Arithmétique

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

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ est l'ensemble des entiers naturels.
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ est l'ensemble des entiers relatifs.
$\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ (entiers strictement positifs) et $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ (entiers relatifs non nuls).

Dans le cours, entier sera synonyme d'entier relatif.

Remarque. Si a et b sont des entiers tels que $a < b$ alors $a \leq b - 1$ (et, de façon équivalente, $a + 1 \leq b$).
Par exemple, si $n > 0$ alors $n \geq 1$.

Propriété 1. Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

2 Divisibilité dans $\mathbb{Z}$

a) Diviseurs et multiples

Définition. Soit a et b deux entiers. On dit que a **divise** b s'il existe un entier k tel que $b = ka$. On note $a|b$.
On dit également que a est un **diviseur** de b ou que b est un **multiple** de a.

Exemples.
• 3 divise 6 car $6 = 2 \times 3$. -3 divise également 6 car $6 = (-2) \times (-3)$.
De façon générale, si $b|a$ alors $(-b)|a$.
• Pour tout $n \in \mathbb{Z}$, $n + 1$ divise $n^2 - 1$ car $n^2 - 1 = (n - 1)(n + 1)$.

Diviseurs particuliers.
• Tout entier a divise 0 car $0 = 0.a$, mais 0 ne divise aucun entier $b \neq 0$.
• Tout entier n admet $1, -1, n$ et $-n$ comme diviseurs car $n = 1 \times n = (-1) \times (-n)$.
• Les seuls diviseurs de 1 sont 1 et -1.

b) Propriétés

Soit a, b, c des entiers relatifs.

Propriété 2. Si $b \neq 0$ et a divise b alors $|a| \leq |b|$. En particulier, tout entier non nul a un nombre fini de diviseurs.

Preuve. On suppose dans un premier temps que a et b sont positifs. a divise b donc il existe un entier k tel que $b = ka$. Comme $b \neq 0$, on a $a \neq 0$ et $k \neq 0$. Comme il s'agit d'entiers naturels, $a \geq 1$ et $k \geq 1$. On a $b - a = a(k-1) \geq 0$ car $a \geq 1$ et $k - 1 \geq 0$. Donc $b - a \geq 0$. On a donc $1 \leq a \leq b$, autrement dit $a \in \{1, 2, \ldots, b\}$ qui est un ensemble fini.
On considère maintenant a et b des entiers relatifs. a divise b donc $|a|$ divise $|b|$. Par ce qui précède $1 \leq |a| \leq |b|$, autrement dit $a \in \{-|b|, \ldots, -1, 1, 2, \ldots, |b|\}$ qui est un ensemble fini. □

Propriété 3. Si a divise b et b divise a alors $a = b$ ou $a = -b$.

Preuve. a divise b donc il existe $k \in \mathbb{Z}$ tel que $b = ka$. b divise a donc il existe $k' \in \mathbb{Z}$ tel que $a = k'b$. On a alors $a = kk'a$. Si $a \neq 0$ alors $kk' = 1$, ce qui implique que k et k' sont tous les deux égaux à 1 ou à -1, et par conséquent $a = b$ ou $a = -b$. Si $a = 0$, alors $b = ka = 0$. □

Propriété 4. Si a divise b et b divise c alors a divise c.

Preuve. Par hypothèse, il existe des entiers k, k' tels que $b = ka$ et $c = k'b$. On a alors $c = kk'a$, donc $a|c$. □

Propriété 5. Si a divise b et c, alors, pour tous entiers n et m, a divise $nb + mc$.

Preuve. Par hypothèse, il existe des entiers k et k' tels que $b = ka$ et $c = k'a$. Donc $nb + mc = (nk + mk')a$ est un multiple de a. □

Conséquences : si a divise b et c, alors a divise nb (on prend $m = 0$), a divise $(b + c)$ (on prend $n = m = 1$), a divise $(b - c)$ (on prend $n = 1$, $m = -1$).

La propriété 5 se généralise sans difficulté à 3 termes ou plus.

Exemples.
• Pour tout $n \in \mathbb{Z}$, 3 divise $3n - 6$ car $3|3$ et $3|6$.

• Montrons que pour tout $n \in \mathbb{N}$, 9 divise $u_n = 4^n + 6n - 1$. On montre le résultat par récurrence[1] sur n.
– Initialisation : $u_0 = 0$ est divisible par 9.
– On suppose que 9 divise u_n. On écrit

$$u_{n+1} = 4 \cdot 4^n + 6(n + 1) - 1 = 4(u_n - 6n + 1) + 6(n + 1) - 1 = 4u_n - 18n + 9.$$

9 divise u_n (hypothèse de récurrence), et 9 divise 18 et 9, donc 9 divise $u_{n+1} = 4u_n + 18n - 9$.
– Conclusion : 9 divise u_n pour tout $n \in \mathbb{N}$.

3 Nombres premiers

a) Reconnaître un nombre premier

Définition. On dit qu'un entier naturel n est **premier** s'il a exactement 2 diviseurs positifs : 1 et n.

Remarque. 1 n'est pas premier, il a un seul diviseur positif, qui est 1.
0 n'est pas premier, il a une infinité de diviseurs.

Exemple. $2, 3, 5, 7$ sont des nombres premiers.

Lemme 6. Soit n un entier, $n \geq 2$. Son plus petit diviseur positif différent de 1 est un nombre premier.
En particulier, tout entier $n \geq 2$ a au moins un diviseur premier.

Preuve. L'ensemble des diviseurs positifs de n différents de 1 est non vide car il contient n. Donc il admet un plus petit élément qu'on note p (propriété 1). Soit d un diviseur positif de p distinct de 1. On a $d \leq p$ (propriété 2). De plus, $d|n$ (propriété 4 avec $d|p$ et $p|n$), donc $d \geq p$ par choix de p. Donc $d = p$. On en déduit que p a un unique diviseur positif différent de 1, donc p est un nombre premier. □

Propriété 7. Soit n un entier, $n \geq 2$. Si n n'est divisible par aucun nombre premier $p \leq \sqrt{n}$, alors n est un nombre premier.

Preuve. Soit $n \geq 2$. On suppose que n n'est pas premier. Soit p le plus petit diviseur positif de n différent de 1. Par le lemme 6, p est premier. On écrit $n = pq$, avec $q \in \mathbb{N}^*$. Si $q = 1$ alors $n = p$ est premier, ce qui est exclu, donc $q \geq 2$. Comme q est un diviseur positif de n différent de 1, $q \geq p$ par choix de p. Donc $n = pq \geq p^2$, autrement dit $p \leq \sqrt{n}$.
On vient de montrer que si n n'est pas premier alors n est divisible par un nombre premier $p \leq \sqrt{n}$. Par contraposée[2], on en déduit que si n n'est divisible par aucun nombre premier $p \leq \sqrt{n}$, alors n est premier. □

Application. On considère $n = 29$. On a $\sqrt{29} \simeq 5,4$. Les nombres premiers inférieurs à $\sqrt{29}$ sont $2, 3, 5$. Aucun ne divise 29, donc 29 est premier.

b) Ensemble des nombres premiers

Théorème 8. Il existe une infinité de nombres premiers.

Preuve. Faisons une preuve par l'absurde[3]. Supposons qu'il n'y a qu'un nombre fini de nombres premiers, notons-les $p_1, \ldots, p_n$. On pose $N = p_1 p_2 \cdots p_n + 1$. $N > 1$ donc N a au moins un diviseur premier p (lemme 6), et p est nécessairement égal à p_i pour un certain $i \in \{1, \ldots, n\}$. Donc p divise $p_1 p_2 \cdots p_n$. Or p divise également N, donc p divise $N - p_1 p_2 \cdots p_n = 1$ (propriété 5). C'est impossible. Conclusion : il existe une infinité de nombres premiers. □

[1] Un raisonnement par récurrence comporte toujours 3 étapes :
– Initialisation : on vérifie la propriété pour $n = n_0$.
– Passage de n à $n + 1$: on suppose que la propriété est vraie au rang $n \geq n_0$, on en déduit qu'elle est vraie au rang $n + 1$.
– Conclusion : la propriété est vraie pour tout $n \in \mathbb{N}$, $n \geq n_0$.

[2] Raisonnement par contraposée : on veut montrer que si la propriété P est vraie, alors la propriété Q est vraie aussi ; il est équivalent de montrer que si la propriété Q est fausse, alors la propriété P est fausse aussi.

[3] Raisonnement par l'absurde : on suppose que la propriété P est fausse, on en déduit un résultat impossible, on conclut que la propriété P est vraie.

c) Décomposition en produit de facteurs premiers

Théorème 9. Tout entier $n \geq 2$ peut s'écrire de façon unique

$$\boldsymbol{n = p_1 p_2 \cdots p_r},$$

où $r \in \mathbb{N}^*$ et $p_1, p_2, \ldots, p_r$ sont des nombres premiers tels que $p_1 \leq p_2 \leq \cdots \leq p_r$.

Remarque.
• Si $r = 1$, le produit est réduit à un facteur : $n = p_1$.
• Si les p_i ne sont pas ordonnés, la décomposition n'est pas unique. Par exemple, $6 = 2 \times 3 = 3 \times 2$.

