Arithmétique dans l'anneau $(\mathbb{Z}, +, \cdot)$

Aperçu

D 1 Soit $(a, b) \in \mathbb{Z}^2$. On dit que a **divise** b, et l'on note $a \,\Big|\, b$ lorsqu'il existe $q \in \mathbb{Z}$ tel que $b = aq$.
Dans ce cas, on dit aussi que a est un **diviseur** de b ou que b est un **multiple** de a.

N

- On note par $a\mathbb{Z} = \{ \, aq \mid q \in \mathbb{Z} \, \}$ l'ensemble des multiples de a.
- On note $D(b) = \left\{ \, a \in \mathbb{N} \,\middle|\, a \,\Big|\, b \, \right\}$ l'ensemble des diviseurs positifs de b.

E 2

1. $5 \,\Big|\, 210$, $3 \,\Big|\, 18$.
2. $D(6) = \{\ 1, 2, 3, 6\ \}$.
3. $4\mathbb{Z} = \{\ \dots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \dots\ \}$.
4. 0 est divisible par n'importe quel entier et le seul entier divisible par 0 est 0.

$$\forall a \in \mathbb{Z}, a \,\Big|\, 0 \text{ et } \left(0 \,\Big|\, a \iff a = 0\right).$$

5. Le seul diviseurs de 1 est 1, mais 1 divise tout entier relatif.

$$\forall b \in \mathbb{Z}, 1 \,\Big|\, b.$$

P 3 **Lien avec la relation $\leq$**

La divisibilité est liée à l'ordre naturel sur $\mathbb{Z}$ par

$$\forall b \in \mathbb{Z}, \forall a \in \mathbb{Z}, a \,\Big|\, b \implies (b = 0 \text{ ou } |a| \leq |b|).$$

La réciproque est fausse.

Démonstration. Pour tout $k \geq 1$, on a $k|a| \geq |a|$. ∎

P 4 **Propriétés de la relation $\Big|$ sur $\mathbb{Z}$**

La relation $\Big|$ sur $\mathbb{Z}$ est

1. *réflexive :* $\forall a \in \mathbb{Z}, a \Big| a$;
2. *transitive :* $\forall (a, b, c) \in \mathbb{Z}^3, (a \Big| b \text{ et } b \Big| c) \implies a \Big| c$;

C 5 *Soit* $(a, b) \in \mathbb{Z}^2$.

$$a \Big| b \iff b \in a\mathbb{Z} \iff b\mathbb{Z} \subset a\mathbb{Z}.$$

D 6 Soit $(a, b) \in \mathbb{Z}^2$. On dit que les entiers a et b sont **associés** si $\left(a \,\middle|\, b \text{ et } b \,\middle|\, a\right)$.

P 7 **Caractérisation des couples d'entiers associés**

Soit $(a, b) \in \mathbb{Z}^2$. Les assertions suivantes sont équivalentes

1. *a et b sont associés.*
2. *$a\mathbb{Z} = b\mathbb{Z}$.*
3. *$a = b$ ou $a = -b$.*

P 8 **Compatibilité avec les opérations algèbriques**

Soit $(a, b, c, d) \in \mathbb{Z}^4$.

1. *Combinaison linéaire à coefficients entiers : si* $a \mid b$ *et* $a \mid c$, *alors*

$$\forall (u, v) \in \mathbb{Z}^2 \; a \mid ub + vc.$$

   En particulier, si $a \mid b$ *et* $a \mid c$, *alors* $a \mid b + c$ *et* $a \mid b - c$.

2. *Produit : Si* $a \mid b$ *et* $c \mid d$, *alors* $ac \mid bd$.

   En particulier, si $a \mid b$ *alors pour tout* $k \in \mathbb{N}$, $a^k \mid b^k$.

3. *Multiplication/division par un entier : si* $c \neq 0$, *alors* $a \mid b \iff ac \mid bc$.

