Chapitre 3

Arithmétique des entiers

Sommaire

3.1 Divisibilité et primalité 1
3.2 PGCD et théorème de Bézout 4
3.3 Décomposition en facteurs premiers 9
3.4 Congruences 10

Dans ce chapitre, on rappelle les bases de l'arithmétique, c'est-à-dire l'étude des nombres entiers et des notions de divisibilité et de nombre premier. Le chapitre suivant sera consacré à l'arithmétique des polynômes, qui généralise une grande partie des notions et résultats connus sur les nombres entiers.

Le mot « entier » sans précision désignera un élément de $\mathbb{Z}$, c'est-à-dire un nombre entier positif ou négatif. On parlera explicitement d'« entier naturel » ou simplement de « naturel » pour désigner un élément de $\mathbb{N}$, c'est-à-dire un entier positif ou nul.

3.1 Divisibilité et primalité

3.1 **Théorème (division euclidienne).** *Soient n un entier et p un entier naturel non nul ; il existe un unique couple d'entiers (q, r) satisfaisant :*

- $n = pq + r$;
- $0 \leq r < p$.

L'entier q est appelé le quotient *de n par p et l'entier naturel r est appelé le* reste *de n par p. On dit aussi que r est le* reste de n modulo p *ce que l'on note $n = r \bmod p$. La fonction qui au couple (n, p) associe le couple (q, r) (fonction de $\mathbb{Z} \times \mathbb{N}^*$ dans $\mathbb{Z} \times \mathbb{N}$) s'appelle la* division euclidienne.

Démonstration. On commence par traiter le cas où $n \geq 0$ et on montre l'existence de q et r par récurrence sur n. Si $n = 0$ alors on a $n = 0p + 0$, donc le résultat est démontré en prenant le quotient et le reste tous deux égaux à 0. Pour l'étape de récurrence, considérons un entier n et supposons qu'il existe deux entiers q et r tels que $n = pq + r$ et $0 \leq r < p$. Puisque $r < p$ on a $r + 1 \leq p$ et on peut distinguer deux cas :

- $r + 1 < p$: dans ce cas on a $n + 1 = pq + r + 1$ et comme $0 \leq r + 1 < p$ le résultat est démontré pour $n + 1$ en prenant q pour le quotient et $r + 1$ pour le reste ;

— $r+1=p$: dans ce cas on a $n+1=pq+p=p(q+1)$ et le résultat est démontré pour $n+1$ en prenant $q+1$ comme quotient et 0 comme reste.

Si maintenant $n<0$ alors $-n>0$ et on vient de voir qu'il existe q et r tels que $-n=pq+r$ et $0\leq r<p$; donc $n=-pq-r=p(-q)-r$. Si $r=0$ alors $n=p(-q)$ et le résultat est démontré en prenant $-q$ comme quotient et 0 comme reste. Si $r>0$ alors $n=p(-q)-r=p(-q-1)+p-r$ et comme $0<r<p$ on a $0<p-r<p$ également, donc le résultat est démontré en prenant $-q-1$ comme quotient et $p-r$ comme reste.

Montrons maintenant l'unicité : soient q,r,q',r' tels que $n=pq+r=pq'+r'$, $0\leq r<p$ et $0\leq r'<p$. Alors on a $pq+r-pq'-r'=p(q-q')+r-r'=0$. Mais comme r et r' sont tous deux compris entre 0 et p, on a $-p<r-r'<p$, donc $p(q-q')-p<p(q-q')+r-r'<p(q-q')+p$, c'est à dire $p(q-q'-1)<0<p(q-q'+1)$. Comme p est positif non nul on obtient $q-q'-1<0<q-q'+1$. La première inéquation est équivalente à $q-q'\leq 0$ et la seconde à $q-q'\geq 0$, donc $q-q'=0$, soit $q=q'$. Comme par hypothèse $pq+r=pq'+r'$ on en déduit que l'on a également $r=r'$. □

3.2 **Définition (divisibilité).** Soient n et p deux entiers. On dit que p *divise* n, et l'on note $p\mid n$, si n est un multiple de p, c'est à dire s'il existe un entier k tel que $n=kp$. On appelle *diviseurs* de n les entiers strictement positifs qui divisent n.

3.3 *Exemple.* L'ensemble des diviseurs de 24 est $\{1,2,3,4,6,8,12,24\}$. C'est aussi l'ensemble des diviseurs de -24.

3.4 En d'autres termes, p divise n si et seulement si le reste de la division euclidienne de n par p est 0, c'est-à-dire $n \bmod p=0$. C'est le cas où la division « tombe juste ».

3.5 Si p divise n alors $-p$ divise aussi n, de même p divise $-n$ et $-p$ divise $-n$. En particulier p divise n si et seulement si p divise $|n|$.

3.6 Si $p=0$ alors p divise n si et seulement si $n=0$. D'autre part, si $n=0$ alors tout entier p divise n. En général il est donc inutile de spécifier qu'un diviseur est non nul puisque 0 ne divise que 0. La condition d'être strictement positif, dans la définition des diviseurs, n'est là que pour éviter de considérer 0 comme un diviseur de 0.

3.7 **Exercice.** Montrer que si $p\mid n$ alors $p\mid n+kp$ pour tout $k\in\mathbb{Z}$.

3.8 **Exercice.** Montrer que si $p\mid m$ et $p\mid n$ alors pour tous $u,v\in\mathbb{Z}$, $p\mid um+vn$.