Preuve.
Existence de la décomposition. Montrons par récurrence sur n que tout entier $n \geq 2$ peut s'écrire $n = p_1 p_2 \cdots p_r$, avec $p_1 \leq p_2 \leq \cdots \leq p_r$ des nombres premiers.
• *$n = 2$ est premier, on a la décomposition voulue avec $p_1 = 2$ et $r = 1$.*
• *Soit $n \geq 3$. Supposons que la propriété est vraie pour tout entier k tel que $2 \leq k \leq n-1$. Par le lemme 6, le plus petit diviseur positif de n différent de 1 est un nombre premier. On le note p_1. On pose $m = \frac{n}{p_1} \in \mathbb{N}^*$. On distingue deux cas :*
– *Si $m = 1$ alors $n = p_1$ et on a la décomposition voulue ($r = 1$).*
– *Si $m \geq 2$, on peut appliquer l'hypothèse de récurrence à m car $m = \frac{n}{p_1} \leq \frac{n}{2} < n$. On écrit $m = p_2 \cdots p_r$ avec $p_2 \leq \cdots \leq p_r$ des nombres premiers ($r \geq 2$ parce qu'il y a au moins un facteur dans la décomposition de m et qu'on a numéroté à partir de 2). On a alors $n = p_1 m = p_1 p_2 \ldots p_r$. Les nombres premiers $p_2, \ldots, p_r$ divisent n. Comme p_1 est le plus petit diviseur positif de n différent de 1, on a $p_1 \leq p_2 \leq \cdots p_r$. On a donc la décomposition voulue.*
• *Conclusion : tout entier $n \geq 2$ a une décomposition de la forme voulue.*

Unicité de la décomposition. Nous verrons la preuve de l'unicité après le théorème de Gauss (section 6). □

La preuve de l'existence de la décomposition en produit de facteurs premiers donne la méthode pour trouver en pratique cette décomposition.

Exemple. $180 = 2 \times 90 = 2 \times 2 \times 45 = 2 \times 2 \times 3 \times 15 = 2 \times 2 \times 3 \times 3 \times 5$.

Quand on a déjà un produit, il suffit de décomposer les facteurs. Exemple : $15 \times 10 = (3 \times 5) \times (2 \times 5) = 2 \times 3 \times 5 \times 5$.

Définition. Soit $n \in \mathbb{N}^*$ et p un nombre premier.
• Si p divise n, on dit que p est un **facteur premier** de n
• Le plus grand entier k tel que p^k divise n s'appelle **l'exposant de p dans n.**

Dans la décomposition en facteurs premiers, on regroupe les nombres premiers identiques et on écrit

$$\boldsymbol{n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}}$$

où $p_1, \ldots, p_s$ sont des nombres premiers tels que $p_1 < p_2 < \cdots < p_s$ et $\alpha_1, \ldots, \alpha_s$ sont des entiers strictement positifs.
L'exposant de p_i dans n est α_i. Si p n'apparaît pas dans la décomposition, son exposant est 0.

Exemple. n^2 n'a que des exposants pairs car $n^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_s^{2\alpha_s}$.
$180 = 2^2 \times 3^2 \times 5$ n'est pas un carré. $2^2 \times 7^6 = (2 \times 7^3)^2$ est un carré.

Application à la divisibilité :

Théorème 10. Soit a et b des entiers strictement positifs. Pour tout nombre premier p, notons $\alpha(p)$ l'exposant de p dans a et $\beta(p)$ l'exposant de p dans b. Alors a divise b si et seulement si pour tout nombre premier p on a $\alpha(p) \leq \beta(p)$.

Preuve. Si a divise b alors il existe un entier q tel que $b = aq$. La décomposition en facteurs premiers de b est obtenue en multipliant la décomposition de a par celle de q, donc $\beta(p) \geq \alpha(p)$ pour tout nombre premier p.
Réciproquement, supposons que $\alpha(p) \leq \beta(p)$ pour tout nombre premier p. Soit $p_1, \ldots, p_r$ l'ensemble des facteurs premiers de a et de b. On écrit

$$a = p_1^{\alpha(p_1)} p_2^{\alpha(p_2)} \cdots p_r^{\alpha(p_r)} \text{ et } b = p_1^{\beta(p_1)} p_2^{\beta(p_2)} \cdots p_r^{\beta(p_r)}.$$

On a alors $b = aq$ avec $q = p_1^{\beta(p_1)-\alpha(p_1)} p_2^{\beta(p_1)-\alpha(p_2)} \cdots p_r^{\beta(p_r)-\alpha(p_r)}$ (q est bien un entier car $\beta(p_i) - \alpha(p_i) \geq 0$ par hypothèse). Donc a divise b. □

Exemples.
• $15 = 3 \times 5 = 2^0 \times 3^1 \times 5^1$ divise $180 = 2^2 \times 3^2 \times 5^1$.
• $25 = 5^2$ ne divise pas 180.
• $20 = 2^2 \times 5$, donc les diviseurs positifs de 20 sont de la forme $2^\alpha 5^\beta$ avec $\alpha = 0$, 1 ou 2 et $\beta = 0$ ou 1.

d) Crible d'Ératosthène

Le crible d'Ératosthène[4] est un algorithme pour trouver tous les nombres premiers inférieurs à un entier N fixé.
– On écrit tous les entiers de 1 à N. On barre 1 qui n'est pas premier.
– Le premier entier non barré est 2, il est premier. On barre tous ses multiples sauf lui-même.
– Le premier entier non barré est 3, il est premier. On barre tous ses multiples sauf lui-même.
– On répète l'opération. À chaque étape, le premier entier non barré est premier (car il n'est divisible par aucun nombre premier plus petit). On s'arrête au moment où on considère un nombre premier $p > \sqrt{N}$ (les entiers n avec $\sqrt{N} < n \leq N$ qui ne sont pas encore barrés sont premiers car ils ne sont divisibles par aucun nombre premier $p \leq \sqrt{n}$).
– L'ensemble des nombres premiers inférieurs à N est alors l'ensemble des entiers non barrés.

Exemple avec $N = 100$.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Remarque. Quand on considère le nombre premier p, il suffit de barrer les multiples kp avec $k \geq p$ car les multiples plus petits ont déjà été barrés à une étape précédente.

[4] Ératosthène est un mathématicien et philosophe grec du IIIe siècle avant J.C.

4 Division euclidienne

Théorème 11. Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe des entiers q et r tels que $a = bq + r$ et $0 \leq r < b$. De plus, q et r sont uniques.

Preuve.
Existence de q et r. Supposons pour commencer que $a \in \mathbb{N}$. Comme $b \geq 1$, l'ensemble des $n \in \mathbb{N}$ tels que $bn > a$ est non vide, donc il a un plus petit élément $k \in \mathbb{N}$. Si $k = 0$ alors $a < 0 = kb$, ce qui est exclu, donc $k \geq 1$. Par conséquent, $k - 1 \in \mathbb{N}$ et $b(k-1) \leq a$ par choix de k (k est le plus petit entier n tel que $bn > a$, donc $n = k - 1$ ne vérifie pas cette inégalité). Posons $q = k - 1$. On a : $qb \leq a < (q+1)b = qb + b$. Si on pose $r = a - bq$, on a alors $0 \leq r < b$. Conclusion : $a = bq + r$ avec $0 \leq r < b$.

Supposons maintenant $a \in \mathbb{Z}$, $a < 0$. Posons $a' = -a > 0$. Par ce qui précède, il existe des entiers q' et r' tels que $a' = bq' + r'$ avec $0 \leq r' < b$.
• Si $r' = 0$, $a = -a' = -q'b$. On pose $q = -q'$ et $r = 0$, et on a bien $a = bq + r$.
• Si $r' > 0$, on écrit $a = (-q'b - r') - b + b = b(-q' - 1) + (b - r')$. On pose $q = -q' - 1$ et $r = b - r'$. On a $a = bq + r$ et comme $0 < r' < b$, on a $0 < r < b$. C'est l'écriture recherchée.

Unicité de q et r. Supposons que $a = bq_1 + r_1 = bq_2 + r_2$ avec $0 \leq r_1 < b$ et $0 \leq r_2 < b$. On a $b(q_1 - q_2) = r_2 - r_1$, donc $r_2 - r_1$ est un multiple de b. Si $r_2 - r_1 \neq 0$, alors $b \leq |r_2 - r_1|$ (propriété 2). Or $-b < r_2 - r_1 < b$, et donc $|r_2 - r_1| < b$. Par conséquent, $r_2 - r_1 = 0$, autrement dit $r_1 = r_2$. Comme $b \neq 0$, l'égalité $b(q_1 - q_2) = 0$ entraîne $q_1 - q_2 = 0$, soit $q_1 = q_2$. D'où l'unicité des entiers q et r. □

Définition. Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Effectuer la **division euclidienne** de a par b, c'est trouver les entiers q et r tels que $a = bq + r$ avec $0 \leq r < b$. q est le **quotient** et r est le **reste** de la division euclidienne de a par b.

La division euclidienne est la division avec reste qu'on apprend à l'école primaire. Si $a \geq 0$ alors $q \geq 0$.

Exemple. $a = 100$, $b = 7$.

100	7
−7	14
30	
−28	
2	

Le quotient est $q = 14$, le reste est $r = 2$.

Remarque. Le reste de la division euclidienne de a par b est nul si et seulement si b divise a.

Propriété 12. Soit $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ et $a = bq + r$ avec $0 \leq r < b$. Alors $q = \left[\frac{a}{b}\right]$ (partie entière de $\frac{a}{b}$).

Preuve. $\frac{a}{b} = \frac{bq+r}{b} = q + \frac{r}{b}$. $0 \leq \frac{r}{b} < 1$, *donc* $q \leq \frac{a}{b} < q + 1$. *Comme* $q \in \mathbb{Z}$, q *est la partie entière de* $\frac{a}{b}$. □

Les restes possibles de la division euclidienne de n par b sont $0, 1, 2, \ldots, b - 1$.
En prenant $b = 2$, on voit que tout entier n peut s'écrire sous la forme $n = 2q$ ($r = 0$) ou $n = 2q + 1$ ($r = 1$).
De même, tout entier n peut s'écrire sous la forme $n = 3k$ ou $n = 3k + 1$ ou $n = 3k + 2$ (en prenant $b = 3$).

