgcd}(a,b)=1\quad\textit{alors}\quad a|c}$$

Exemple : si $4|7\times c$, et comme 4 et 7 sont premiers entre eux, alors $4|c$.

Démonstration. Comme $\text{pgcd}(a,b)=1$ alors il existe $u,v\in\mathbb{Z}$ tels que $au+bv=1$. On multiplie cette égalité par c pour obtenir $acu+bcv=c$. Mais $a|acu$ et par hypothèse $a|bcv$ donc a divise $acu+bcv=c$. □

2.3. Équations $ax+by=c$

Proposition 1.
Considérons l'équation

$$ax+by=c \tag{E}$$

où $a,b,c\in\mathbb{Z}$.

1. *L'équation (E) possède des solutions $(x,y)\in\mathbb{Z}^2$ si et seulement si $\text{pgcd}(a,b)|c$.*
2. *Si $\text{pgcd}(a,b)|c$ alors il existe même une infinité de solutions entières et elles sont exactement les $(x,y)=(x_0+\alpha k, y_0+\beta k)$ avec $x_0,y_0,\alpha,\beta\in\mathbb{Z}$ fixés et k parcourant $\mathbb{Z}$.*

Le premier point est une conséquence du théorème de Bézout. Nous allons voir sur un exemple comment prouver le second point et calculer explicitement les solutions. Il est bon de refaire toutes les étapes de la démonstration à chaque fois.

Exemple 10.
Trouver les solutions entières de

$$161x+368y=115 \tag{E}$$

- **Première étape. Y a-t-il des solutions ? L'algorithme d'Euclide.** On effectue l'algorithme d'Euclide pour calculer le pgcd de $a=161$ et $b=368$.

$$\begin{aligned} 368 &= 161\times 2+46\\ 161 &= 46\times 3+23\\ 46 &= 23\times 2+0 \end{aligned}$$

  Donc $\text{pgcd}(368,161)=23$. Comme $115=5\times23$ alors $\text{pgcd}(368,161)|115$. Par le théorème de Bézout, l'équation (E) admet des solutions entières.
- **Deuxième étape. Trouver une solution particulière : la remontée de l'algorithme d'Euclide.** On effectue la remontée de l'algorithme d'Euclide pour calculer les coefficients de Bézout.

$$\begin{aligned} 368 &= 161\times 2+46\\ 161 &= 46\times 3+23\\ 46 &= 23\times 2+0 \end{aligned}$$

$$\begin{aligned} 23 &= \left|\begin{array}{l} 161\times 7+368\times(-3)\\ 161+(368-2\times161)\times(-3)\end{array}\right.\\ 23 &= 161-3\times46 \end{aligned}$$

On trouve donc $161\times 7+368\times(-3)=23$. Comme $115=5\times 23$ en multipliant par 5 on obtient :

$$161\times 35+368\times(-15)=115$$

Ainsi $(x_0,y_0)=(35,-15)$ est une ***solution particulière*** de (E).

- **Troisième étape. Recherche de toutes les solutions.** Soit $(x,y)\in\mathbb{Z}^2$ une solution de (E). Nous savons que (x_0,y_0) est aussi solution. Ainsi :

$$161x+368y=115 \quad \text{et} \quad 161x_0+368y_0=115$$

(on n'a aucun intérêt à remplacer x_0 et y_0 par leurs valeurs). La différence de ces deux égalités conduit à

$$\begin{aligned} & 161\times(x-x_0)+368\times(y-y_0)=0\\ \Longrightarrow\quad & 23\times 7\times(x-x_0)+23\times 16\times(y-y_0)=0\\ \Longrightarrow\quad & 7(x-x_0)=-16(y-y_0) \qquad (*)\end{aligned}$$

Nous avons simplifié par 23 qui est le pgcd de 161 et 368. (Attention, n'oubliez surtout pas cette simplification, sinon la suite du raisonnement serait fausse.)
Ainsi $7|16(y-y_0)$, or $\text{pgcd}(7,16)=1$ donc par le lemme de Gauss $7|y-y_0$. Il existe donc $k\in\mathbb{Z}$ tel que $y-y_0=7\times k$. Repartant de l'équation $(*)$: $7(x-x_0)=-16(y-y_0)$. On obtient maintenant $7(x-x_0)=-16\times 7\times k$. D'où $x-x_0=-16k$. (C'est le même k pour x et pour y.) Nous avons donc $(x,y)=(x_0-16k,y_0+7k)$. Il n'est pas dur de voir que tout couple de cette forme est solution de l'équation (E). Il reste donc juste à substituer (x_0,y_0) par sa valeur et nous obtenons :

Les solutions entières de $161x+368y=115$ sont les $(x,y)=(35-16k,-15+7k)$, k parcourant $\mathbb{Z}$.