3.9 **Théorème.** *Soit n un entier non nul. Si d est un diviseur de n alors $d\leq|n|$. En particulier l'ensemble des diviseurs de n est fini.*

Démonstration. Un diviseur de n est également un diviseur de $|n|$. Il existe donc un $k\in\mathbb{Z}$ tel que $|n|=kd$. Mais comme $|n|$ et d sont positifs, k est également positif ; de plus comme $|n|>0$ (puisque n est supposé non nul), $k>0$ également, c'est à dire que $k\geq 1$. On a donc $d\leq kd=|n|$. L'ensemble des diviseurs de n étant un ensemble d'entiers naturels majoré par n, il est donc fini. □

3.10 **Théorème.** *La relation de divisibilité est une relation d'ordre partiel sur les entiers naturels, c'est à dire qu'elle est*

— *réflexive : pour tout $n\in\mathbb{N}$, on a $n\mid n$;*
— *antisymétrique : pour tous $m,n\in\mathbb{N}$, si $m\mid n$ et $n\mid m$ alors $m=n$;*
— *transitive : pour tous $m,n,p\in\mathbb{N}$, si $m\mid n$ et $n\mid p$ alors $m\mid p$.*

Démonstration. Pour la réflexivité, on obtient $n \mid n$ en écrivant $n = 1 \times p$.

Pour l'antisymétrie, supposons que m et n se divisent l'un l'autre, il existe alors deux entiers p et q tels que $n = pm$ et $m = qn$. On distingue alors deux cas : soit $n = 0$ soit $n \neq 0$. Dans le premier cas on a $m = p \times 0 = 0$ donc $m = n$. Dans le second cas on déduit des hypothèses l'égalité $n = pqn$ que l'on peut simplifier par n, ce qui donne $pq = 1$. Dans les entiers naturels, la seule solution de l'équation $pq = 1$ est $p = q = 1$ (on peut le justifier en utilisant le théorème 3.9), on en déduit donc $m = n$.

Pour la transitivité, si m divise n qui divise p, alors il existe deux entiers k et ℓ tels que $n = km$ et $p = \ell n$, d'où on déduit $p = k\ell m$ donc m divise p. □

3.11 **Exercice.** Qu'est ce qui devient faux dans le théorème précédent si on considère non pas des entiers naturels mais des entiers relatifs ?

Un entier $n > 1$ a toujours au moins deux diviseurs distincts : n lui-même, qui est le plus grand, et 1, qui est le plus petit. Si n n'a pas d'autres diviseurs que ces deux là, on dit que n est premier.

3.12 **Définition (nombre premier).** Un entier n est *premier* si $n > 1$ et pour tous $k, p \in \mathbb{N}$, si $n = kp$ alors $p = 1$ ou $p = n$.

3.13 *Exemple.* Les premiers nombres premiers sont $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 \ldots$

3.14 Avec cette définition un nombre négatif ne peut pas être premier.

3.15 On peut se demander si 1 devrait être considéré comme un nombre premier ou pas, puisqu'il satisfait aussi la propriété que si $kp = 1$ alors $p = 1$. Dans notre définition, ce n'est pas le cas, puisqu'on pose la condition explicite qu'un nombre premier est strictement supérieur à 1. C'est une question de convention et on aurait pu faire le choix inverse, mais dans la pratique c'est cette définition qui est la plus pertinente car beaucoup d'énoncés portant sur les nombre premiers devraient traiter le cas de 1 à part.

3.16 **Exercice.** Soit n un entier naturel. Montrer que n est premier si et seulement si n n'admet aucun diviseur premier inférieur à $\sqrt{n}$.

3.17 **Théorème.** *Tout entier $n \geq 2$ admet au moins un diviseur premier.*

Démonstration. On raisonne par récurrence forte. Considérons un entier $n \geq 2$ et supposons le résultat démontré pour tout entier $m < n$ c'est-à-dire que tout entier m tel que $2 \leq m < n$ admet un diviseur premier. Si n est premier alors le résultat est démontré sans avoir besoin de cette hypothèse de récurrence. Sinon n a au moins un diviseur m différent de 1 et de n et on a alors $2 \leq m < n$. Par hypothèse de récurrence, m admet donc un diviseur premier p. Comme p divise m qui divise n, on en conclut par transitivité que p divise n qui admet donc un diviseur premier. □

3.18 Dans ce raisonnement on applique l'hypothèse de récurrence non pas à $n - 1$ comme il est d'usage, mais à un entier m dont on a montré qu'il est strictement plus petit que n. Il s'agit d'une forme tout à fait licite du raisonnement par récurrence si on pense que le théorème démontré est : pour tout $n \geq 2$, pour tout m tel que $2 \leq m \leq n$, m admet un diviseur premier. Cette énoncé est équivalent au théorème mais c'est celui-là qui nous sert d'hypothèse de récurrence.

3.19 **Définition (factorielle).** On rappelle que la *factorielle* d'un entier n est l'entier $1 \times 2 \times 3 \times \cdots \times n$, le produit des entiers de 1 à n, noté $n!$. En particulier on a $0! = 1$.

3.20 **Théorème (Euclide).** *Il y a une infinité de nombres premiers.*

Démonstration. On montre que pour tout entier naturel n il existe un nombre premier supérieur à n. Ceci entraîne qu'il y a une infinité de nombres premiers.

Soit n un entier naturel. On considère le nombre $c_n := n! + 1$. Soit d un diviseur de c_n. Si $d \leq n$ alors d divise $n!$, donc d divise également 1 puisque $1 = c_n - n!$. Or 1 n'a qu'un seul diviseur, lui-même, donc $d = 1$. Autrement dit tout diviseur de c_n différent de 1 est strictement plus grand que n.