Exemple. Soit $n \in \mathbb{Z}$. Montrons que $n(n + 1)$ est multiple de 2. On écrit $n = 2k + r$ avec $r = 0$ ou $r = 1$.
– Cas 1 : $r = 0$. $n = 2k$ donc $n(n + 1) = 2k(n + 1)$.
– Cas 2 : $r = 1$. $n = 2k + 1$ donc $n(n + 1) = n(2k + 2) = 2n(k + 1)$.
Dans les deux cas, $n(n + 1)$ est un multiple de 2.

5 PGCD et PPCM

a) PGCD

Soit a et b deux entiers non nuls. 1 divise a et b donc a et b ont au moins un diviseur commun. Comme a et b ont un nombre fini de diviseurs, ils ont un nombre fini de diviseurs communs. Ceci justifie la définition suivante.

Définition. Soit $a, b \in \mathbb{Z}^*$. Le plus grand entier qui divise à la fois a et b s'appelle le **plus grand commun diviseur** ou **pgcd** de a et b. On le note **pgcd(a, b)**.

Exemple. $\text{pgcd}(6, 9) = 3$ car les diviseurs positifs de 6 sont $1, 2, 3, 6$ et les diviseurs positifs de 9 sont $1, 3, 9$.

Remarques.
• $\text{pgcd}(a, b) \geq 1$ car 1 est un diviseur commun à a et b.
• $\text{pgcd}(a, b) = \text{pgcd}(b, a)$.
• $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$ car un nombre et son opposé ont les mêmes diviseurs. On peut donc toujours se ramener à des entiers strictement positifs.

Propriété 13. Soit $a, b \in \mathbb{N}^*$. Si a divise b alors $\text{pgcd}(a, b) = a$.

Preuve. Tout diviseur de a est un diviseur de b, et a est le plus grand diviseur de a. □

Application de la décomposition en facteurs premiers au calcul de pgcd :

Théorème 14. Soit $a, b \in \mathbb{N}^*$ et p un nombre premier. Soit $\alpha(p)$ l'exposant de p dans a et $\beta(p)$ l'exposant de p dans b. Alors l'exposant de p dans $\text{pgcd}(a, b)$ est $\min(\alpha(p), \beta(p))$.

Preuve. Soit d un diviseur positif commun à a et b. Pour tout nombre premier p, notons $\gamma(p)$ l'exposant de p dans d. d divise a donc $\gamma(p) \leq \alpha(p)$. De même, $\gamma(p) \leq \beta(p)$ car d divise b. Donc $\gamma(p) \leq \min(\alpha(p), \beta(p))$. Réciproquement, tout entier positif dont les exposants sont inférieurs où égaux à $\min(\alpha(p), \beta(p))$ est un diviseur commun à a et b. Le plus grand diviseur commun est donc obtenu quand pour tout nombre premier p, l'exposant est le plus grand possible, c'est-à-dire égal à $\min(\alpha(p), \beta(p))$. □

Exemple. $\begin{array}{rcl} a & = & 2^4 \times 5 \times 7^2 \\ & = & 2^4 \times 3^0 \times 5^1 \times 7^2 \end{array}$, $\begin{array}{rcl} b & = & 2^2 \times 3 \times 5^2 \\ & = & 2^2 \times 3^1 \times 5^2 \times 7^0 \end{array}$. $\text{pgcd}(a, b) = 2^2 \times 3^0 \times 5^1 \times 7^0 = 20$.

b) Algorithme d'Euclide

Lemme 15 (lemme d'Euclide[5]). Soit $a, b \in \mathbb{Z}^*$. S'il existe des entiers q et r avec $r \neq 0$ tels que $a = bq + r$ alors les diviseurs communs à a et b sont exactement les diviseurs communs à b et r, et $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Preuve. Soit d un diviseur commun à a et b. d divise a et b, donc d divise $a - bq = r$. Donc d est un diviseur commun à b et r.
Réciproquement, si d' un diviseur commun à b et r, alors d' divise $bq + r = a$. Donc d' est un diviseur commun à a et b.
On en déduit que les diviseurs communs à a et b sont exactement les diviseurs communs à b et r. En prenant le plus grand diviseur commun, on obtient $\text{pgcd}(a, b) = \text{pgcd}(b, r)$. □

Exemple. Calculons $d = \text{pgcd}(273, 12)$.
On fait la division euclidienne de 273 par 12 : $273 = 22 \times 12 + 9$. Donc $d = \text{pgcd}(12, 9)$.
On fait la division euclidienne de 12 par 9 : $12 = 9 + 3$. Donc $d = \text{pgcd}(9, 3)$.
Comme 3 divise 9, on obtient $d = 3$.

Algorithme d'Euclide.
Soit $a, b \in \mathbb{N}^*$. On cherche $d = \text{pgcd}(a, b)$. On effectue des divisions euclidiennes successives tant que le reste est non nul.

$$\begin{array}{rcll} a & = & bq_1 + r_1 & r_1 < b & d = \text{pgcd}(b, r_1) \\ b & = & r_1 q_2 + r_2 & r_2 < r_1 & d = \text{pgcd}(r_1, r_2) \\ r_1 & = & r_2 q_3 + r_3 & r_3 < r_2 & d = \text{pgcd}(r_2, r_3) \\ \vdots & & & & \\ r_{n-2} & = & r_{n-1} q_n + r_n & r_n < r_{n-1} & d = \text{pgcd}(r_{n-1}, r_n) \\ r_{n-1} & = & r_n q_{n+1} + 0 & r_{n+1} = 0 & \end{array}$$

r_k est une suite strictement décroissante d'entiers naturels donc, au bout d'un certain temps, on tombe sur un reste nul et l'algorithme s'arrête. Si $r_{n+1} = 0$ alors r_n divise r_{n-1}, donc $\text{pgcd}(r_{n-1}, r_n) = r_n$.

Théorème 16. Le pgcd de a et b est le dernier reste non nul obtenu par l'algorithme d'Euclide.

Remarque. Si $r_1 = 0$, c'est que b divise a, donc $\text{pgcd}(a, b) = b$ (l'algorithme s'arrête immédiatement).

Théorème 17. Soit $a, b \in \mathbb{Z}^*$. Si d divise a et b alors d divise $\text{pgcd}(a, b)$.

Preuve. On se place d'abord dans le cas où $a, b \in \mathbb{N}^*$. On reprend les notations de l'algorithme d'Euclide. Par le lemme d'Euclide, les diviseurs communs à a et b sont les diviseurs communs à b et r_1, à r_1 et r_2,..., à r_{n-1} et r_n. Comme r_n divise r_{n-1}, ce sont les diviseurs de r_n. Par conséquent, d divise r_n puisque c'est un diviseur commun à a et b. Or $r_n = \text{pgcd}(a, b)$ par l'algorithme d'Euclide.
Si $a, b \in \mathbb{Z}^*$, on se ramène au cas précédent en remarquant que les diviseurs communs à a et b sont les diviseurs communs à $|a|$ et $|b|$, et $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$. □

[5] Euclide est un célèbre mathématicien grec du IIIe siècle avant J.C.

Propriété 18. Si $a, b, k \in \mathbb{Z}^*$, $\text{pgcd}(ka, kb) = |k| \,\text{pgcd}(a, b)$.

Preuve. On se place d'abord dans le cas où $a, b, k \in \mathbb{N}^*$. On note $r_1, \ldots, r_n$ et $r_{n+1} = 0$ les restes obtenus en appliquant l'algorithme d'Euclide à a et b. $a = bq_1 + r_1$ avec $0 \leq r_1 < b$, donc $ka = kbq_1 + kr_1$ avec $0 \leq kr_1 < kb$, donc kr_1 est le reste de la division euclidienne de ka par kb. De même, si on calcule le pgcd de ka et kb avec l'algorithme d'Euclide, on trouve les restes successifs $kr_1, kr_2, \ldots, kr_n$ et $kr_{n+1} = 0$. Donc $\text{pgcd}(ka, kb) = kr_n = k \,\text{pgcd}(a, b)$.
Si $a, b \in \mathbb{Z}^*$, il suffit de remarquer que $\text{pgcd}(ka, kb) = \text{pgcd}(|ka|, |kb|) = |k| \,\text{pgcd}(|a|, |b|) = |k| \,\text{pgcd}(a, b)$. □

Exemple. $\text{pgcd}(1200, 900) = 100 \,\text{pgcd}(12, 9) = 100 \times 3 = 300$.

c) Nombres premiers entre eux

Définition. Soit a et b deux entiers non nuls. On dit que a et b sont **premiers entre eux** si $\text{pgcd}(a, b) = 1$. On dit aussi que a est premier avec b.

Exemples.
• 15 et 26 sont premiers entre eux.
• Deux nombres premiers différents sont premiers entre eux.

Propriété 19. Deux entiers strictement positifs sont premiers entre eux si et seulement s'il n'ont aucun facteur premier commun.

Preuve. C'est une conséquence du théorème 14. □

Propriété 20. Soit a, b deux entiers non nuls et $d = \text{pgcd}(a, b)$. Alors $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.