D 9 **Division euclidienne dans $\mathbb{Z}$**

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^\star$. Alors il existe un unique couple d'entiers $(q, r) \in \mathbb{Z} \times \mathbb{N}$ vérifiant

$$a = bq + r \qquad \text{et} \qquad 0 \leq r < b.$$

- q est le **quotient** de la division euclidienne de a par b.
- r est le **reste** de la division euclidienne de a par b et on le note $a \mod b$..

L'opération qui remplace a par r s'appelle la **réduction modulo** b.

E 10

$$\begin{array}{r|l} 543 & 17 \\ \cline{2-2} 33 & 31 \\ 16 & \end{array}$$

Ici $a = 543, b = 17, q = 31, r = 16.$

P 11 *Soit r le reste de la division euclidienne de a par b. On a*

$$b \mid a \iff r = 0.$$

D 12 Une partie A de $\mathbb{Z}$ est appelée **sous-groupe** (additif) de $\mathbb{Z}$ si elle vérifie les conditions ci-dessous:

1. $0 \in A$.
2. A est **stable pour l'addition**:
$$\forall (x, y) \in A^2, x + y \in A.$$
3. A est **stable par passage à l'opposé**:
$$\forall x \in A, -x \in A.$$

T 13

1. *Pour tout entier* $a \in \mathbb{Z}$*,* $a\mathbb{Z}$ *est un sous-groupe de* $\mathbb{Z}$*.*
2. *Réciproquement, soit* A *un sous-groupe de* $\mathbb{Z}$*, il existe un unique entier* $a \geq 0$ *tel que*
$$A = a\mathbb{Z}.$$

P 14 *Soient* A *et* B *deux sous-groupes de* $\mathbb{Z}$*, alors l'intersection* $A \cap B$ *de ces deux sous-groupes est un sous-groupe de* $\mathbb{Z}$*.*

P 15 *Soient* A *et* B *deux sous-groupes de* $\mathbb{Z}$*, alors la somme de ces deux sous-groupes*

$$A + B = \{\, x + y \mid x \in A \ \text{ et } \ y \in B \,\}$$

est un sous-groupe de $\mathbb{Z}$*.*

D 16 Un **nombre premier** est un entier naturel $p \geq 2$ dont les seuls diviseurs strictement positifs sont 1 et p. On note $\mathbb{P}$ l'ensemble des nombres premiers.

Avec des quantificateurs, cela s'écrit

$$\forall (a, b) \in \mathbb{N}, p = ab \implies a = 1 \text{ ou } b = 1.$$

P 17 *Pour qu'un entier $p > 1$ soit premier, il faut et il suffit qu'il ne soit pas produit de deux entiers strictement plus grand que 1.*

T 18 **(Euclide)**
Tout entier $n > 1$ est un produit (fini) de nombres premiers. En particulier, n possède au moins un diviseur premier.

P 19 *Soit $n > 1$. Si n n'est pas premier, il possède un facteur premier p tel que $p^2 \leq n$.*

A 20 **Crible d'Erathosthène**

Si l'entier n n'est divisible par aucun nombre premier p tel que $p^2 \leq n$, alors n est un nombre premier.

	$\boxed{2}$	$\boxed{3}$	4	$\boxed{5}$	6	$\boxed{7}$	8	9	10
$\boxed{11}$	12	$\boxed{13}$	14	15	16	$\boxed{17}$	18	$\boxed{19}$	20
21	22	$\boxed{23}$	24	25	26	27	28	$\boxed{29}$	30
$\boxed{31}$	32	33	34	35	36	$\boxed{37}$	38	39	40
$\boxed{41}$	42	$\boxed{43}$	44	45	46	$\boxed{47}$	48	49	50
51	52	$\boxed{53}$	54	55	56	57	58	$\boxed{59}$	60
$\boxed{61}$	62	63	64	65	66	$\boxed{67}$	68	69	70
$\boxed{71}$	72	$\boxed{73}$	74	75	76	77	78	$\boxed{79}$	80
81	82	$\boxed{83}$	84	85	86	87	88	$\boxed{89}$	90
91	92	93	94	95	96	$\boxed{97}$	98	99	100