Comme $c_n \geq 2$, le théorème 3.17 nous assure qu'il existe un nombre premier p qui divise c_n. Mais si p est premier il est en particulier différent de 1, et comme c'est un diviseur de c_n il est donc strictement supérieur à n. On a donc trouvé un nombre premier plus grand que n comme annoncé. □

3.2 PGCD et théorème de Bézout

3.21 **Définition (PGCD).** Soient m et n deux entiers. Le *PGCD* (pour *plus grand commun diviseur*) de m et n, noté $\text{pgcd}(m, n)$ ou $m \wedge n$, est le plus grand des diviseurs communs à m et n. Autrement dit $m \wedge n$ est l'unique entier naturel non nul d qui vérifie :

— $d \mid m$ et $d \mid n$;

— pour tout d', si $d' \mid m$ et $d' \mid n$ alors $d' \leq d$.

3.22 *Exemple.* Le PGCD de 24 et 18 est 6. En effet, l'ensemble des diviseurs de 24 est $\{1, 2, 3, 4, 6, 8, 12, 24\}$ et l'ensemble des diviseurs de 18 est $\{1, 2, 3, 6, 9, 18\}$, l'ensemble de leurs diviseurs communs est donc $\{1, 2, 3, 6\}$ et le plus grand d'entre eux est 6.

3.23 Dans le cas particulier où $m = n = 0$, le PGCD de m et n n'est pas défini car 0 a une infinité de diviseurs. En règle générale dans tous les énoncés mentionnant le PGCD, on supposera implicitement que les deux entiers dont on prend le PGCD ne sont pas tous les deux nuls.

On peut également remarquer que m et n ont toujours au moins 1 comme diviseur commun, si bien que le PGCD de m et n est bien défini dès que l'on suppose que m et n ne sont pas tous les deux nuls.

3.24 **Définition.** Deux entiers sont *premiers entre eux* si leur PGCD est 1, autrement dit si 1 est leur seul diviseur commun.

3.25 *Exemple.* Les nombres 18 et 25 sont premiers entre eux. En effet, 18 a pour diviseurs $\{1, 2, 3, 6, 9, 18\}$ et 25 a pour diviseurs $\{1, 5, 25\}$, donc 1 est le seul élément commun.

3.26 En conséquence, 0 n'est premier avec aucun autre entier que 1.

L'existence d'un PGCD pour toute paire de nombres non tous les deux nuls est facile à établir puisque deux entiers ont toujours des diviseurs communs et que ceux-ci sont majorés. En revanche cela ne donne pas d'indication pour calculer le PGCD de façon efficace. L'algorithme d'Euclide répond à cette préoccupation.

3.27 **Définition (algorithme d'Euclide).** L'algorithme d'Euclide prend en entrée deux entiers a et b et renvoie un entier calculé comme suit :

Tant que $b \neq 0$, faire :
$r \leftarrow a \bmod b$,
$a \leftarrow b$,
$b \leftarrow r$.
Renvoyer a.

3.28 *Exemple.* Pour reprendre l'exemple de 24 et 18, en appliquant l'algorithme avec $a = 24$ et $b = 18$ on a les étapes suivantes :

k	a_k	b_k	division euclidienne
0	24	18	$24 = 1 \times 18 + 6$
1	18	6	$18 = 3 \times 6 + 0$
2	6	0	

On obtient donc le PGCD après deux itérations.

3.29 **Exercice.** Construire la suite (a_k) des valeurs successives de a dans l'algorithme d'Euclide en partant de $a = 55$ et $b = 34$.

3.30 **Théorème.** *Pour tous entiers naturels a et b non tous deux nuls, l'algorithme d'Euclide appliqué à a et b termine et renvoie $a \wedge b$.*

Démonstration. On commence par simplifier le cas initial en remarquant que si $b > a$ alors $b \neq 0$ et $a \bmod b = a$ donc la première itération de la boucle consiste simplement à échanger a et b, on se ramène donc au cas $a \geq b \geq 0$.

Notons a_k et b_k les valeurs de a et b après avoir appliqué k itérations de la boucle, en supposant qu'il y ait eu au moins k itérations. On a donc $a_0 = a$ et $b_0 = b$. Supposons que pour un k donné les entiers a_k et b_k soient définis.

— Si $b_k = 0$ alors l'algorithme termine après k itérations. Sinon on a $b_k \neq 0$ donc on peut poser la division euclidienne $a_k = qb_k + r$ et par définition on a $r = a_k \bmod b_k$ et $0 \leq r < b$. Dans ce cas on aura $a_{k+1} = b_k$ et $b_{k+1} < b_k$. Par conséquent la suite (b_k) est strictement décroissante et donc de longueur finie, puisqu'il n'existe pas de suite infinie strictement décroissante à valeurs dans $\mathbb{N}$.

— On a $a_{k+1} \wedge b_{k+1} = a_k \wedge b_k$. En effet, si d est un diviseur de a_k et b_k alors d divise aussi a_{k+1} puisque $a_{k+1} = b_k$, il divise aussi $a_k - qb_k$ qui est égal à r et donc à b_{k+1}. Réciproquement, si d divise a_{k+1} et b_{k+1} alors il divise b_k puisque $a_{k+1} = b_k$ et il divise $qa_{k+1} + b_{k+1}$ qui est égal à $qb_k + r_k$ donc à a_k. Ainsi les diviseurs communs de a_k et b_k sont les diviseurs communs de a_{k+1} et b_{k+1} donc $a_{k+1} \wedge b_{k+1} = a_k \wedge b_k$.