Preuve. Soit $e = \text{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right)$. Il faut montrer que $e = 1$. Comme e divise $\frac{a}{d}$ et $\frac{b}{d}$, il existe des entiers a', b' tels que $\frac{a}{d} = a'e$ et $\frac{b}{d} = b'e$, donc $a = a'ed$ et $b = b'ed$. ed est un diviseur commun à a et b, donc $ed \leq \text{pgcd}(a, b) = d$. Comme $d > 0$, on peut simplifier l'inégalité : $e \leq 1$. Or $e \geq 1$ car c'est un pgcd, donc $e = 1$. □

Une fraction est irréductible si le numérateur et le dénominateur sont premiers entre eux. Pour obtenir une fraction irréductible égale à $\frac{p}{q}$, il suffit de simplifier par le pgcd :
$\frac{p}{q} = \frac{p'}{q'}$ avec $p' = \frac{p}{pgcd(p,q)}$ et $q' = \frac{q}{pgcd(p,q)}$. Par la proposition 20, $\text{pgcd}(p', q') = 1$.

d) PPCM

Soit a et b deux entiers non nuls. ab est un multiple commun à a et b, $|ab| > 0$ aussi. Par conséquent, a et b ont au moins un multiple commun strictement positif, ce qui rend possible la définition suivante.

Définition. Soit a et b deux entiers non nuls. Le plus petit entier strictement positif qui est à la fois multiple de a et b s'appelle le **plus petit commun multiple** ou **ppcm** de a et b. On le note $\boldsymbol{\text{ppcm}(a, b)}$.

Exemple. $\text{ppcm}(4, 6) = 12$.
Le ppcm sert à mettre des fractions au même dénominateur : $\frac{1}{4} + \frac{1}{6} = \frac{3}{12} + \frac{2}{12} = \frac{5}{12}$.

Remarques.
• $\text{ppcm}(a, b) = \text{ppcm}(b, a)$.
• $\text{ppcm}(a, b) = \text{ppcm}(|a|, |b|)$ car un nombre et son opposé ont les mêmes multiples. On peut donc toujours se ramener à des entiers strictement positifs.

Propriété 21. Soit $a, b \in \mathbb{Z}^*$. Si c est un multiple commun à a et b, alors c est un multiple de $\text{ppcm}(a, b)$.

Preuve. On note $m = \text{ppcm}(a, b) \geq 1$. On fait la division euclidienne de c par m : $c = qm + r$ avec $0 \leq r < m$. a divise m et c, donc a divise $c - qm = r$. De même, b divise r. Par conséquent, r est un multiple commun à a et b avec $0 \leq r < m$. Comme m est le plus petit multiple commun strictement positif, on ne peut pas avoir $0 < r < m$. Donc $r = 0$, et c est un multiple de $m = \text{ppcm}(a, b)$. □

Application de la décomposition en facteurs premiers au calcul de ppcm :

Théorème 22. Soit $\boldsymbol{a, b \in \mathbb{N}^*}$ et $\boldsymbol{p}$ un nombre premier. Soit $\boldsymbol{\alpha(p)}$ l'exposant de $\boldsymbol{p}$ dans $\boldsymbol{a}$ et $\boldsymbol{\beta(p)}$ l'exposant de $\boldsymbol{p}$ dans $\boldsymbol{b}$. Alors l'exposant de $\boldsymbol{p}$ dans $\boldsymbol{\text{ppcm}(a, b)}$ est $\boldsymbol{\max(\alpha(p), \beta(p))}$.

La preuve est analogue à celle du théorème 14.

Exemple. $a = 2^4 \times 5 \times 7^2 = 2^4 \times 3^0 \times 5^1 \times 7^2$, $b = 2^2 \times 3 \times 5^2 = 2^2 \times 3^1 \times 5^2 \times 7^0$. $\text{ppcm}(a,b) = 2^4 \times 3^1 \times 5^2 \times 7^2$.

Théorème 23. Soit $a, b \in \mathbb{Z}^*$. Alors $\text{pgcd}(a,b).\text{ppcm}(a,b) = |ab|$.

Preuve. On se place d'abord dans le cas où $a, b \in \mathbb{N}^*$. Soit $p_1, \ldots, p_n$ les nombres premiers qui apparaissent dans les décompositions de a et b. On écrit $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$ (avec $\alpha_i, \beta_i \in \mathbb{N}$ pour $i \in \{1, \ldots n\}$). Par les théorèmes 14 et 22, on sait que

$$\text{pgcd}(a,b) = p_1^{\gamma_1} \cdots p_n^{\gamma_n} \text{ avec } \gamma_i = \min(\alpha_i, \beta_i) \text{ pour } i \in \{1, \ldots, n\},$$

$$\text{ppcm}(a,b) = p_1^{\delta_1} \cdots p_n^{\delta_n} \text{ avec } \delta_i = \max(\alpha_i, \beta_i) \text{ pour } i \in \{1, \ldots, n\}.$$

Si $\alpha_i \leq \beta_i$ alors $\gamma_i = \alpha_i$ et $\delta_i = \beta_i$. Si $\alpha_i > \beta_i$ alors $\gamma_i = \beta_i$ et $\delta_i = \alpha_i$. Dans les deux cas, $\gamma_i + \delta_i = \alpha_i + \beta_i$. Donc

$$\text{pgcd}(a,b).\text{ppcm}(a,b) = p_1^{\gamma_1+\delta_1} \cdots p_n^{\gamma_n+\delta_n} = p_1^{\alpha_1+\beta_1} \cdots p_n^{\alpha_n+\beta_n}.$$

Or $ab = p_1^{\alpha_1+\beta_1} \cdots p_n^{\alpha_n+\beta_n}$. Donc $\text{pgcd}(a,b).\text{ppcm}(a,b) = ab$.

Si $a, b \in \mathbb{Z}^*$, il suffit de remarquer que $\text{pgcd}(a,b).\text{ppcm}(a,b) = \text{pgcd}(|a|,|b|).\text{ppcm}(|a|,|b|) = |a||b|$. □

Il est facile de calculer le pgcd de deux entiers grâce à l'algorithme d'Euclide. Le théorème 23 permet de calculer le ppcm à partir du pgcd.

Exemple. Calculons $\text{ppcm}(792, 54)$. Appliquons tout d'abord l'algorithme d'Euclide :

$$\begin{aligned} 792 &= 54 \times 14 + 36 \\ 54 &= 36 \times 1 + 18 \\ 36 &= 18 \times 2 + 0 \end{aligned}$$

Donc $\text{pgcd}(792, 54) = 18$. On en déduit que $\text{ppcm}(792, 54) = \dfrac{792 \times 54}{18} = 2376$.

6 Théorèmes de Bézout et de Gauss

a) Théorème de Bézout

Théorème 24 (théorème de Bézout[6]). Soit a et b deux entiers non nuls. Il existe des entiers relatifs u et v tels que $au + bv = \text{pgcd}(a,b)$.

Preuve. Soit $E = \{au + bv \mid u \in \mathbb{Z}, v \in \mathbb{Z}, au + bv > 0\}$[7]. E un sous-ensemble de $\mathbb{N}$, et il est non vide car il contient $|a| = a \times (\pm 1) + b \times 0$. Il a donc un plus petit élément, qu'on appelle d. Comme d est un élément de E, il existe des entiers u_0 et v_0 tels que $d = au_0 + bv_0$. Nous allons montrer que $d = \text{pgcd}(a,b)$.

• *Montrons que d divise a. On effectue la division euclidienne de a par d : $a = qd + r$ avec $0 \leq r < d$.*

$$r = a - qd = a - q(au_0 + bv_0) = a(1 - qu_0) - bqv_0,$$

donc r est de la forme $au + bv$ avec $u = 1 - qu_0$ et $v = -qv_0$. Si $r > 0$, alors $r \in E$, donc $r \geq d$ (d est le plus petit élément de E). C'est impossible puisque $0 \leq r < d$. Par conséquent, $r = 0$ et d divise a.

• *De façon analogue, d divise b. Par conséquent, d est un diviseur commun à a et b, donc $d \leq \text{pgcd}(a,b)$.*

• *$\text{pgcd}(a,b)$ divise a et b, donc il divise $au_0 + bv_0 = d$. Donc $\text{pgcd}(a,b) \leq d$ (rappelons que $d > 0$).*

Conclusion : $\text{pgcd}(a,b) = d = au_0 + bv_0$. □

Théorème 25 (théorème de Bézout). Deux entiers non nuls a et b sont premiers entre eux si et seulement s'il existe des entiers u et v tels que $au + bv = 1$.

Preuve. Si $\text{pgcd}(a,b) = 1$, alors par le théorème 24, il existe des entiers u et v tels que $au + bv = 1$.
Réciproquement, supposons qu'il existe des entiers u et v tels que $au + bv = 1$. Soit $d = \text{pgcd}(a,b)$. d divise a et b, donc d divise $au + bv = 1$, donc $d \leq 1$. Or $d \geq 1$ (c'est un pgcd), donc $d = 1$. □

Exemple. n^2 et $n^2 + 1$ sont premiers entre eux car $(n^2 + 1) \times 1 + n^2 \times (-1) = 1$.

Remarque. Si $au + bv = c \neq 1$, c n'est pas nécessairement égal à $\text{pgcd}(a,b)$.
Exemple : $a = 4, b = 10$, $4a - b = 6$ et $\text{pgcd}(a,b) = 2$.

[6] Étienne Bézout est un mathématicien français du XVIIIe siècle.

[7] Notation d'un ensemble : $\{x \mid \ldots\}$ est l'ensemble des x tels que ... ("..." désigne les conditions vérifiées par x ou par les paramètres définissant x). On note également $\{x\ ;\ \ldots\}$ ou $\{x : \ldots\}$.

b) Comment trouver une relation de Bézout

Trouver une relation de Bézout pour a et b, c'est trouver des entiers u et v tels que $au + bv = \text{pgcd}(a, b)$.
On applique l'algorithme d'Euclide à a et b. On part de l'égalité donnant le pgcd, et on « remonte » l'algorithme.