T 21 *L'ensemble $\mathbb{P}$ des nombres premiers est infini.*

Démonstration. Supposons que l'ensemble des nombres premiers $\mathbb{P}$ soit fini. On peut alors écrire $\mathbb{P} = \{ p_1, \dots, p_k \}$. On introduit l'entier $n = p_1 p_2 \dots p_k + 1 \geq 2$. Cet entier a un diviseur premier p. Ce nombre premier p est donc l'un des p_i. Or p divise n et divise $p_1 p_2 \dots p_k = n - 1$, donc p divise $(n-1) - n = 1$, ce qui est absurde. ∎

D 22 Soient a et b deux entiers relatifs quelconques. On appelle **plus grand commun diviseur** (ou pgcd) de a et b l'unique entier $d \geq 0$ tel que

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

on note cet entier $\mathrm{pgcd}(a, b)$ ou $a \wedge b$.

T 23 *Soient a et b deux entiers relatifs quelconques et $d = \operatorname{pgcd}(a, b)$.*

1. *L'entier d divise a et b.*
2. *Réciproquement, tout diviseur commun à a et b divise d.*
3. *On a la* ***relation de Bézout****:*

$$\exists (u, v) \in \mathbb{Z}^2, ua + vb = d.$$

4. *Si a et b sont deux entiers relatifs non nuls, alors*

$$\operatorname{pgcd}(a, b) = \max \left\{ n \in \mathbb{N} \;\middle|\; n \,\middle|\, a \text{ et } n \,\middle|\, b \right\}.$$

T 24 Déterminer le pgcd de 105 et 48.

R

- On a toujours $\operatorname{pgcd}(0,0)=0$.
- On a toujours $\operatorname{pgcd}(a,0)=|a|$.
- Si $a,b\in\mathbb{Z}$, $\operatorname{pgcd}(a,b)=\operatorname{pgcd}(|a|,|b|)$.
- a divise b si, et seulement si, $\operatorname{pgcd}(a,b)=|a|$.

R

☕ La relation divise est une relation d'ordre dans $\mathbb{N}$ (mais pas dans $\mathbb{Z}$). Pour tous $a,b\in\mathbb{N}$, le pgcd de a et b est le plus grand (pour la relation divise) des minorants (c'est-à-dire les diviseurs) de $\{a,b\}$. Autrement dit, $\operatorname{pgcd}(a,b)$ est la borne inférieure de $\{a,b\}$ pour la relation divise dans $\mathbb{N}$.

D 25 Soient $a, b \in \mathbb{Z}$. On dit que a et b sont **premiers entre eux** lorsque leur seuls diviseurs communs sont -1 et 1:

$$\forall d \in \mathbb{Z}, \left(d \,\Big|\, a \text{ et } d \,\Big|\, b \implies d = \pm 1\right).$$

T 26 **Égalité de Bézout**

Soient a et b deux entiers. Les assertions suivantes sont équivalentes

1. *Les entiers a et b sont premiers entre eux.*
2. $\mathrm{pgcd}(a, b) = 1$
3. $\exists (u, v) \in \mathbb{Z}^2, ua + vb = 1.$

D 27 Le nombre des entiers k vérifiant

$$1 \leq k \leq n \qquad \text{et} \qquad \operatorname{pgcd}(k, n) = 1$$

est noté $\varphi(n)$. L'application $\varphi : \mathbb{N}^\star \to \mathbb{N}^\star$ ainsi définie s'appelle **indicateur d'Euler**.

D 28 Soient $a_1, a_2, \ldots, a_r \in \mathbb{Z}$.

- On dit que $a_1, \ldots, a_r$ sont **premiers entre eux dans leur ensemble** si leurs seuls diviseurs communs sont ± 1.
- On dit que $a_1, \ldots, a_r$ sont **premiers entre eux deux à deux** a_i et a_j sont premiers entre eux pour tous $i, j \in [\![1, r]\!]$ distincts.