Pour se rassurer, prenez une valeur de k au hasard et vérifiez que vous obtenez bien une solution de l'équation.

2.4. ppcm

Définition 4.
Le ppcm(a,b) (***plus petit multiple commun***) est le plus petit entier $\geqslant 0$ divisible par a et par b.

Par exemple $\text{ppcm}(12,9)=36$.
Le pgcd et le ppcm sont liés par la formule suivante :

Proposition 2.
Si a,b sont des entiers (non tous les deux nuls) alors

$$\text{pgcd}(a,b)\times ppcm(a,b)=|ab|$$

Démonstration. Posons $d=\text{pgcd}(a,b)$ et $m=\frac{|ab|}{\text{pgcd}(a,b)}$. Pour simplifier on suppose $a>0$ et $b>0$. On écrit $a=da'$ et $b=db'$. Alors $ab=d^2a'b'$ et donc $m=da'b'$. Ainsi $m=ab'=a'b$ est un multiple de a et de b.
Il reste à montrer que c'est le plus petit multiple. Si n est un autre multiple de a et de b alors $n=ka=\ell b$ donc $kda'=\ell db'$ et $ka'=\ell b'$. Or $\text{pgcd}(a',b')=1$ et $a'|\ell b'$ donc $a'|\ell$. Donc $a'b|\ell b$ et ainsi $m=a'b|\ell b=n$. □

Voici un autre résultat concernant le ppcm qui se démontre en utilisant la décomposition en facteurs premiers :

Proposition 3.
Si $a|c$ et $b|c$ alors $ppcm(a,b)|c$.

Il serait faux de penser que $ab|c$. Par exemple $6|36$, $9|36$ mais 6×9 ne divise pas 36. Par contre $\text{ppcm}(6,9)=18$ divise bien 36.

Mini-exercices.

1. Calculer les coefficients de Bézout correspondant à $\text{pgcd}(560,133)$, $\text{pgcd}(12\,121,789)$.
2. Montrer à l'aide d'un corollaire du théorème de Bézout que $\text{pgcd}(a,a+1)=1$.
3. Résoudre les équations : $407x+129y=1$; $720x+54y=6$; $216x+92y=8$.
4. Trouver les couples (a,b) vérifiant $\text{pgcd}(a,b)=12$ et $\text{ppcm}(a,b)=360$.

3. Nombres premiers

Les nombres premiers sont –en quelque sorte– les briques élémentaires des entiers : tout entier s'écrit comme produit de nombres premiers.

3.1. Une infinité de nombres premiers

Définition 5.
Un ***nombre premier*** p est un entier $\geqslant 2$ dont les seuls diviseurs positifs sont 1 et p.

Exemples : $2, 3, 5, 7, 11$ sont premiers, $4 = 2 \times 2$, $6 = 2 \times 3$, $8 = 2 \times 4$ ne sont pas premiers.

Lemme 2.
Tout entier $n \geqslant 2$ admet un diviseur qui est un nombre premier.

Démonstration. Soit $\mathscr{D}$ l'ensemble des diviseurs de n qui sont $\geqslant 2$:

$$\mathscr{D} = \{k \geqslant 2 \mid \ k|n\}.$$

L'ensemble $\mathscr{D}$ est non vide (car $n \in \mathscr{D}$), notons alors $p = \min \mathscr{D}$.
Supposons, par l'absurde, que p ne soit pas un nombre premier alors p admet un diviseur q tel que $1 < q < p$ mais alors q est aussi un diviseur de n et donc $q \in \mathscr{D}$ avec $q < p$. Ce qui donne une contradiction car p est le minimum.
Conclusion : p est un nombre premier. Et comme $p \in \mathscr{D}$, p divise n. □

Proposition 4.
Il existe une infinité de nombres premiers.