Exemple. $a = 116, b = 10$

$$\begin{array}{rcll} 116 & = & 11 \times 10 + 6 & (L1) \\ 10 & = & 1 \times 6 + 4 & (L2) \\ 6 & = & 1 \times 4 + 2 & (L3) \\ 4 & = & 2 \times 2 + 0 & \end{array} \qquad \begin{array}{rcl} a & = & 11b + r_1 \\ b & = & r_1 + r_2 \\ r_1 & = & r_2 + \text{pgcd}(a, b) \end{array}$$

Par la ligne (L3), $\text{pgcd}(a, b) = 2$, et on a l'égalité : $\text{pgcd}(a, b) = r_1 - r_2$. $(*)$
On exprime r_2 (reste avec le numéro le plus élevé) à l'aide de (L2) : $r_2 = b - r_1$, puis on remplace dans $(*)$:

$$\text{pgcd}(a, b) = r_1 - (b - r_1) = 2r_1 - b. \quad (**)$$

On exprime r_1 à l'aide de (L1) : $r_1 = a - 11b$, puis on remplace dans $(**)$:

$$\text{pgcd}(a, b) = 2(a - 11b) - b = 2a - 23b.$$

$2a - 23b = 2$ est une relation de Bézout pour $a = 116$ et $b = 10$ ($u = 2, v = -23$).

Remarques.
• Une fois qu'on a calculé u et v, il est très facile de vérifier que $au + bv = \text{pgcd}(a, b)$.
• u et v ne sont pas uniques. Exemple : $7a - 81b = 2$ est une autre relation de Bézout pour $a = 116$ et $b = 10$.

Variante de l'algorithme (plus adapté à la programmation).
On applique l'algorithme d'Euclide à a et b. On note $q_1, \ldots, q_n$ les quotients et $r_1, \ldots, r_n$ les restes obtenus, avec r_n le dernier reste non nul.
– On pose $u_0 = 0$, $v_0 = 1$, $u_1 = 1$, $v_1 = -q_1$.
– Pour $i = 2, \ldots, n$, on définit u_i et v_i par récurrence : $u_i = u_{i-2} - q_i u_{i-1}$ et $v_i = v_{i-2} - q_i v_{i-1}$.
– On a la relation de Bézout suivante : $\boldsymbol{au_n + bv_n = \text{pgcd}(a, b)}$.
Cette égalité repose sur le résultat suivant, dont la preuve est laissée au lecteur :

Exercice. Vérifier que $au_i + bv_i = r_i$ pour tout $i \in \{0, \ldots, n\}$ (pour $i = 0$, on prend $r_0 = b$).

c) Théorème de Gauss

Théorème 26 (théorème de Gauss[8]). Soit a, b, c des entiers non nuls. Si a divise bc et si a est premier avec b, alors a divise c.

Preuve. Par le théorème de Bézout, il existe des entiers u et v tels que $au + bv = 1$. Donc $acu + bcv = c$ en multipliant par c. a divise bc par hypothèse, et a divise a, donc a divise $a(cu) + (bc)v = c$. □

Propriété 27. Soit a_1, a_2, b des entiers tels que a_1 et a_2 sont premiers entre eux. Si a_1 et a_2 divisent b, alors le produit $a_1 a_2$ divise b.

Preuve. a_1 divise b, donc il existe un entier b' tel que $b = b'a_1$. a_2 divise $b = b'a_1$ et $\text{pgcd}(a_1, a_2) = 1$, donc a_2 divise b' par le théorème de Gauss. Par conséquent, il existe b'' tel que $b' = b''a_2$, donc $b = b''a_1a_2$. □

Remarques.
• On peut avoir $a|bc$ avec a ne divisant ni b ni c. Exemple : $60 = 15 \times 4$, 6 divise 60 mais 6 ne divise ni 15 ni 4.
• La propriété 27 se généralise à 3 entiers ou plus : si $a_1, a_2, \ldots, a_n$ sont deux à deux premiers entre eux et divisent b, alors $a_1 a_2 \cdots a_n$ divise b. Exemple : si 5, 6 et 7 divisent n, alors n est un multiple de $5 \times 6 \times 7$.

d) Résoudre l'équation $ax + by = c$

On veut trouver toutes les solutions entières de l'équation :

$$ax + by = c \qquad (E)$$

où a, b, c sont des entiers donnés avec a, b non nuls, et x, y sont les inconnues.

Existence de solutions :

Théorème 28. L'équation (E) admet au moins une solution si et seulement si $\text{pgcd}(a, b)$ divise c.

Preuve. Supposons que (E) a une solution (x, y). $\text{pgcd}(a, b)$ divise a et b, donc il divise $ax + by = c$.
Réciproquement, supposons que $\text{pgcd}(a, b)$ divise c, autrement dit, il existe un entier c' tel que $c = c'\text{pgcd}(a, b)$. Par le théorème de Bézout, il existe des entiers u et v tels que $au + bv = \text{pgcd}(a, b)$. Alors $x_0 = c'u$ et $y_0 = c'v$ forment une solution de (E) car $ax_0 + by_0 = c'(au + bv) = c'\text{pgcd}(a, b) = c$. □

[8] Carl Friedrich Gauss est un célèbre mathématicien allemand – fin XVIIIe début XIXe siècle.

La preuve du théorème 28 indique comment trouver une solution particulière de (E).

Recherche de toutes les solutions.
On suppose que (x_0, y_0) est une solution de (E). Exprimons les autres solutions en fonction de (x_0, y_0).

$$ax + by = c \iff ax + by = ax_0 + by_0 \iff a(x - x_0) + b(y - y_0) = 0$$

Soit $X = x - x_0$ et $Y = y - y_0$. Pour résoudre (E), il est équivalent de résoudre

$$aX = -bY \quad (E').$$

Soit $a' = \frac{a}{\text{pgcd}(a,b)}$ et $b' = \frac{b}{\text{pgcd}(a,b)}$. L'équation (E') est équivalente à $a'X = -b'Y$.

a' et b' sont premiers entre eux (propriété 19) et b' divise $a'X$, donc b' divise X par le théorème de Gauss, autrement dit il existe $k \in \mathbb{Z}$ tel que $X = kb'$. On a alors $ka'b' = -b'Y$, et en simplifiant par $b' \neq 0$ on trouve $Y = -ka'$. On vient de montrer qu'une solution de (E') est nécessairement de la forme $X = kb', Y = -ka'$. On vérifie facilement que $X = kb', Y = -ka'$ est bien une solution de (E') pour tout $k \in \mathbb{Z}$. On a donc déterminé exactement les solutions de (E').

Par conséquent, l'ensemble des solutions de (E) est donné par $x = x_0 + kb', y = y_0 - ka'$, pour tous les $k \in \mathbb{Z}$.

$$\boldsymbol{S = \{(x_0 + kb', y_0 - ka') \mid k \in \mathbb{Z}\} \text{ avec } a' = \frac{a}{\text{pgcd}(a,b)} \text{ et } b' = \frac{b}{\text{pgcd}(a,b)}.}$$

Remarque. Si l'équation (E) a au moins une solution, alors elle a une infinité de solutions.

Exemple. Trouver toutes les solutions entières positives de $116x + 10y = 20$.
On résout d'abord l'équation dans $\mathbb{Z}$. C'est l'équation (E) avec $a = 116$, $b = 10$ et $c = 20$. On cherche ensuite les solutions vérifiant les conditions demandées.

Solution particulière : En b), on a vu que $\text{pgcd}(116, 10) = 2$ et que $116 \times 2 - 10 \times 23 = 2$ est une relation de Bézout pour a et b ($u = 2, v = -23$). $c = 10 \times \text{pgcd}(a, b)$, donc $x_0 = 10u = 20$ et $y_0 = 10v = -230$ conviennent.
Solution générale : la solution générale est (x, y) où $x = x_0 + k\frac{b}{\text{pgcd}(a,b)} = 20 + 5k$ et $y = y_0 - k\frac{a}{\text{pgcd}(a,b)} = -230 - 58k$, avec $k \in \mathbb{Z}$.
Solutions positives :
- $x = 20 + 5k \geq 0 \iff k \geq -\frac{20}{5} = -4$.
- $y = -230 - 58k \geq 0 \iff k \leq -\frac{230}{58} \approx -3,97 \iff k \leq -4$ (k est entier).
- x et y sont tous les deux positifs si et seulement si $k = -4$. Il y a donc une unique solution : $(x, y) = (0, 2)$.

e) Unicité de la décomposition en facteurs premiers

Nous avons vu en section 3 le théorème suivant :

Théorème 9. Tout entier $n \geq 2$ peut s'écrire de façon unique $n = p_1 p_2 \cdots p_r$, où $r \in \mathbb{N}^*$ et $p_1, p_2, \ldots, p_r$ sont des nombres premiers tels que $p_1 \leq p_2 \leq \cdots \leq p_r$.

Nous avons montré l'existence de cette décomposition, il restait à montrer son unicité .

Lemme 29. Soit $a_1, \ldots, a_n$ des entiers (où $n \in \mathbb{N}^*$), et p un nombre premier. Si p divise le produit $a_1 a_2 \ldots a_n$, alors p divise au moins un des entiers $a_1, \ldots, a_n$.