T 29 **Lemme de Gauß**

Si a est premier avec b et a divise bc, alors a divise c.

Démonstration. Il existe des entier u, v, w tel que $ua + vb = 1$ et $bc = aw$. On peut donc écrire

$$c = uac + vbc = uac + vaw = a(uc + vw).$$

∎

T 30 **Lemme d'Euclide**

Un entier $p \geq 2$ est un nombre premier si et seulement si il vérifie la condition

$$\forall (a,b) \in \mathbb{Z}^2, p \,\Big|\, ab \implies (p \,\Big|\, a \ \text{ou} \ p \,\Big|\, b);$$

appelée lemme d'Euclide.

Démonstration. C'est un cas particulier du lemme de Gauß. Ou bien p divise a, ou bien il est premier avec a et il divise alors b. ∎

C 31

1. *Si p premier divise $a_1 a_2 \cdots a_n$, il divise au moins l'un des facteurs.*
2. *Si p premier divise a^n, $(n \in \mathbb{N}^\star)$, alors il divise a.*

T 32

1. *Si* a *est premier avec* b *et* c, *alors* a *est premier avec* bc.
2. *Si* a *et* b *sont premiers entre eux, et que* $a \mid c$ *et* $b \mid c$, *alors* $ab \mid c$.

Démonstration. À faire (exercice!). ∎

T 33 *Soient des entiers a et b.*

1. *Soit k un entier, alors $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(a-kb,b)$.*
2. *Si $b>0$, $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(b,r)$ avec $r = a \mod b$.*
3. *Soit un entier $m>0$, alors $\operatorname{pgcd}(ma,mb) = m \times \operatorname{pgcd}(a,b)$.*
4. *Soit un entier $d>0$; si d divise a et b, soient a' et b' les entiers tels que $a = da'$ et $b = db'$. Alors d est le pgcd de a et b si, et seulement si, a' et b' sont premiers entre eux.*

A 34 **Algorithme d'Euclide**

On pose $r_0 = a$, $r_1 = b$, *puis pour tout* k *jusqu'à avoir* $r_N = 0$,

$$r_{k+2} = r_k \mod r_{k+1},$$

c'est-à-dire r_{k+2} *est le reste dans la division euclidienne de* r_k *par* r_{k+1}.
Alors $\mathrm{pgcd}(a, b) = r_{N-1}$.

E 35 On a $\mathrm{pgcd}(105, 48) = 3$.
En «remontant les calculs», cela permet de trouver des entiers $u, v \in \mathbb{Z}$ tels que

$$105u + 48v = 3.$$

D 37 Soient a et b deux entiers relatifs quelconques. On appelle **plus petit commun multiple** (ou ppcm) de a et b l'unique entier $m \geq 0$ tel que

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z},$$

on note cet entier $\mathrm{ppcm}(a, b)$ ou $a \vee b$.

T 38 *Soient a et b deux entiers relatifs quelconques et $m = \mathrm{ppcm}(a, b)$.*

1. *L'entier m est un multiple de a et de b.*
2. *Réciproquement, tout multiple commun à a et b est multiple de m.*
3. *Si a et b sont deux entiers relatifs non nuls, alors*

$$\mathrm{ppcm}(a, b) = \min\left(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^\star\right).$$

D 39 Soient $a_1, a_2, \dots, a_r \in \mathbb{Z}$.