Ces deux observations montrent qu'il existe un k tel que $b_k = 0$ et $a_k \wedge b_k = a \wedge b$ or $a_k \wedge b_k = a_k \wedge 0 = a_k$, donc l'algorithme termine toujours en renvoyant la valeur $a \wedge b$. □

3.31 **Théorème (Bézout).** *Deux entiers m et n sont premiers entre eux si et seulement si il existe deux entiers u et v tels que $um + vn = 1$.*

Démonstration. Supposons qu'il existe u et v tels que $um + vn = 1$ et soit d un diviseur de m et n. Alors d divise um et vn donc d divise 1 et par conséquent $d = 1$. Le seul diviseur commun de m et n est donc 1, ce qui signifie que m et n sont premiers entre eux.

Supposons maintenant que m et n sont premiers entre eux. Notons I l'ensemble des entiers de la forme $um + vn$ pour tous les $u, v \in \mathbb{Z}$. D'après la remarque 3.26, m et n

ne sont pas tous les deux nuls donc I contient au moins un entier strictement positif. On peut alors considérer le plus petit élément strictement positif de I, nommons-le d. Par définition de I il existe des entiers u_0 et v_0 tels que $u_0m + v_0n = d$.

Faisons maintenant la division euclidienne de m par d : on obtient q et r tels que $m = dq + r$, avec $0 \leq r < d$. Donc $r = m - dq = m - (u_0m + v_0n)q = (1 - u_0q)m - v_0qn$ et par conséquent $r \in I$. Mais puisque $0 \leq r < d$ et que d est par définition le plus petit élément strictement positif dans I, on a nécessairement $r = 0$, donc d divise m. On peut voir de même que d divise n. Par conséquent, comme m et n sont premiers entre eux on a $d = 1$ et comme $d = u_0m + v_0n$ le théorème est démontré. □

3.32 **Corollaire.** *Pour tous entiers m et n, il existe deux entiers u et v tels que $um+vn = m\wedge n$.*

Démonstration. Soit $d = m \wedge n$ le PGCD de m et n. Comme d divise m il existe m' tel que $m = m'd$; de même il existe n' tel que $n = n'd$. On va voir que m' et n' sont premiers entre eux.

Soit p un diviseur de m' et n' ; on a donc deux entiers k et l tels que $m' = kp$ et $n' = lp$; par conséquent on a $m = kpd$ et $n = lpd$, donc pd divise m et n. Mais d est le PGCD de m et n donc $pd \leq d$ ce qui ne se peut que si $p = 0$ ou $p = 1$. Mais p ne peut être nul car c'est un diviseur, donc $p = 1$. On vient de montrer que le seul diviseur commun de m' et n' est 1, c'est à dire que m' et n' sont premiers entre eux comme annoncé.

On applique le théorème de Bézout à m' et n' ce qui nous donne deux entiers u et v tels que $um' + vn' = 1$, donc $um'd + vn'd = d$, c'est à dire $um + vn = d$ et le corollaire est démontré. □

3.33 Ce corollaire n'est pas une équivalence, contrairement au théorème de Bézout : ce n'est pas parce que l'on a $um + vn = d$ que d est le PGCD de m et n. Par exemple, on a $1 \times 5 + (-1) \times 3 = 2$ or 2 n'est pas le PGCD de 5 et 3 puisqu'il n'est même pas diviseur de 3 ni de 5.

3.34 **Exercice.** Soient m, n, u, v des entiers et d un entier positif. Montrer que si $um + vn = d$ et d divise m et d divise n alors $d = m \wedge n$.

3.35 **Corollaire.** *Soient m et n deux entiers. Tout diviseur commun de m et de n divise aussi $m \wedge n$.*

Démonstration. Par le corollaire précédent on sait qu'il existe u et v tels que $um + vn = m \wedge n$. Si un entier p divise m et n alors il divise um et vn donc il divise aussi leur somme qui est $m \wedge n$. □

3.36 **Exercice.** Soient m, n et p des entiers. Montrer que $pm \wedge pn = p(m \wedge n)$.

La démonstration donnée plus haut du théorème de Bézout et de son corollaire assure l'existence des deux coefficients u et v tels que $um + vn = m \wedge n$, mais elle ne permet pas facilement de déduire une méthode pour calculer u et v. On peut en fait étendre l'algorithme d'Euclide pour faire ce calcul.

En effet, observons l'étape de récurrence dans la démonstration du théorème précédent : pour un k donné, on suppose $b_k \neq 0$ et on pose $r = a_k \bmod b_k$ puis $a_{k+1} = b_k$ et $b_{k+1} = r$. On justifie alors que $a_k \wedge b_k = a_{k+1} \wedge b_{k+1}$. Supposons alors que l'on sache obtenir deux

entiers relatifs u_{k+1} et v_{k+1} tels que $a_{k+1}u_{k+1} + b_{k+1}v_{k+1} = a_{k+1} \wedge b_{k+1}$. On a alors les égalités suivantes :

$$\begin{aligned} a_k \wedge b_k &= a_{k+1} \wedge b_{k+1} && \text{par les remarques précédentes} \\ &= a_{k+1}u_{k+1} + b_{k+1}v_{k+1} && \text{par hypothèse} \\ &= b_k u_{k+1} + (a_k - qb_k)v_{k+1} && \text{parce que } a_{k+1} = b_k \text{ et } a_k = qb_k + b_{k+1} \\ &= a_k v_{k+1} + b_k(u_{k+1} - qv_{k+1}) \end{aligned}$$

on obtient donc les coefficients de Bézout en posant $u_k = v_{k+1}$ et $v_k = u_{k+1} - qv_{k+1}$ où q est le quotient de a_k par b_k. Dans le cas où $b_k = 0$, on a directement $a_k \wedge b_k = a_k$ et donc on pose $u_k = 1$ et $v_k = 0$. Il s'agit donc d'un calcul par récurrence en partant du cas initial k où $b_k = 0$ et en faisant décroître l'indice jusqu'à trouver u_0 et v_0.