Preuve. On montre le résultat par récurrence sur $n \in \mathbb{N}^*$.
- *Si $n = 1$, alors p divise a_1.*
- *Supposons que le résultat est vrai pour $n \in \mathbb{N}^*$ et que p divise $a_1 \ldots a_n a_{n+1}$. Si p divise $a_1 \ldots a_n$, alors p divise un des entiers $a_1, \ldots, a_n$ par hypothèse de récurrence. Si p ne divise pas $b = a_1 \ldots a_n$ alors b et p sont premiers entre eux car les seuls diviseurs positifs de p sont 1 et p. p divise ba_n, donc p divise a_{n+1} d'après le théorème de Gauss.*
- *Conclusion : le résultat est vrai pour tout entier $n \geq 1$.* □

Preuve de l'unicité de la décomposition en facteurs premiers.
Supposons que $n = p_1 p_2 \cdots p_r = q_1 q_2 \ldots, q_s$, avec $p_1 \leq \cdots \leq p_r$, $q_1 \leq \cdots \leq q_s$ des nombres premiers. Commençons par montrer que $p_1 = q_1$. p_1 divise $q_1 \cdots q_s$ donc par le lemme 29, p_1 divise q_j pour un certain entier $j \in \{1, \ldots, s\}$. Si $p_1 < q_1$, alors $p_1 < q_j$, donc p_1 ne divise pas q_j (les seuls diviseurs positifs de q_j sont 1 et q_j). C'est absurde. On en déduit que $p_1 \geq q_1$. Un raisonnement analogue montre que $q_1 \geq p_1$. Donc $p_1 = q_1$. Montrons l'unicité de la décomposition par récurrence sur r (nombre de facteurs premiers).
- *Si $r = 1$ alors $n = p_1$. Or $p_1 = q_1$ donc $n = q_1$ et $s = 1$.*
- *Si $r > 1$, posons $n' = \frac{n}{p_1}$. Alors $n' = p_2 \ldots p_r$ (produit de $r - 1$ facteurs premiers) et $n' = q_2 \ldots q_s$. On applique l'hypothèse de récurrence à n' et on obtient : $r = s$, $p_2 = q_2, \ldots, p_r = q_r$.*
- *Conclusion : si $n = p_1 p_2 \cdots p_r = q_1 q_2 \ldots, q_s$ comme ci-dessus, alors $r = s$ et $p_1 = q_1, \ldots, p_r = q_r$.* □

7 Congruences

Dans la suite, on considère un entier $n \geq 2$.

a) Définition et propriétés

Définition. Soit $a, b \in \mathbb{Z}$. On dit que $\boldsymbol{a}$ **et congru à** $\boldsymbol{b}$ **modulo** $\boldsymbol{n}$ si $a - b$ est un multiple de n. On dit aussi que a et b sont congrus modulo n. On note $a \equiv b\ (n)$.

$a \equiv b\ (n) \iff \exists k \in \mathbb{Z}, a = b + kn$
$a \equiv 0\ (n) \iff n|a$.

Propriété 30. Soit $a \in \mathbb{Z}$. Il existe un unique entier r tel que $a \equiv r\ (n)$ et $0 \leq r \leq n-1$. r est le reste de la division euclidienne de a par n.

Exemple. Que jour de la semaine sera le 6 octobre 2007 ? Les jours de la semaine correspondent aux congruences modulo 7 (lundi : $1\ (n)$, mardi : $2\ (n)$, ...vendredi : $5\ (n)$,...). Le 6 octobre 2006 est un vendredi, le 6 octobre 2007 est dans 365 jours. $5 + 365 = 370$ et $370 \equiv 6\ (n)$. Donc le 6 octobre 2007 sera un samedi.

Propriétés 31. Soit $a, b, c \in \mathbb{Z}$.
• $a \equiv a\ (n)$.
• si $a \equiv b\ (n)$ alors $b \equiv a\ (n)$.
• si $a \equiv b\ (n)$ et $b \equiv c\ (n)$ alors $a \equiv c\ (n)$.

Preuve. Les deux premiers points sont immédiats.
Si $a \equiv b\ (n)$ et $b \equiv c\ (n)$, alors n divise $a-b$ et $b-c$, donc n divise $(a-b)+(b-c) = a-c$, donc $a \equiv c\ (n)$ □

Remarque. En raison de ces trois propriétés, on dit que la congruence modulo n est une relation d'équivalence (comme l'égalité ou le parallélisme de droites).

b) Compatibilité avec les opérations

Propriétés 32. Soit $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b\ (n)$ et $c \equiv d\ (n)$. Alors
• $a + c \equiv b + d\ (n)$.
• $ac \equiv bc\ (n)$.
• pour tout entier $k \geq 1$, $a^k \equiv b^k\ (n)$.

Preuve.
• *n divise $a-b$ et $c-d$, donc n divise $(a-b)+(c-d) = (a+c)-(b+d)$, c'est-à-dire $a + c \equiv b + d\ (n)$.*
• *$ac - bd = a(c-d) + ad - bd = a(c-d) + (a-b)d$. Comme $c-d$ et $a-b$ sont des multiples de n, $ac-bd$ est également multiple de n. Autrement dit, $ac \equiv bc\ (n)$.*
• *Du point précédent appliqué à $a \equiv b\ (n)$, on trouve $a^2 \equiv b^2\ (n)$. En réutilisant la propriété précédente, on trouve $a^3 \equiv b^3\ (n)$,...$a^k \equiv b^k\ (n)$.* □

On utilise souvent les deux premières propriétés 32 sous la forme suivante :
si $a \equiv b\ (n)$ alors $a + c \equiv b + c\ (n)$ et $ac \equiv bc\ (n)$.

Remarque. Si $ac \equiv bc\ (n)$, on ne peut pas simplifier par c, même si $c \not\equiv 0$. Exemple : $6 \equiv 2\ (4)$ mais $3 \not\equiv 1\ (4)$.

Exemples.
• Calculer $16^k\ (n)$ pour tout $k \in \mathbb{N}$. $16 \equiv -1\ (17)$. Donc $16^k \equiv (-1)^k\ (17)$ pour tout $k \geq 1$. Et $16^0 = 1 = (-1)^0$. Donc $16^k \equiv (-1)^k\ (17)$ pour tout entier $k \geq 0$.

• Quelles sont les valeurs possibles de $a^2\ (5)$? Peut-on avoir $a^2 \equiv 2\ (5)$?
Pour tout $a \in \mathbb{Z}$, il existe r tel que $a \equiv r\ (5)$ avec $0 \leq r < 5$. Il y a donc 5 cas :
– si $a \equiv 0\ (5)$ alors $a^2 \equiv 0\ (5)$.
– si $a \equiv 1\ (5)$ alors $a^2 \equiv 1\ (5)$.
– si $a \equiv 2\ (5)$ alors $a^2 \equiv 4\ (5)$.
– si $a \equiv 3\ (5)$ alors $a^2 \equiv 9 \equiv 4\ (5)$.
– si $a \equiv 4\ (5)$ alors $a^2 \equiv 16 \equiv 1\ (5)$.
Conclusion : a^2 est congru à $0, 1$ ou 4 modulo 5. On n'a jamais $a^2 \equiv 2\ (5)$.

Remarque : si $a \equiv 4\ (5)$, alors $a \equiv -1\ (5)$ et $a^2 \equiv 1\ (5)$. De même, si $a \equiv 3\ (5)$, alors $a \equiv -2\ (5)$ et $a^2 \equiv 4\ (5)$. C'est un calcul déjà fait pour $a \equiv 2\ (5)$.

Quand on fait des calculs (notamment des puissances), il peut être intéressant de prendre comme représentants des nombres (positifs ou négatifs) avec la plus petite valeur absolue.

c) Critères de divisibilité

Divisibilité par 9
$10 \equiv 1\ (9)$ donc $10^n \equiv 1^n \equiv 1\ (9)$ pour tout entier $n \geq 1$. De plus, $10^0 = 1$ donc $10^n \equiv 1\ (9)$ pour tout $n \in \mathbb{N}$.

$243 = 2 \times 10^2 + 4 \times 10^1 + 3 \times 10^0$ (c'est la définition de l'écriture en base 10). Donc
$243 \equiv 2 \times 1 + 4 \times 1 + 3 \times 1\ (9) \equiv 2 + 4 + 3\ (9) \equiv 0\ (9)$. Donc 243 est un multiplie de 9.

De façon générale, si l'entier N s'écrit $a_k a_{k-1} \dots a_1 a_0$ en base 10, alors $N = a_k 10^k + \dots + a_1 10^1 + a_0 10^0$ et $N \equiv a_k + a_{k-1} + \dots + a_1 + a_0\ (9)$. Par conséquent, N est multiple de 9 si et seulement si la somme de ses chiffres est multiple de 9.

Exemple : $9764 \equiv 9 + 7 + 6 + 1\ (9) \equiv 26\ (9) \equiv 2 + 6\ (9) \equiv 8\ (9)$ donc 9764 n'est pas multiple de 9.

Divisibilité par 3
$10 \equiv 1\ (3)$, donc le même raisonnement que pour 9 montre qu'un entier N est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

Divisibilité par 5 et par 2
$10 \equiv 0\ (5)$ donc $10^n \equiv 0\ (5)$ pour tout entier $n \geq 1$.
Si l'entier N s'écrit $a_k a_{k-1} \dots a_1 a_0$ en base 10, alors $N \equiv a_0\ (5)$. Donc N est divisible par 5 si et seulement si a_0 est divisible par 5, c'est-à-dire $a_0 = 0$ ou 5.

De même, $10 \equiv 0\ (2)$ donc $N \equiv a_0\ (2)$ et N est divisible par 2 si et seulement si a_0 est un chiffre pair.