- On appelle **plus grand commun diviseur** de $a_1, \dots, a_r$ l'unique entier naturel d pour lequel
$$a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_r\mathbb{Z} = d\mathbb{Z}.$$
- On appelle **plus petit commun multiple** de $a_1, \dots, a_r$ l'unique entier naturel m pour lequel
$$a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \cdots \cap a_r\mathbb{Z} = m\mathbb{Z}.$$

T 40 **Décomposition en facteurs premiers**

Soit $n \in \mathbb{N}$ tel que $n \geq 2$. Alors n admet une factorisation unique en facteurs premiers, à l'ordre des facteurs près, c'est-à-dire

$$\exists ! m \in \mathbb{N}^{\star}, \exists !(p_1, \ldots, p_m) \in \mathbb{P}^m, p_1 \leq p_2 \leq \cdots \leq p_m \text{ et } n = p_1 p_2 \cdots p_m.$$

E 41 $90 = 9 \times 10 = 3 \times 3 \times 2 \times 5 = 2 \times 3 \times 3 \times 5 = 2 \times 3^2 \times 5.$

D 42 La décomposition de $n \geq 2$ en facteurs premiers peut également s'écrire sous la forme

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdots p_r^{\alpha_r}$$

où

- les p_i sont des nombres premiers deux à deux distincts,
- $\alpha_i \geq 1$.

Cette écriture est unique, à l'ordre des facteurs près.

- L'entier α_i est appelé **exposant** du nombre premier p_i dans la décomposition de n en facteur premier et noté $v_{p_i}(n)$.
- Si p est un nombre premier distinct de $p_1, \dots, p_r$, on pose $v_p(n) = 0$.

On dit que $v_p(n)$ est la **valuation p-adique** de n, on a donc

$$v_p(n) = \max \left\{ k \in \mathbb{N} \;\middle|\; p^k \;\middle|\; n \right\}.$$

P 43 *Soit* $a, b \in \mathbb{N}^\star$, *et* $p \in \mathbb{P}$. *On a*

$$v_p(ab) = v_p(a) + v_p(b).$$

P 44 *Soit* $a, b \in \mathbb{N}^\star$, *alors* $a \,\Big|\, b$ *si, et seulement si*

$$\forall p \in \mathbb{P}, v_p(a) \leq v_p(b).$$

P 45 *Soit n un entier non nul qui se décompose en produit de facteurs premiers (distincts) de la façon suivante*

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

Alors, les diviseurs de n dans $\mathbb{N}^\star$ sont les entiers naturels de la forme

$$d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \cdots \cdots p_r^{\gamma_r}, \quad \textit{avec } 0 \leq \gamma_i \leq \alpha_i \textit{ pour } i = 1 \ldots r.$$

T 46 Quels sont les diviseurs de 90?

P 47 *Soit a et b deux entiers non nuls qui se décomposent en produits de facteurs premiers (distincts) de la façon suivante*

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdots p_r^{\alpha_r} \qquad\qquad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdots p_r^{\beta_r}$$

où les α_i et β_i sont des entiers éventuellement nuls. Alors

$$\mathrm{pgcd}(a, b) = p_1^{\min(\alpha_1,\beta_1)} \times p_2^{\min(\alpha_2,\beta_2)} \times \cdots \times p_r^{\min(\alpha_r,\beta_r)}$$

T 48 Retrouver le pgcd de 105 et 48.

P 49 *Soit a et b deux entiers non nuls qui se décomposent en produits de facteurs premiers (distincts) de la façon suivante*

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdots p_r^{\alpha_r} \qquad\qquad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdots p_r^{\beta_r}$$

où les α_i et β_i sont des entiers éventuellement nuls. Alors

$$\mathrm{ppcm}(a, b) = p_1^{\max(\alpha_1,\beta_1)} \times p_2^{\max(\alpha_2,\beta_2)} \times \cdots \times p_r^{\max(\alpha_r,\beta_r)}$$

P 50 *Soit de entiers $a > 0$ et $b > 0$. Si $d = \mathrm{pgcd}(a, b)$ et $m = \mathrm{ppcm}(a, b)$, alors $ab = dm$.*

Démonstration. On remarque que pour $x, y \in \mathbb{N}$, on a $x + y = \max(x, y) + \min(x, y)$.
Il suffit alors de comparer les exposants de p dans ab et dm : ils sont égaux. ∎

D 51 Soit $a, b, n \in \mathbb{Z}$ trois entiers. On défini la relation de congruence par

$$(a \equiv b \pmod{n}) \iff (\exists k \in \mathbb{Z}, a = b + kn)\,.$$

On dit que «a est **congru** à b **modulo** n». Les réels a et b diffèrent donc d'un multiple entier de n c'est-à-dire $x - y \in n\mathbb{Z}$.