3.37 *Exemple.* Déterminons le PGCD et les coefficients de Bézout pour 55 et 36 :

k	a_k	b_k	q	r	u_k	v_k
0	55	36	1	19	-17	26
1	36	19	1	17	9	-17
2	19	17	1	2	-8	9
3	17	2	8	1	1	-8
4	2	1	2	0	0	1
5	1	0			1	0

On déduit de ce calcul d'une part que $55 \wedge 36 = 1$ et donc que 55 et 36 dont premiers entre eux (première phase qui applique l'algorithme d'Euclide) et d'autre part que les coefficients de Bézout sont -17 et 26 et que $-17 \times 55 + 26 \times 36 = 1$.

3.38 **Exercice.** Appliquer l'algorithme d'Euclide pour trouver les coefficients de Bézout de 55 et 34. Faire de même avec 55 et 35.

3.39 Le calcul des coefficients de Bézout et les propriétés du PGCD permettent de résoudre des équations linéaires dans les nombres entiers. Considérons par exemple l'équation

$$57x + 39y = 12$$

et cherchons ses solutions dans $\mathbb{Z}$. On peut résoudre cette équation par les étapes suivantes :

— *Simplification.* Le PGCD des coefficients 57 et 39 est 3, on sait donc que l'ensemble $\{57x + 39y \mid x, y \in \mathbb{Z}\}$ de toutes les valeurs possibles du membre gauche est $3\mathbb{Z}$ puisque tout entier de cette forme est multiple de 3 et que 3 est effectivement de cette forme par le théorème de Bézout. Le membre droit est multiple de 3 donc il y a des solutions. On peut alors diviser par 3 et se ramener à l'équation

$$19x + 13y = 4$$

où les coefficients sont premiers entre eux.

— *Solution particulière.* L'algorithme d'Euclide donne deux entiers u et v tels que $19u + 13v = 1$, par exemple $u = -2$ et $v = 3$. En multipliant par le membre de droite qui est 4, on obtient une première solution à l'équation :

$$x = -2 \times 4 = -8 \qquad y = 3 \times 4 = 12$$

— *Équation homogène.* Si (x, y) et (x', y') sont deux solutions de l'équation $19x+13y = 4$ alors on a $19(x' - x) + 13(y' - y) = 0$. Réciproquement, si (x, y) est une solution de $19x + 13y = 4$ et (x', y') est un couple qui vérifie $19(x' - x) + 13(y' - y) = 0$ alors $19x' + 13y' = 19x + 13y + 19(x' - x) - 13(y' - y) = 4 + 0 = 4$ donc (x', y') est une solution de l'équation de départ. Ainsi on aura l'ensemble des solutions en résolvant l'équation homogène

$$19x + 13y = 0$$

L'équation est équivalente à $19x = -13y$ donc
— $-13y$ doit être multiple de 19 or 19 et 13 sont premiers entre eux donc y doit être multiple de 19 et donc s'écrire $y = 19t$ pour un certain entier $t \in \mathbb{Z}$,
— on doit avoir $19x = -13 \times 19 \times t$ donc $x = -13t$.
Il est clair que pour tout t on a $19 \times (-13t) + 13 \times (19t) = 0$, donc l'ensemble des solutions de l'équation homogène est $\{(-13t, 19t) \mid t \in \mathbb{Z}\}$.

On conclut que l'ensemble des solutions de l'équation est

$$\{(-8 - 13t, 12 + 19t) \mid t \in \mathbb{Z}\}.$$

3.40 **Exercice.** Trouver les entiers x et y tels que :

1. $283x + 1722y = 31$;

2. $365x + 72y = 18$;

3. $1111x + 2345y = 66$.

3.41 **Définition (PPCM).** Soient m et n deux entiers. Le *PPCM* (pour *plus petit commun multiple*) de m et n, noté $\text{ppcm}(m, n)$ ou $m \vee n$, est le plus petit des multiples communs à m et n. Autrement dit $m \vee n$ est l'unique entier naturel non nul c qui vérifie :
— $m \mid c$ et $n \mid c$;
— pour tout c', si $m \mid c'$ et $n \mid c'$ alors $c \leq c'$.

3.42 *Exemple.* Le PPCM de 24 et 18 est 72. En effet, les premiers multiples de 24 sont $\{24, 48, 72, 96, 120 \ldots\}$ et ceux de 18 sont $\{18, 36, 54, 72, 90, 108 \ldots\}$ donc le plus petit élément commun de ces deux ensembles est 72.

Le PPCM est donc en quelque sorte symétrique du PGCD. On peut faire un lien très précis entre les deux grâce à la propriété suivante.

3.43 **Proposition.** *Pour tous entiers m et n on a $(m \wedge n) \times (m \vee n) = m \times n$.*

Démonstration. Posons $d = m \wedge n$ de sorte que l'on a une décomposition $m = d \times m'$ et $n = d \times n'$ où m' et n' sont premiers entre eux. On observe alors que $m \vee n = d \times m' \times n'$, en effet :
— le produit $d \times m' \times n'$ est multiple à la fois de $d \times m' = m$ et de $d \times n' = n$,
— si c est un multiple commun de m et n, alors il est multiple de d donc on peut le décomposer en $d \times c'$; comme $d \times c'$ est multiple de $d \times m'$, on en déduit que c' est multiple de m', de même c' est multiple de n', or m' et n' sont premiers entre eux donc c' est multiple de leur produit $m' \times n'$, ainsi $c = d \times c'$ est multiple de $d \times m' \times n'$.