Pourquoi a-t-on des critères de divisibilité pour ces valeurs-là ?
On est en base 10. $9 = 10 - 1$, *c'est pour cela que* $10 \equiv 1\ (9)$, *ce qui conduit au critère de divisibilité par* 9. *Comme* 3 *divise* 9, *on a également* $10 \equiv 1\ (3)$ *et on a un critère analogue pour* 3.
5 *est un diviseur de* 10, *donc* $10 \equiv 0\ (5)$, *ce qui conduit au critère de divisibilité par* 5. *De même pour* 2, *qui est un autre diviseur de* 10.

Si on était en base 16 *(base utilisée en informatique), on aurait un critère de divisibilité par* $15 = 16 - 1$, *analogue à celui par* 9 *en base* 10. *On aurait également des critères de divisibilité pour les diviseurs de* 15 *et pour les diviseurs de* 16.

8 $\mathbb{Z}/n\mathbb{Z}$

On considère un entier $n \geq 2$.

a) Définition

Définition. Soit $a \in \mathbb{Z}$. La **classe de congruence modulo n** de a est l'ensemble $\{x \in \mathbb{Z} \mid x \equiv a\ (n)\} = \{a + kn \mid k \in \mathbb{Z}\}$. On note cette classe $\overline{a}$.
$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes de congruence modulo n : $\mathbb{Z}/n\mathbb{Z} = \{\overline{a} \mid a \in \mathbb{Z}\}$.

Propriété 33. $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ a n éléments.

Preuve. Par définition, $\overline{a} = \overline{b}$ *si et seulement si* $a \equiv b\ (n)$. *Or, pour tout entier* a, *il existe un unique entier* r *tel que* $a \equiv r\ (n)$ *et* $0 \leq r \leq n-1$. *Donc* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$, *et ces classes sont différentes par unicité de* r, *donc* $\mathbb{Z}/n\mathbb{Z}$ *a bien* n *éléments.* □

Remarque. On peut choisir d'autres représentants pour les classes de congruence.
Exemple : $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \{\overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}\}$ car $4 \equiv -1\ (5)$ et $3 \equiv -2\ (5)$.
$\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\} = \{\overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

De façon générale :
$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{-\frac{n-1}{2}}, \dots, \overline{-1}, \overline{0}, \overline{1}, \dots, \overline{\frac{n-1}{2}}\right\}$ si n est impair, $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{-\left(\frac{n}{2}-1\right)}, \dots, \overline{-1}, \overline{0}, \overline{1}, \dots, \overline{\frac{n}{2}}\right\}$ si n est impair.

b) Opérations dans $\mathbb{Z}/n\mathbb{Z}$

Soit $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$ et $a, b \in \mathbb{Z}$ tels que $\alpha = \overline{a}$ et $\beta = \overline{b}$. On définit $\alpha + \beta = \overline{a+b}$ et $\alpha\beta = \overline{ab}$.

Ces opérations sont bien définies car le résultat est indépendant du choix des représentants a *et* b *: si* $\overline{a} = \overline{a'}$ *et* $\overline{b} = \overline{b'}$, *alors* $a \equiv a'\ (n)$ *et* $b \equiv b'\ (n)$. *Or* $a + b \equiv a' + b'\ (n)$ *et* $ab \equiv a'b'\ (n)$, *donc* $\overline{a+b} = \overline{a'+b'}$ *et* $\overline{ab} = \overline{a'b'}$.

Propriété 34. Dans $\mathbb{Z}/n\mathbb{Z}$, $\overline{0}$ est le neutre pour l'addition et $\overline{1}$ est le neutre pour la multiplication :
$\forall \alpha \in \mathbb{Z}/n\mathbb{Z}$, $\alpha + \overline{0} = \alpha$ et $\overline{1}\alpha = \alpha$.

Exemple. Tables d'addition et de multiplication dans $\mathbb{Z}/6\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Remarque. Si $\alpha\beta = \overline{0}$, on n'a pas nécessairement $\alpha = \overline{0}$ ou $\beta = \overline{0}$. Exemple : dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{2}.\overline{3} = \overline{0}$.

c) Éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$

Si on a l'égalité $\alpha\beta = \alpha\gamma$ dans $\mathbb{Z}/n\mathbb{Z}$, on ne peut pas toujours simplifier par α.
Dans $\mathbb{R}$, simplifier c'est multiplier par l'inverse. Tout réel non nul a un inverse.
Dans $\mathbb{Z}/n\mathbb{Z}$, seuls certains éléments ont un inverse.

Théorème 35. Soit $\alpha = \overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Il existe un élément $\beta \in \mathbb{Z}/n\mathbb{Z}$ tel que $\alpha\beta = \overline{1}$ si et seulement si a et n sont premiers entre eux. Si β existe, il est unique, et β et appelé l'inverse de α dans $\mathbb{Z}/n\mathbb{Z}$.

Preuve. $\alpha = \overline{a}$ *est inversible si et seulement s'il existe* $\beta = \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ *tel que* $\alpha\beta = \overline{1}$*, ce qui s'écrit également* $ab \equiv 1\ (n)$*. Autrement dit,* $\alpha = \overline{a}$ *est inversible si et seulement s'il existe des entiers* b *et* k *tels que* $ab = 1 + kn$*.*

• *Si* α *est inversible, alors il existe* b, k *tels que* $ab = 1 + kn$*, autrement dit* $ab - kn = 1$*. Donc* a *et* n *sont premiers entre eux par le théorème de Bézout.*

• *Réciproquement, si* a *et* n *sont premiers entre eux, alors il existe* u_0 *et* v_0 *tels que* $au_0 + nv_0 = 1$ *(théorème de Bézout). Si on prend* $b = u_0$*,* $\beta = \overline{b}$ *et* $k = -v_0$*, alors* $ab - kn = 1$*, c'est-à-dire* $\alpha\beta = \overline{1}$*. Donc* α *est inversible. Montrons que* β *est unique. L'ensemble des* u, v *tels que* $au + bv = 1$ *est* $u = u_0 + nm, v = v_0 - am$*,* $m \in \mathbb{Z}$*. Donc l'ensemble des* b *tels que* $ab \equiv 1\ (n)$ *est* $b = u_0 + nm, m \in \mathbb{Z}$*. Donc* $b \equiv u_0\ (n)$ *pour tout* m*, c'est-à-dire que tous les* b *solutions sont dans la même classe de congruence modulo* n*. Donc* $\beta = \overline{u_0} = \overline{b}$ *est l'unique inverse de* α *dans* $\mathbb{Z}/n\mathbb{Z}$*.* □

Éléments particuliers.
• $\overline{0}$ n'est jamais inversible.
• $\overline{1}$ est toujours inversible, d'inverse $\overline{1}$.
• $\overline{n-1} = \overline{-1}$ est toujours inversible, d'inverse $\overline{-1}$.

Remarque. L'inverse de $\alpha \in \mathbb{Z}/n\mathbb{Z}$ est noté α^{-1}. Mais attention avec cette notation : l'inverse de $\overline{2}$ n'est pas $\frac{\overline{1}}{2}$ ou $\overline{2^{-1}}$ ($2^{-1} = \frac{1}{2}$ n'est pas un entier !), c'est $(\overline{2})^{-1}$.

La preuve du théorème 35 indique comment calculer l'inverse de $\overline{a}$: en cherchant une relation de Bézout entre a et n. Il n'y a pas de méthode directe.

Exemple. On se place dans $\mathbb{Z}/9\mathbb{Z}$. 9 est premier avec $1, 2, 4, 5, 7, 8$ et n'est pas premier avec $0, 3, 6$, donc les éléments inversibles sont $\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}$. Cherchons les inverses.
• L'inverse de $\overline{1}$ est $\overline{1}$, l'inverse de $\overline{-1} = \overline{8}$ est $\overline{-1} = \overline{8}$.
• $9 - 4 \times 2 = 1$ est une relation de Bézout entre 9 et 2, donc $\overline{-4}.\overline{2} = \overline{1}$. L'inverse de $\overline{2}$ est $\overline{-4} = \overline{5}$. On en déduit que l'inverse de $\overline{5}$ est $\overline{2}$. On en déduit également $\overline{-2}.\overline{4} = \overline{1}$, donc $\overline{-2} = \overline{7}$ et $\overline{4}$ sont inverses l'un de l'autre.

On a ainsi trouvé tous les inverses :

classe	inverse
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{7}$
$\overline{5}$	$\overline{2}$
$\overline{7}$	$\overline{4}$
$\overline{8}$	$\overline{8}$

Propriété 36. Si $\alpha = \overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible alors :
• $\forall b, c \in \mathbb{Z},\ \ ab \equiv ac\ (n) \iff b \equiv c\ (n)$.
• $\forall \beta, \gamma \in \mathbb{Z}/n\mathbb{Z},\ \ \alpha\beta = \alpha\gamma \iff \beta = \gamma$.

Preuve. On sait que $b \equiv c\ (n)$ entraîne que $ab \equiv ac\ (n)$. Montrons la réciproque. Soit $\overline{u}$ l'inverse de $\overline{a}$ dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire $ua \equiv 1\ (n)$. Si $ab \equiv ac\ (n)$, alors $uab \equiv uac\ (n)$, donc $b \equiv c\ (n)$.
Les égalités dans $\mathbb{Z}/n\mathbb{Z}$ s'en déduisent. □

Théorème 37.
Si p est un nombre premier, tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles sauf $\overline{0}$.
Si n n'est pas un nombre premier, il existe au moins un élément différent de $\overline{0}$ qui n'est pas inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Preuve.
Soit p un nombre premier et $a \in \mathbb{Z}$. Si p divise a, alors $\overline{a} = \overline{0}$. Si p ne divise pas a, alors a et p sont premiers entre eux, donc $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ par le théorème 35.
Si n n'est pas premier, il existe en entier d qui divise n et tel que $1 < d < n$. $\overline{d} \neq \overline{0}$ et d n'est pas premier avec n donc $\overline{d}$ n'est pas inversible. □

9 Résoudre l'équation $ax \equiv b\ (n)$

On veut trouver toutes les solutions entières de l'équation :

$$ax \equiv b\ (n) \qquad (E)$$

où a et b sont des entiers donnés avec a non nul, et où $x \in \mathbb{Z}$ est l'inconnue.