P 52 *Soit $n \in \mathbb{Z}$. La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. La classe d'équivalence de $a \in \mathbb{Z}$ modulo n est*

$$a + n\mathbb{Z} = \{\, a + kn \mid k \in \mathbb{Z} \,\}\,.$$

E 53

- $230897 \equiv 7 \pmod{10}$.
- $17 \equiv 2 \pmod{3}$, mais aussi $17 \equiv -1 \pmod{3}$.

P 54 *Soit $a, b, r \in \mathbb{Z}$. Le reste de la division euclidienne de a par b est r si, et seulement si*

$$a \equiv r \pmod{b} \qquad \textit{et} \qquad 0 \leq r < b.$$

On a donc

$$b \,\Big|\, a \iff a \equiv 0 \pmod{b}.$$

P 55 *Soient* $n \in \mathbb{Z}^\star$, $a, b, c, d, k \in \mathbb{Z}$ *et* $p \in \mathbb{N}$.

1. *Si* $a \equiv b \pmod{n}$ *et* $c \equiv d \pmod{n}$, *alors*

$$a + c \equiv b + d \pmod{n}; \qquad a - c \equiv b - d \pmod{n}; \qquad ac \equiv bd \pmod{n}.$$

2. *Si* $a \equiv b \pmod{n}$, *alors*

$$ka \equiv kb \pmod{kn}; \qquad ka \equiv kb \pmod{n}; \qquad a^p \equiv b^p \pmod{n}$$

T 56 Démontrer la proposition précédente.

Soit un entier $n > 0$, et $a, b \in \mathbb{Z}$. On cherche les entiers $x \in \mathbb{Z}$ tels que

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

Tout revient à chercher $x \in \mathbb{Z}$ pour lequel il existe $y \in \mathbb{Z}$ tel que $ax + ny = b$. Ce problème a déjà été étudié et il admet des solutions si, et seulement si b est un multiple de $\operatorname{pgcd}(a, n)$.
On se limite désormais au cas où a est premier avec n. L'égalité de Bézout permet d'introduire $(u, v) \in \mathbb{Z}^2$ tel que

$$au + nv = 1.$$

On a $au \equiv 1 \pmod{n}$ et on dit que u est **un inverse modulo n** de a. Il y a unicité de u si l'on décide que $0 \leq u < n$.
Pour résoudre $ax \equiv b \pmod{n}$, multiplions par u:

$$aux \equiv ub \pmod{n}, \text{ c'est-à-dire } x \equiv ub \pmod{n}.$$

Inversement, et en remultipliant par n, on trouve comme solution du problème tout entier congru à $ub \pmod{n}$.

E 57 Résoudre $5x \equiv 9 \pmod{17}$.

T 58 **Théorème Chinois**

Soient $m_1, \dots, m_r$ *des entiers premiers entre eux deux à deux* ($m_i \geq 2$ *et* $r \geq 2$) *et* M *leur produit. Étant donnée des entiers* $a_1, \dots, a_r$*, considérons le système de congruences*

$$\forall i \in \{ 1, \dots, r \}, x \equiv a_i \pmod{m_i}. \tag{S}$$

Ce système possède une solution $x \in \mathbb{Z}$*, qui est unique modulo* M*.*

Démonstration. Commençons par l'unicité. Soient $x, y \in \mathbb{Z}$ deux solutions de (S). Pour tout i, $x \equiv a_i \equiv y \pmod{m_i}$, donc $x - y$ est multiple de m_i. Ainsi, $x - y$ est multiple du ppcm des m_i qui vaut M puisque les m_i sont premiers entre eux deux à deux. D'où
$x \equiv y \pmod{M}$.
Pour l'existence, supposons que $r = 2$. Puisque m_1 et m_2 sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que

$$um_1 + vm_2 = 1.$$

Posons $x_1 = vm_2 = 1 - um_1$ et $x_2 = um_1 = 1 - vm_2$. Alors

$$\begin{aligned} x_1 &\equiv 1 \pmod{m_1}, & x_2 &\equiv 0 \pmod{m_1}, \\ x_1 &\equiv 0 \pmod{m_2}, & x_2 &\equiv 1 \pmod{m_2}. \end{aligned}$$