Démonstration. Par l'absurde, supposons qu'il n'y ait qu'un nombre fini de nombres premiers que l'on note $p_1 = 2$, $p_2 = 3$, $p_3, \ldots, p_n$. Considérons l'entier $N = p_1 \times p_2 \times \cdots \times p_n + 1$. Soit p un diviseur premier de N (un tel p existe par le lemme précédent), alors d'une part p est l'un des entiers p_i donc $p|p_1 \times \cdots \times p_n$, d'autre part $p|N$ donc p divise la différence $N - p_1 \times \cdots \times p_n = 1$. Cela implique que $p = 1$, ce qui contredit que p soit un nombre premier.
Cette contradiction nous permet de conclure qu'il existe une infinité de nombres premiers. □

3.2. Eratosthène et Euclide

Comment trouver les nombres premiers ? Le ***crible d'Eratosthène*** permet de trouver les premiers nombres premiers. Pour cela on écrit les premiers entiers : pour notre exemple de 2 à 25.

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Rappelons-nous qu'un diviseur positif d'un entier n est inférieur ou égal à n. Donc 2 ne peut avoir comme diviseurs que 1 et 2 et est donc premier. On entoure 2. Ensuite on raye (ici en grisé) tous les multiples suivants de 2 qui ne seront donc pas premiers (car divisible par 2) :

[2] 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Le premier nombre restant de la liste est 3 et est nécessairement premier : il n'est pas divisible par un diviseur plus petit (sinon il serait rayé). On entoure 3 et on raye tous les multiples de 3 (6, 9, 12, ...).

[2] [3] 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Le premier nombre restant est 5 et est donc premier. On raye les multiples de 5.

[2] [3] 4 [5] 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

7 est donc premier, on raye les multiples de 7 (ici pas de nouveaux nombres à barrer). Ainsi de suite : $11, 13, 17, 19, 23$ sont premiers.

[2] [3] 4 [5] 6 [7] 8 9 10 [11] 12 [13] 14 15 16 [17] 18 [19] 20 21 22 [23]

Remarque.
Si un nombre n n'est pas premier alors un de ses facteurs est $\leqslant \sqrt{n}$. En effet si $n = a \times b$ avec $a, b \geqslant 2$ alors $a \leqslant \sqrt{n}$ ou $b \leqslant \sqrt{n}$ (réfléchissez par l'absurde !). Par exemple pour tester si un nombre $\leqslant 100$ est premier il suffit de tester les diviseurs $\leqslant 10$. Et comme il suffit de tester les diviseurs premiers, il suffit en fait de tester la divisibilité par $2, 3, 5$ et 7. Exemple : 89 n'est pas divisible par $2, 3, 5, 7$ et est donc un nombre premier.

Proposition 5 (Lemme d'Euclide)**.**
Soit p un nombre premier. Si $p|ab$ alors $p|a$ ou $p|b$.

Démonstration. Si p ne divise pas a alors p et a sont premiers entre eux (en effet les diviseurs de p sont 1 et p, mais seul 1 divise aussi a, donc $\text{pgcd}(a, p) = 1$). Ainsi par le lemme de Gauss $p|b$. □

Exemple 11.
Si p est un nombre premier, $\sqrt{p}$ n'est pas un nombre rationnel.
La preuve se fait par l'absurde : écrivons $\sqrt{p} = \frac{a}{b}$ avec $a \in \mathbb{Z}, b \in \mathbb{N}^*$ et $\text{pgcd}(a, b) = 1$. Alors $p = \frac{a^2}{b^2}$ donc $pb^2 = a^2$. Ainsi $p|a^2$ donc par le lemme d'Euclide $p|a$. On peut alors écrire $a = pa'$ avec a' un entier. De l'équation $pb^2 = a^2$ on tire alors $b^2 = pa'^2$. Ainsi $p|b^2$ et donc $p|b$. Maintenant $p|a$ et $p|b$ donc a et b ne sont pas premiers entre eux. Ce qui contredit $\text{pgcd}(a, b) = 1$. Conclusion $\sqrt{p}$ n'est pas rationnel.