Par conséquent on a $(m \wedge n) \times (m \vee n) = d \times (d \times m' \times n') = (d \times m') \times (d \times n') = m \times n$. □

On peut ainsi calculer le PPCM de deux nombres en divisant leur produit par leur PGCD.

3.3 Décomposition en facteurs premiers

3.44 **Théorème (lemme de Gauss).** *Soient m et n et p trois entiers tels que p divise mn. Si p est premier avec m alors p divise n. En particulier si p est premier alors p divise m ou p divise n.*

Démonstration. Supposons p premier avec m. Par le théorème de Bézout, il existe u et v tels que $up + vm = 1$. Par conséquent on a $upn + vmn = n$. Mais p divise upn et par hypothèse p divise mn, donc p divise $upn + vmn$, c'est à dire que p divise n.

Supposons maintenant p premier. Si p divise m alors le résultat est démontré, supposons donc que p ne divise pas m et montrons que p est premier avec m. Soit d un diviseur commun de p et m ; alors d divise en particulier p donc est égal à 1 ou à p puisque p est premier ; mais p ne divise pas m, donc $d = 1$. Autrement dit le seul diviseur commun de p et m est 1, c'est à dire que p est premier avec m. On vient de voir qu'alors p divise n. □

3.45 L'hypothèse de primalité de p est nécessaire. En effet, si on pose $p = 6$, $m = 3$ et $n = 4$, alors p divise mn mais p ne divise ni m ni n, et en effet p n'est pas premier avec m ni avec n.

3.46 On peut immédiatement généraliser ce lemme à un produit d'un nombre quelconque de facteurs : si un nombre premier p divise un produit d'entiers $n_1 n_2 \dots n_k$ alors il existe un entier i tel que $1 \leq i \leq k$ et p divise n_i. On démontre cette propriété généralisée par récurrence sur k, en appliquant le lemme de Gauss pour justifier l'étape de récurrence.

3.47 **Théorème (décomposition en facteurs premiers).** *Soit n un entier naturel non nul. Il existe un unique $k \in \mathbb{N}$ et un unique ensemble de couples $D_n = \{(p_1, \alpha_1), \dots, (p_k, \alpha_k)\}$ tel que*

- *les p_i sont des nombres premiers deux à deux distincts,*
- *les α_i sont des entiers naturels non nuls,*
- *$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$.*

3.48 De façon peut-être plus intuitive, le théorème signifie que pour tout n il existe une écriture de n sous la forme $p_1^{\alpha_1} \dots p_k^{\alpha_k}$ (avec les conditions de l'énoncé sur les p_i et α_i) et que cette écriture est unique, à l'ordre près des termes $p_i^{\alpha_i}$. L'ensemble D_n est appelé la *décomposition de n en facteurs premiers.*

3.49 Si on prend $n = 1$ le théorème est vérifié en prenant $k = 0$ et $D_1 = \emptyset$.

Démonstration. On procède par récurrence forte, autrement dit on montre par récurrence sur n la propriété suivante :

> Pour tout entier n, tout entier m tel que $1 \leq m \leq n$ admet une et une seule décomposition en facteurs premiers.

Cette propriété entraîne évidemment l'existence d'une unique décomposition pour tout entier n (en l'appliquant à $m = n$ par exemple).

Le cas initial est $n = 1$. On a vu que 1 admet une décomposition en facteurs premiers en prenant $k = 0$ et $D_1 = \emptyset$. De plus toute décomposition non vide (avec $k \geq 1$ et $D \neq \emptyset$) contient au moins un facteur premier p avec un exposant non nul, donc son produit est supérieur ou égal à p, or on a $p \geq 2$ tout nombre premier. Ainsi la décomposition vide est la seule qui convienne pour 1.

Pour l'étape de récurrence, prenons un entier $n > 1$ et supposons que la propriété est vraie au rang $n-1$, donc tout $m \leq n-1$ admet une décomposition en facteurs premiers. Il reste donc à montrer que n admet une décomposition et une seule.

Comme $n > 1$, on sait par le théorème 3.17 que n admet au moins un diviseur premier, prenons donc un tel diviseur p. Par définition de la divisibilité, il existe un entier m tel que $n = pm$ et $m \neq 0$ puisque $n \neq 0$. Comme p est premier on a $p \geq 2$ donc $n \geq 2m$ et en particulier $m \leq n - m \leq n - 1$. Par hypothèse de récurrence on a donc une décomposition $D = \{(p_1, \alpha_1), \ldots, (p_k, \alpha_k)\}$ de m. Pour en déduire une décomposition de n, on distingue deux cas :

— Si p est égal à l'un des p_i, par exemple à p_1 alors $n = pm = pp_1^{\alpha_1} \ldots p_k^{\alpha_k} = p_1^{\alpha_1+1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ donc $\{(p_1, \alpha_1 + 1), (p_2, \alpha_2), \ldots, (p_k, \alpha_k)\}$ est une décomposition de n en facteurs premiers.

— Si au contraire p est distinct de tous les p_i alors $n = pm = p^1 p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ et donc $\{(p, 1), (p_1, \alpha_1), \ldots, (p_k, \alpha_k)\}$ est une décomposition de n en facteurs premiers.