Posons $x_0 = a_1x_1 + a_2x_2$. Alors x_0 est solution de (S), ainsi que tout $x \equiv x_0 \pmod{M}$.
Pour le cas général, on effectue une récurrence sur r. ∎

E 59 La preuve précédente fournit une méthode pratique de résolution du système. Résoudre par exemple

$$x \equiv 5 \pmod{17} \quad \text{et} \quad x \equiv 3 \pmod{23}. \tag{S}$$

Les nombre 17 et 23 étant premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $17u + 23v = 1$, par exemple $(u, v) = (-4, 3)$ convient. On pose $x_1 = 3{\times}23 = 69$ et $x_2 = 17{\times}(-4) = -68$. D'où une solution de (S)

$$x_0 = 5x_1 + 3x_2 = 5 \times 69 + 3 \times (-68) = 141.$$

Ensuite,

$$\begin{aligned}
& x \equiv 5 \pmod{17} \quad \text{et} \quad x \equiv 3 \pmod{23} \\
\iff & x \equiv x_0 \pmod{17} \quad \text{et} \quad x \equiv x_0 \pmod{23} \\
\iff & 17 \,\Big|\, (x - x_0) \quad \text{et} \quad 23 \,\Big|\, (x - x_0) \\
\iff & 391 \,\Big|\, (x - x_0) \qquad\qquad \text{car } \operatorname{pgcd}(17, 23) = 1.
\end{aligned}$$

Les solutions de (S) sont donc les entiers

$$x = 141 + 391k \quad \text{avec} \quad k \in \mathbb{Z}.$$

T 60 **Petit théorème de Fermat**

Soit p un nombre premier. Si $a \in \mathbb{Z}$ n'est pas multiple de p, on a

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

Démonstration. Supposons que a n'est pas divisible par p et notons

$$N = a \times 2a \times 3a \times \cdots \times (p-1)a = (p-1)!a^{p-1}.$$

Pour tout entier k, notons r_k le reste de la division euclidienne de ka par p. Alors

$$N \equiv r_1 \times r_2 \times \dots r_{p-1} \pmod{p}.$$

Montrons que $r_1, \dots, r_{p-1}$ sont tous distincts deux à deux. En effet, si $r_i = r_j$, alors $(i-j)a$ est divisible par p, donc, en utilisant le lemme d'Euclide, $(i-j)$ est aussi divisible par p. Or $-p < i-j < p$, on a donc nécessairement $i = j$.
De plus, en utilisant de nouveau le lemme d'Euclide, aucun ka n'est divisible par p, donc aucun r_k n'est nul. On en déduit alors que $(r_1, r_2, \dots, r_{p-1})$ est une permutation de $(1, 2, \dots, p-1)$ et donc

$$r_1 \times r_2 \times r_3 \times \dots r_{p-1} = (p-1)!$$

Finalement, on en déduit

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p},$$

autrement dit, $(p-1)!\left(a^{p-1}-1\right)$ est divisible par p. Puisque p est premier, p ne divise pas $(p-1)!$ et le lemme d'Euclide assure alors que $a^{p-1}-1$ est divisible par p. ∎

Démonstration. On peut également faire une démonstration par récurrence (voir en exercice). ∎

Un énoncé équivalent est

T 61 **Petit théorème de Fermat**

Soit p un nombre premier et $a \in \mathbb{Z}$. On a

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