3.3. Décomposition en facteurs premiers

Théorème 3.
Soit $n \geqslant 2$ un entier. Il existe des nombres premiers $p_1 < p_2 < \cdots < p_r$ et des exposants entiers $\alpha_1, \alpha_2, \ldots, \alpha_r \geqslant 1$ tels que :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}.$$

De plus les p_i et les α_i $(i = 1, \ldots, r)$ sont uniques.

Exemple : $24 = 2^3 \times 3$ est la décomposition en facteurs premiers. Par contre $36 = 2^2 \times 9$ n'est pas la décomposition en facteurs premiers, c'est $2^2 \times 3^2$.

Remarque.
La principale raison pour laquelle on choisit de dire que 1 n'est pas un nombre premier, c'est que sinon il n'y aurait plus unicité de la décomposition : $24 = 2^3 \times 3 = 1 \times 2^3 \times 3 = 1^2 \times 2^3 \times 3 = \cdots$

Démonstration.
Existence. Nous allons démontrer l'existence de la décomposition par une récurrence sur n.
L'entier $n = 2$ est déjà décomposé. Soit $n \geqslant 3$, supposons que tout entier $< n$ admette une décomposition en facteurs premiers. Notons p_1 le plus petit nombre premier divisant n (voir le lemme 2). Si n est un nombre premier alors $n = p_1$ et c'est fini. Sinon on définit l'entier $n' = \frac{n}{p_1} < n$ et on applique notre hypothèse de récurrence à n' qui admet une décomposition en facteurs premiers. Alors $n = p_1 \times n'$ admet aussi une décomposition.

Unicité. Nous allons démontrer qu'une telle décomposition est unique en effectuant cette fois une récurrence sur la somme des exposants $\sigma = \sum_{i=1}^{r} \alpha_i$.
Si $\sigma = 1$ cela signifie $n = p_1$ qui est bien l'unique écriture possible.
Soit $\sigma \geqslant 2$. On suppose que les entiers dont la somme des exposants est $< \sigma$ ont une unique décomposition. Soit n un entier dont la somme des exposants vaut σ. Écrivons le avec deux décompositions :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r} = q_1^{\beta_1} \times q_2^{\beta_2} \times \cdots \times q_s^{\beta_s}.$$

(On a $p_1 < p_2 < \cdots$ et $q_1 < q_2 < \cdots$.)
Si $p_1 < q_1$ alors $p_1 < q_j$ pour tous les $j = 1, \ldots, s$. Ainsi p_1 divise $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r} = n$ mais ne divise pas $q_1^{\beta_1} \times q_2^{\beta_2} \times \cdots \times q_s^{\beta_s} = n$. Ce qui est absurde. Donc $p_1 \geqslant q_1$.
Si $p_1 > q_1$ un même raisonnement conduit aussi à une contradiction. On conclut que $p_1 = q_1$. On pose alors

$$n' = \frac{n}{p_1} = p_1^{\alpha_1 - 1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r} = q_1^{\beta_1 - 1} \times q_2^{\beta_2} \times \cdots \times q_s^{\beta_s}$$

L'hypothèse de récurrence qui s'applique à n' implique que ces deux décompositions sont les mêmes. Ainsi $r = s$ et $p_i = q_i$, $\alpha_i = \beta_i$, $i = 1, \ldots, r$. □

Exemple 12.

$$504 = 2^3 \times 3^2 \times 7, \quad 300 = 2^2 \times 3 \times 5^2.$$

Pour calculer le pgcd on réécrit ces décompositions :

$$504 = 2^3 \times 3^2 \times 5^0 \times 7^1, \quad 300 = 2^2 \times 3^1 \times 5^2 \times 7^0.$$

Le pgcd est le nombre obtenu en prenant le plus petit exposant de chaque facteur premier :

$$\text{pgcd}(504, 300) = 2^2 \times 3^1 \times 5^0 \times 7^0 = 12.$$

Pour le ppcm on prend le plus grand exposant de chaque facteur premier :

$$\text{ppcm}(504, 300) = 2^3 \times 3^2 \times 5^2 \times 7^1 = 12\,600$$

Mini-exercices.