Pour l'unicité, supposons maintenant que n admet deux décompositions, que l'on notera $\{(p_1, \alpha_1), \ldots, (p_k, \alpha_k)\}$ et $\{(q_1, \beta_1), \ldots, (q_\ell, \beta_\ell)\}$, et montrons qu'elles sont égales. Par définition de la décomposition on a $n = p_1 m$ en posant $m = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Or p_1 est premier et divise $q_1^{\beta_1} \ldots q_\ell^{\beta_\ell}$, donc il y a un i tel que p_1 divise q_i d'après le lemme de Gauss. Comme q_i est premier, on en déduit que $q_i = p_1$. On a donc $n = p_1 q_1^{\beta_1} \ldots q_i^{\beta_i - 1} \ldots q_l^{\beta_l}$ et par conséquent $m = q_1^{\beta_1} \ldots q_i^{\beta_i - 1} \ldots q_l^{\beta_l}$. Comme $m \leq n - 1$, par hypothèse de récurrence on a l'unicité de la décomposition de m en facteurs premiers, par conséquent on a $\{(p_1, \alpha_1 - 1), \ldots, (p_k, \alpha_k)\} = \{(q_1, \beta_1), \ldots, (q_i, \beta_i - 1), \ldots, (q_l, \beta_l)\}$ ce qui entraîne l'égalité cherchée. □

3.4 Congruences

3.50 **Définition.** Soit n un entier naturel non nul. Soient a et b deux entiers. On dit que a est *congru* à b modulo n et on note $a \equiv b\ [n]$ ou $a \equiv b \pmod{n}$ si n divise $a - b$.

3.51 *Exemple.* Les entiers 124 325 et 4 568 925 sont congrus modulo 100.

3.52 Un cas important est que $a \equiv 0 \pmod{n}$ si et seulement si a est multiple de n.

3.53 Pour chaque n fixé, la relation de congruence modulo n est une relation d'équivalence, en effet elle est

— réflexive : pour tout a on a $a \equiv a \pmod{n}$,

— symétrique : pour tout a et b, si $a \equiv b \pmod{n}$ alors $b \equiv a \pmod{n}$,

— transitive : pour tout a, b et c, si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$ alors $a \equiv c \pmod{n}$.

L'ensemble des classes d'équivalence pour cette relation est noté $\mathbb{Z}/n\mathbb{Z}$ (on justifiera cette notation dans le chapitre suivant). On peut le voir comme l'ensemble des « entiers modulo n », c'est-à-dire l'ensemble des entiers en considérant comme égaux deux éléments qui sont congrus modulo n.

3.54 La condition que n soit strictement positif n'est pas strictement nécessaire pour la définition, mais elle correspond à l'usage. En effet, en appliquant strictement la définition sans contrainte sur n, d'une part on a $a \equiv b \pmod{n}$ si et seulement si $a \equiv b \pmod{-n}$, d'autre part $a \equiv b \pmod{0}$ si et seulement si $a = b$.

3.55 **Proposition.** *Pour chaque n, la relation de congruence modulo n est compatible avec l'addition et la multiplication : si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a + c \equiv b + d \pmod{n}$ et $ac \equiv bd \pmod{n}$.*

Démonstration. Par définition, on sait qu'il existe deux entiers k et ℓ tels que $a - b = nk$ et $c - d = n\ell$, on a donc

— $(a+c)-(b+d) = (a-b)+(c-d) = nk+n\ell = n(k+\ell)$ donc $a+c \equiv b+d \pmod{n}$,

— $ac - bd = ac - ad + ad - bd = a(c-d) + (a-b)d = an\ell + nkd = n(a\ell + kd)$ donc $ac \equiv dd \pmod{n}$.

□

3.56 Cela implique que la relation de congruence modulo n est compatible avec l'opération puissance, mais uniquement pour la base. En effet, modulo n on a $a^k = a \times a \times \cdots \times a \equiv b \times b \times \cdots \times b = b^k$, pour k fixé.

En revanche, la congruence n'est pas compatible avec la fonction puissance du côté de l'exposant. Par exemple on a $3 \equiv 8 \pmod{5}$ mais $2^3 \not\equiv 2^8 \pmod{5}$ puisque $2^8 - 2^3 = 256 - 8 = 248$ n'est pas multiple de 5.

3.57 *Exemple.* Un phénomène bien connu qui illustre la congruence et sa compatibilité avec les opérations est la classique « preuve par 9 » qui dit qu'un nombre est divisible par 9 si et seulement la somme de ses chiffres est divisible par 9.

On peut le prouver de la façon suivante. Soit n un entier naturel, soit $c_k c_{k-1} \cdots c_2 c_1 c_0$ son écriture en base 10, où c_i représente le i-ème chiffre en partant de la droite, avec la convention que le chiffre des unités a le numéro 0. Alors on a $n = 10^k c_k + 10^{k-1} c_{k-1} + \cdots + 10^1 c_1 + 10^0 c_0$. On remarque alors que $10 - 1 = 9$ donc $10 \equiv 1 \pmod{9}$, et par conséquent pour chaque i on a $10^i \equiv 1^i = 1 \pmod{9}$, et donc $n \equiv c_k + c_{k-1} + \cdots + c_1 + c_0 \pmod{9}$. Ainsi n est multiple de 9 si et seulement si $n \equiv 0 \pmod{9}$ si et seulement si $c_k + c_{k-1} + \cdots + c_1 + c_0 \equiv 0 \pmod{9}$ si et seulement si $c_k + c_{k-1} + \cdots + c_1 + c_0$ est multiple de 9.