1. Montrer que $n! + 1$ n'est divisible par aucun des entiers $2, 3, \ldots, n$. Est-ce toujours un nombre premier ?
2. Trouver tous les nombres premiers $\leqslant 103$.
3. Décomposer $a = 2\,340$ et $b = 15\,288$ en facteurs premiers. Calculer leur pgcd et leur ppcm.
4. Décomposer 48 400 en produit de facteurs premiers. Combien 48 400 admet-il de diviseurs ?
5. Soient $a, b \geqslant 0$. À l'aide de la décomposition en facteurs premiers, reprouver la formule $\text{pgcd}(a, b) \times \text{ppcm}(a, b) = a \times b$.

4. Congruences

4.1. Définition

Définition 6.
Soit $n \geqslant 2$ un entier. On dit que a est ***congru*** à b ***modulo*** n, si n divise $b - a$. On note alors

$$a \equiv b \pmod{n}.$$

On note aussi parfois $a = b \pmod{n}$ ou $a \equiv b[n]$. Une autre formulation est

$$\boxed{a \equiv b \pmod{n} \iff \exists k \in \mathbb{Z} \quad a = b + kn.}$$

Remarquez que n divise a si et seulement si $a \equiv 0 \pmod{n}$.

Proposition 6.

1. *La relation « congru modulo n » est une relation d'équivalence :*
   - $a \equiv a \pmod{n}$,
   - *si* $a \equiv b \pmod{n}$ *alors* $b \equiv a \pmod{n}$,
   - *si* $a \equiv b \pmod{n}$ *et* $b \equiv c \pmod{n}$ *alors* $a \equiv c \pmod{n}$.
2. *Si* $a \equiv b \pmod{n}$ *et* $c \equiv d \pmod{n}$ *alors* $a + c \equiv b + d \pmod{n}$.
3. *Si* $a \equiv b \pmod{n}$ *et* $c \equiv d \pmod{n}$ *alors* $a \times c \equiv b \times d \pmod{n}$.
4. *Si* $a \equiv b \pmod{n}$ *alors pour tout* $k \geqslant 0$, $a^k \equiv b^k \pmod{n}$.

Exemple 13.

- $15 \equiv 1 \pmod{7}$, $72 \equiv 2 \pmod{7}$, $3 \equiv -11 \pmod{7}$,
- $5x + 8 \equiv 3 \pmod{5}$ pour tout $x \in \mathbb{Z}$,
- $11^{20xx} \equiv 1^{20xx} \equiv 1 \pmod{10}$, où $20xx$ est l'année en cours.

Démonstration.

1. Utiliser la définition.
2. Idem.

3. Prouvons la propriété multiplicative : $a \equiv b \pmod{n}$ donc il existe $k \in \mathbb{Z}$ tel que $a = b + kn$ et $c \equiv d \pmod{n}$ donc il existe $\ell \in \mathbb{Z}$ tel que $c \equiv d + \ell n$. Alors $a \times c = (b+kn) \times (d+\ell n) = bd + (b\ell + dk + k\ell n)n$ qui est bien de la forme $bd + mn$ avec $m \in \mathbb{Z}$. Ainsi $ac \equiv bd \pmod{n}$.
4. C'est une conséquence du point précédent : avec $a = c$ et $b = d$ on obtient $a^2 \equiv b^2 \pmod{n}$. On continue par récurrence.

□

Exemple 14.
Critère de divisibilité par 9**.**

N est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

Pour prouver cela nous utilisons les congruences. Remarquons d'abord que $9|N$ équivaut à $N \equiv 0 \pmod{9}$ et notons aussi que $10 \equiv 1 \pmod{9}$, $10^2 \equiv 1 \pmod{9}$, $10^3 \equiv 1 \pmod{9}$,...
Nous allons donc calculer N modulo 9. Écrivons N en base 10 : $N = \underline{a_k \cdots a_2 a_1 a_0}$ (a_0 est le chiffre des unités, a_1 celui des dizaines,...) alors $N = 10^k a_k + \cdots + 10^2 a_2 + 10^1 a_1 + a_0$. Donc

$$\begin{aligned} N &= 10^k a_k + \cdots + 10^2 a_2 + 10^1 a_1 + a_0 \\ &\equiv a_k + \cdots + a_2 + a_1 + a_0 \pmod{9} \end{aligned}$$

Donc N est congru à la somme de ses chiffres modulo 9. Ainsi $N \equiv 0 \pmod{9}$ si et seulement si la somme des chiffres vaut 0 modulo 9.
Voyons cela sur un exemple : $N = 488\,889$. Ici $a_0 = 9$ est le chiffre des unités, $a_1 = 8$ celui des dizaines,... Cette écriture décimale signifie $N = 4 \cdot 10^5 + 8 \cdot 10^4 + 8 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10 + 9$.

$$\begin{aligned} N &= 4 \cdot 10^5 + 8 \cdot 10^4 + 8 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10 + 9 \\ &\equiv 4 + 8 + 8 + 8 + 8 + 9 \pmod{9} \\ &\equiv 45 \pmod{9} \qquad \text{et on refait la somme des chiffres de 45} \\ &\equiv 9 \pmod{9} \\ &\equiv 0 \pmod{9} \end{aligned}$$

Ainsi nous savons que 488 889 est divisible par 9 sans avoir effectué de division euclidienne.

Remarque.
Pour trouver un « bon » représentant de $a \pmod{n}$ on peut aussi faire la division euclidienne de a par n : $a = bn + r$ alors $a \equiv r \pmod{n}$ et $0 \leqslant r < n$.

Exemple 15.
Les calculs bien menés avec les congruences sont souvent très rapides. Par exemple on souhaite calculer $2^{21} \pmod{37}$ (plus exactement on souhaite trouver $0 \leqslant r < 37$ tel que $2^{21} \equiv r \pmod{37}$). Plusieurs méthodes :

1. On calcule 2^{21}, puis on fait la division euclidienne de 2^{21} par 37, le reste est notre résultat. C'est laborieux !
2. On calcule successivement les 2^k modulo 37 : $2^1 \equiv 2 \pmod{37}$, $2^2 \equiv 4 \pmod{37}$, $2^3 \equiv 8 \pmod{37}$, $2^4 \equiv 16 \pmod{37}$, $2^5 \equiv 32 \pmod{37}$. Ensuite on n'oublie pas d'utiliser les congruences : $2^6 \equiv 64 \equiv 27 \pmod{37}$. $2^7 \equiv 2 \cdot 2^6 \equiv 2 \cdot 27 \equiv 54 \equiv 17 \pmod{37}$ et ainsi de suite en utilisant le calcul précédent à chaque étape. C'est assez efficace et on peut raffiner : par exemple on trouve $2^8 \equiv 34 \pmod{37}$ mais donc aussi $2^8 \equiv -3 \pmod{37}$ et donc $2^9 \equiv 2 \cdot 2^8 \equiv 2 \cdot (-3) \equiv -6 \equiv 31 \pmod{37}$,...
3. Il existe une méthode encore plus efficace, on écrit l'exposant 21 en base 2 : $21 = 2^4 + 2^2 + 2^0 = 16 + 4 + 1$. Alors $2^{21} = 2^{16} \cdot 2^4 \cdot 2^1$. Et il est facile de calculer successivement chacun de ces termes car les exposants sont des puissances de 2. Ainsi $2^8 \equiv (2^4)^2 \equiv 16^2 \equiv 256 \equiv 34 \equiv -3 \pmod{37}$ et $2^{16} \equiv \left(2^8\right)^2 \equiv (-3)^2 \equiv 9 \pmod{37}$. Nous obtenons $2^{21} \equiv 2^{16} \cdot 2^4 \cdot 2^1 \equiv 9 \times 16 \times 2 \equiv 288 \equiv 29 \pmod{37}$.