3.58 **Proposition.** *Pour tous a, b et n, on a $a \equiv b \pmod{n}$ si et seulement si a et b ont même reste dans la division euclidienne par n.*

Démonstration. Par division euclidienne, on écrit $a = qn + r$ et $b = q'n + r'$, avec $0 \leq r, r' < n$. On a alors $a - b = (qn + r) - (q'n + r') = (q - q')n + (r - r')$. Si $r = r'$ alors on a sonc $a - b = (q - q')n$ donc $a \equiv b \pmod{n}$. Réciproquement, si $a \equiv b \pmod{n}$ alors $a - b$ est multiple de n donc $r - r'$ est multiple de n, or on a $-n < r - r' < n$ et le seul multiple de n strictement compris entre $-n$ et n est 0 donc on a nécessairement $r - r' = 0$ et par conséquent $r = r'$. □

Quand on considère la congruence modulo un nombre *premier*, on a de nombreuses propriétés supplémentaires. La première est que chaque entier non multiple de p a un « inverse » pour la multiplication modulo p.

3.59 **Proposition.** *Soit p un nombre premier. Pour tout entier a, si $a \not\equiv 0 \pmod{p}$ alors il existe un entier b tel que $ab \equiv 1 \pmod{p}$.*

Démonstration. Si $a \not\equiv 0 \pmod{p}$, cela signifie que a n'est pas multiple de p, donc que a et b sont premiers entre eux puisque p est premier. Par le théorème de Bézout, il existe donc deux entiers u et v tels que $au + vp = 1$. Comme $p \equiv 0 \mod p$ on en déduit $au \equiv au + vp \equiv 1 \pmod{p}$. □

3.60 *Exemple.* Modulo 7, l'entier 3 est inversible et son inverse est 5 puisque $3 \times 5 = 15 \equiv 1 \pmod{7}$. Bien sûr, tout entier de la forme $5 + 7k$ pour $k \in \mathbb{Z}$ conviendrait aussi.

3.61 *Exemple.* La condition que p est premier est cruciale. Par exemple, 6 n'est pas inversible modulo 8 parce que tout multiple de 6 sera pair alors que $8k + 1$ est impair pour tout k. En fait, le théorème de Bézout dit qu'un entier a est inversible modulo b si et seulement si a et b sont premiers entre eux (et dans cet exemple 6 et 8 ne le sont pas).

3.62 **Corollaire.** *Soit p un nombre premier. Pour tous entiers a, b et c, si a n'est pas multiple de p et $ab \equiv ac \pmod{p}$ alors $b \equiv c \pmod{p}$.*

3.63 **Théorème (Fermat).** *Soit p un nombre premier. Alors*
- *pour tout entier a on a $a^p \equiv a \pmod{p}$,*
- *pour tout entier a non multiple de p, $a^{p-1} \equiv 1 \pmod{p}$.*

Ce théorème est souvent appelé « petit théorème de Fermat », par opposition au « grand » ou « dernier théorème de Fermat » qui n'a pas été démontré avant 1994 et est hors de portée de ce cours… Le petit théorème de Fermat a de nombreuses démonstrations différentes, on n'en donne qu'une seule ici.

Démonstration. Remarquons que si a est multiple de p, alors on a $a \equiv 0 \pmod{p}$ et $a^p \equiv 0 \pmod{p}$ donc le point 1 est démontré facilement. Si a n'est pas multiple de p, le second énoncé implique le premier en multipliant par a, il suffit donc de démontrer le second énoncé. Pour cela, posons $N = a \times 2a \times 3a \times \cdots \times (p-1)a$.

D'une part, en rassemblant les a dans cette formule on a $N = (p-1)!a^{p-1}$.

D'autre part, pour chaque $k \in \{1, 2, \ldots, p-1\}$ posons $r_k = ka \bmod p$, de sorte que $N \equiv r_1 r_2 \cdots r_{p-1} \pmod{p}$. Comme p est premier, a non multiple de p et k non multiple de p (puisque $1 \leq k \leq p-1$), ka n'est pas multiple de p et donc $r_k \neq 0$ pour chaque k. De plus, les r_k sont deux à deux distincts, en effet pour $1 \leq i < j \leq p-1$ on a $r_j - r_i \equiv ja - ia \pmod{p}$ or $ja - ia = (j-i)a$ ne peut pas être multiple de p puisque a n'est pas multiple de p et $j - i$ non plus puisqu'il est compris entre 1 et $p-1$. Ainsi $r_1, r_2, \ldots, r_{p-1}$ est une permutation de $1, 2, \ldots, p-1$ donc en multipliant les r_k on obtient $N \equiv r_1 r_2 \cdots r_{p-1} = (p-1)! \pmod{p}$.

En comparant les deux calculs de N, on a donc $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$. Comme p est premier, $(p-1)!$ ne peut pas être multiple de p, on peut donc simplifier par $(p-1)!$, ce qui donne $a^{p-1} \equiv 1 \pmod{p}$. □

3.64 *Exemple.* Le petit théorème de Fermat permet de raisonner par congruence sur l'exposant dans une puissance. Calculons par exemple le reste de la division de 2000^{2000} par 7, qui

est premier. On a $2000 = 285 \times 7 + 5$ donc $2000 \equiv 5 \pmod 7$ et $2000^{2000} \equiv 5^{2000} \pmod 7$. Comme 5 n'est pas multiple de 7, le petit théorème de Fermat donne $5^6 \equiv 1 \pmod 7$ donc l'exposant peut être considéré modulo 6. On a $2000 = 333 \times 6 + 2$ donc on en déduit $5^{2000} \equiv 5^2 \pmod 7$ or $5^2 = 25 \equiv 4 \pmod 7$ donc finalement $2000^{2000} \equiv 4 \pmod 7$, autrement dit le reste de la division par 7 de 2000^{2000} est 4.