4.2. Équation de congruence $ax \equiv b \pmod{n}$

Proposition 7.
Soit $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$ fixés et $n \geqslant 2$. Considérons l'équation $\boxed{ax \equiv b \pmod{n}}$ d'inconnue $x \in \mathbb{Z}$:

1. *Il existe des solutions si et seulement si $\text{pgcd}(a,n)|b$.*
2. *Les solutions sont de la forme $x = x_0 + \ell \frac{n}{\text{pgcd}(a,n)}$, $\ell \in \mathbb{Z}$ où x_0 est une solution particulière. Il existe donc $\text{pgcd}(a,n)$ classes de solutions.*

Exemple 16.
Résolvons l'équation $9x \equiv 6 \pmod{24}$. Comme $\text{pgcd}(9,24) = 3$ divise 6 la proposition ci-dessus nous affirme qu'il existe des solutions. Nous allons les calculer. (Il est toujours préférable de refaire rapidement les calculs que d'apprendre la formule). Trouver x tel que $9x \equiv 6 \pmod{24}$ est équivalent à trouver x et k tels que $9x = 6 + 24k$. Mis sous la forme $9x - 24k = 6$ il s'agit alors d'une équation que nous avons étudiée en détails (voir section 2.3). Il y a bien des solutions car $\text{pgcd}(9,24) = 3$ divise 6. En divisant par le pgcd on obtient l'équation équivalente :

$$3x - 8k = 2.$$

Pour le calcul du pgcd et d'une solution particulière nous utilisons normalement l'algorithme d'Euclide et sa remontée. Ici il est facile de trouver une solution particulière ($x_0 = 6, k_0 = 2$) à la main.
On termine comme pour les équations de la section 2.3. Si (x,k) est une solution de $3x - 8k = 2$ alors par soustraction on obtient $3(x - x_0) - 8(k - k_0) = 0$ et on trouve $x = x_0 + 8\ell$, avec $\ell \in \mathbb{Z}$ (le terme k ne nous intéresse pas). Nous avons donc trouvé les x qui sont solutions de $3x - 8k = 2$, ce qui équivaut à $9x - 24k = 6$, ce qui équivaut encore à $9x \equiv 6 \pmod{24}$. Les solutions sont de la forme $x = 6 + 8\ell$. On préfère les regrouper en 3 classes modulo 24 :

$$x_1 = 6 + 24m, \quad x_2 = 14 + 24m, \quad x_3 = 22 + 24m \quad \text{avec } m \in \mathbb{Z}.$$

Remarque.
Expliquons le terme de « classe » utilisé ici. Nous avons considérer ici que l'équation $9x \equiv 6 \pmod{24}$ est une équation d'entiers. On peut aussi considérer que $9, x, 6$ sont des classes d'équivalence modulo 24, et l'on noterait alors $\overline{9}\,\overline{x} = \overline{6}$. On trouverait comme solutions trois classes d'équivalence :

$$\overline{x_1} = \overline{6}, \quad \overline{x_2} = \overline{14}, \quad \overline{x_3} = \overline{22}.$$

Démonstration.

1.
$$\begin{aligned} & x \in \mathbb{Z} \text{ est un solution de l'équation } ax \equiv b \pmod{n} \\ \iff & \exists k \in \mathbb{Z} \quad ax = b + kn \\ \iff & \exists k \in \mathbb{Z} \quad ax - kn = b \\ \iff & \text{pgcd}(a,n)|b \quad \text{par la proposition 1} \end{aligned}$$

   Nous avons juste transformé notre équation $ax \equiv b \pmod{n}$ en une équation $ax - kn = b$ étudiée auparavant (voir section 2.3), seules les notations changent : $au + bv = c$ devient $ax - kn = b$.

2. Supposons qu'il existe des solutions. Nous allons noter $d = \text{pgcd}(a,n)$ et écrire $a = da'$, $n = dn'$ et $b = db'$ (car par le premier point $d|b$). L'équation $ax - kn = b$ d'inconnues $x, k \in \mathbb{Z}$ est alors équivalente à l'équation $a'x - kn' = b'$, notée $(\star)$. Nous savons résoudre cette équation (voir de nouveau la proposition 1), si (x_0, k_0) est une solution particulière de $(\star)$ alors on connaît tous les (x,k) solutions. En particulier $x = x_0 + \ell n'$ avec $\ell \in \mathbb{Z}$ (les k ne nous intéressent pas ici).
   Ainsi les solutions $x \in \mathbb{Z}$ sont de la forme $x = x_0 + \ell \frac{n}{\text{pgcd}(a,n)}$, $\ell \in \mathbb{Z}$ où x_0 est une solution particulière de $ax \equiv b \pmod{n}$. Et modulo n cela donne bien $\text{pgcd}(a,n)$ classes distinctes.

□

4.3. Petit théorème de Fermat

Théorème 4 (Petit théorème de Fermat)**.**
Si p est un nombre premier et $a \in \mathbb{Z}$ alors

$$\boxed{a^p \equiv a \pmod{p}}$$

Corollaire 4.
Si p ne divise pas a alors

$$\boxed{a^{p-1} \equiv 1 \pmod{p}}$$

Lemme 3.
p divise $\binom{p}{k}$ pour $1 \leqslant k \leqslant p-1$, c'est-à-dire $\binom{p}{k} \equiv 0 \pmod{p}$.

Démonstration. $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ donc $p! = k!(p-k)!\binom{p}{k}$. Ainsi $p | k!(p-k)!\binom{p}{k}$. Or comme $1 \leqslant k \leqslant p-1$ alors p ne divise pas $k!$ (sinon p divise l'un des facteurs de $k!$ mais il sont tous $< p$). De même p ne divise pas $(p-k)!$, donc par le lemme d'Euclide p divise $\binom{p}{k}$. □

Preuve du théorème. Nous le montrons par récurrence pour les $a \geqslant 0$.

- Si $a = 0$ alors $0 \equiv 0 \pmod{p}$.
- Fixons $a \geqslant 0$ et supposons que $a^p \equiv a \pmod{p}$. Calculons $(a+1)^p$ à l'aide de la formule du binôme de Newton :

$$(a+1)^p = a^p + \binom{p}{p-1}a^{p-1} + \binom{p}{p-2}a^{p-2} + \cdots + \binom{p}{1} + 1$$

Réduisons maintenant modulo p :

$$\begin{aligned}(a+1)^p &\equiv a^p + \binom{p}{p-1}a^{p-1} + \binom{p}{p-2}a^{p-2} + \cdots + \binom{p}{1} + 1 \pmod{p} \\ &\equiv a^p + 1 \pmod{p} \quad \text{grâce au lemme 3} \\ &\equiv a + 1 \pmod{p} \quad \text{à cause de l'hypothèse de récurrence}\end{aligned}$$

- Par le principe de récurrence nous avons démontré le petit théorème de Fermat pour tout $a \geqslant 0$. Il n'est pas dur d'en déduire le cas des $a \leqslant 0$.

□

Exemple 17.
Calculons $14^{3141} \pmod{17}$. Le nombre 17 étant premier on sait par le petit théorème de Fermat que $14^{16} \equiv 1 \pmod{17}$. Écrivons la division euclidienne de 3141 par 16 :

$$3141 = 16 \times 196 + 5.$$

Alors

$$\begin{aligned}14^{3141} &\equiv 14^{16\times 196+5} \equiv 14^{16\times 196} \times 14^5 \\ &\equiv \left(14^{16}\right)^{196} \times 14^5 \equiv 1^{196} \times 14^5 \\ &\equiv 14^5 \pmod{17}\end{aligned}$$

Il ne reste plus qu'à calculer 14^5 modulo 17. Cela peut se faire rapidement : $14 \equiv -3 \pmod{17}$ donc $14^2 \equiv (-3)^2 \equiv 9 \pmod{17}$, $14^3 \equiv 14^2 \times 14 \equiv 9 \times (-3) \equiv -27 \equiv 7 \pmod{17}$, $14^5 \equiv 14^2 \times 14^3 \equiv 9 \times 7 \equiv 63 \equiv 12 \pmod{17}$. Conclusion : $14^{3141} \equiv 14^5 \equiv 12 \pmod{17}$.

Mini-exercices.

1. Calculer les restes modulo 10 de $122 + 455$, 122×455, 122^{455}. Mêmes calculs modulo 11, puis modulo 12.
2. Prouver qu'un entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.
3. Calculer $3^{10} \pmod{23}$.
4. Calculer $3^{100} \pmod{23}$.

5. Résoudre les équations $3x \equiv 4 \pmod 7$, $4x \equiv 14 \pmod{30}$.

Auteurs du chapitre Arnaud Bodin, Benjamin Boutin, Pascal Romon