Cas où a et n sont premiers entre eux.
Dans ce cas, $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ (théorème 35). Soit $u \in \mathbb{Z}$ tel que $\overline{u}$ est l'inverse de $\overline{a}$. Par la propriété 36, l'équation (E) est équivalente à $uax \equiv ub\ (n)$, c'est-à-dire $x \equiv ub\ (n)$.

Conclusion : l'ensemble des solutions de (E) est $\{x \in \mathbb{Z} \mid x \equiv ub\ (n)\} = \{ub + kn \mid k \in \mathbb{Z}\}$. Il y a une infinité de solutions dans $\mathbb{Z}$.

Exemple. Résoudre dans $\mathbb{Z}$ l'équation $2x \equiv 3\ (9)$.
2 et 9 sont premiers entre eux, et on a vu que l'inverse de $\overline{2}$ dans $\mathbb{Z}/9\mathbb{Z}$ est $\overline{5}$. Donc cette équation est équivalente à $x \equiv 5 \cdot 3\ (9)$. Donc x est solution si et seulement si $x \equiv 6\ (9)$. Autrement dit, $S = \{6 + 9k \mid k \in \mathbb{Z}\}$.

Cas où a et n ne sont pas premiers entre eux.
(E) $\iff \exists k \in \mathbb{Z}, ax - b = kn$.
Soit $d = \text{pgcd}(a, n)$. Si (E) admet une solution x, alors d divise n et a, donc d divise $ax - kn = b$. Dans ce cas, on peut simplifier par $d \neq 0$: on pose $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $n' = \frac{n}{d}$, et l'égalité $ax - b = kn$ est équivalente à $a'x - b' = kn'$.
On en déduit que (E) est équivalente à l'équation $a'x \equiv b'\ (n')$.

Conclusion :
– si $\text{pgcd}(a, n)$ ne divise pas b, il n'y a pas de solution.
– si $\text{pgcd}(a, n)$ divise b, on divise a, b et n par $\text{pgcd}(a, n)$ et on se ramène à l'équation (E') : $a'x \equiv b'\ (n')$ avec a' et n' premiers entre eux.

Exemples.
• Résoudre dans $\mathbb{Z}$ l'équation (E) : $6x \equiv 3\ (9)$.
$\text{pgcd}(6, 9) = 3$, il divise $b = 3$. Donc l'équation (E) est équivalente à (E') : $2x \equiv 1\ (3)$.
$\overline{2} = \overline{-1}$ dans $\mathbb{Z}/3\mathbb{Z}$, donc son inverse est $\overline{-1} = \overline{2}$. L'équation (E') est donc équivalente à $x \equiv 2\ (3)$. Conclusion : l'ensemble des solutions de (E) est $S = \{2 + 3k \mid k \in \mathbb{Z}\}$.

• Résoudre dans $\mathbb{Z}$ l'équation $4x \equiv 5\ (6)$. $\text{pgcd}(4, 6) = 2$, il ne divise pas 5 donc il n'y a pas de solution : $S = \emptyset$.

Équation dans $\mathbb{Z}/n\mathbb{Z}$.
On veut résoudre $\alpha X = \beta$, où $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$ sont donnés $\alpha \neq \overline{0}$, et où $X \in \mathbb{Z}/n\mathbb{Z}$ est l'inconnue.
On se ramène à résoudre $ax \equiv b\ (n)$, avec $\alpha = \overline{a}$, $\beta = \overline{b}$ et $X = \overline{x}$.

Exemples.
• Résoudre $\overline{2}X = \overline{3}$ dans $\mathbb{Z}/9\mathbb{Z}$.
On a vu que x est solution de $2x \equiv 3\ (9)$ si et seulement si $x \equiv 6\ (9)$, autrement dit $\overline{x} = \overline{6}$.
Conclusion : il y a une unique solution dans $\mathbb{Z}/9\mathbb{Z}$, qui est $\overline{6}$.

• Résoudre $\overline{6}X = \overline{3}$ dans $\mathbb{Z}/9\mathbb{Z}$.
On a vu que x est solution de $6x \equiv 3\ (9)$ si et seulement si $x \equiv 2\ (3)$. Quelle est la classe d'équivalence de x modulo 9 ? Si on écrit $x = 9q + r$ avec $0 \leq r \leq 8$, alors $x \equiv r\ (3)$. Comme $r \in \{0, 1, \ldots, 8\}$, $r \equiv 2\ (3)$ si et seulement si $r = 3, 5$ ou 8.
Conclusion : il y a 3 solutions dans $\mathbb{Z}/9\mathbb{Z}$, qui sont $\overline{2}, \overline{5}$ et $\overline{8}$.

10 Théorème des restes chinois

Le général Han Xing part à la bataille avec 100 soldats. Après la bataille, le général veut compter ses soldats. Il les fait mettre par rang de 3, il en reste 2. Puis il les fait mettre par rang de 5, il en reste 3. Enfin, il les fait mettre par rang de 7, il en reste 2. Combien y a-t-il de soldats ? [9]

Ce problème se traduit de la façon suivante : déterminer x sachant que x est un entier naturel inférieur à 100 tel que $x \equiv 2\ (3)$, $x \equiv 3\ (5)$ et $x \equiv 2\ (7)$.

Théorème 38 (théorème des restes chinois[10]). Soit n, m deux entiers positifs premiers entre eux. Pour tous entiers $a, b \in \mathbb{Z}$, le système d'équations

$$(S) \quad \begin{cases} x & \equiv & a\ (n) \\ x & \equiv & b\ (m) \end{cases}$$

a des solutions. De plus, si x_0 est une solution particulière, l'ensemble des solutions de (S) est $\{x \in \mathbb{Z} \mid x \equiv x_0\ (nm)\} = \{x_0 + knm \mid k \in \mathbb{Z}\}$.

Preuve. Les entiers n et m sont premiers entre eux donc, par le théorème de Bézout, il existe des entiers u et v tels que $nu + mv = 1$. On commence par chercher des solutions particulières aux systèmes suivants, qu'on appelle systèmes élémentaires :

$$(S1) \quad \begin{cases} x & \equiv & 1\ (n) \\ x & \equiv & 0\ (m) \end{cases} \qquad (S2) \quad \begin{cases} x & \equiv & 0\ (n) \\ x & \equiv & 1\ (m) \end{cases}$$

$y_1 = mv$ est une solution de (S1) car $y_1 \equiv 1\ (n)$ (relation de Bézout), et y_1 est multiple de m donc $y_1 \equiv 0\ (m)$. De même, $y_2 = nu$ est une solution de (S2) car y_2 est multiple de n et $y_2 \equiv 1\ (m)$ par la relation de Bézout.

Soit $x_0 = ay_1 + by_2$. Alors $x_0 \equiv a \cdot 1 + b \cdot 0\ (n) \equiv a\ (n)$ et $x_0 \equiv a \cdot 0 + b \cdot 1\ (m) \equiv b\ (m)$. Donc x_0 est une solution du système (S). Exprimons toutes les solutions de (S) en fonction de la solution particulière x_0.

$$x \text{ solution de } (S) \iff \begin{cases} x & \equiv & x_0\ (n) \\ x & \equiv & x_0\ (m) \end{cases} \iff \begin{cases} x - x_0 & \equiv & 0\ (n) \\ x - x_0 & \equiv & 0\ (m) \end{cases} \iff n \text{ et } m \text{ divisent } x - x_0. \qquad (*)$$

Si x est solution de (S), alors n et m divisent $x - x_0$ par $(*)$. Comme n et m sont premiers entre eux, le produit nm divise $x - x_0$ (propriété 27), donc $x \equiv x_0\ (nm)$.
Réciproquement, si $x \equiv x_0\ (nm)$, alors nm divise $x - x_0$, donc n et m divisent $x - x_0$, et par $(*)$ x est une solution de (S).
Conclusion : $x \in \mathbb{Z}$ est solution de (S) si et seulement si $x \equiv x_0\ (nm)$. □

Exemple. Résoudre dans $\mathbb{Z}$ le système (S) $\begin{cases} x & \equiv & 3\ (7) \\ x & \equiv & 4\ (15) \end{cases}$
Algorithme d'Euclide appliqué à 15 et 7 :
$15 = 7 \times 2 + 1$
$7 = 7 \times 1 + 0$
Donc $\text{pgcd}(15, 7) = 1$, et $15 - 2 \times 7 = 1$ est une relation de Bézout entre 15 et 7.
Résolvons les systèmes élémentaires $(S1)$ $\begin{cases} x & \equiv & 1\ (7) \\ x & \equiv & 0\ (15) \end{cases}$ et $(S2)$ $\begin{cases} x & \equiv & 0\ (7) \\ x & \equiv & 1\ (15) \end{cases}$
En utilisant la relation de Bézout ci-dessus, on voit que $y_1 = 15$ est une solution particulière de (S1) car $y_1 \equiv 1\ (7)$ et y_2 est un multiple de 15, donc $y_2 \equiv 0\ (15)$. De même, $y_2 = -2 \times 7 = -14$ est une solution particulière de (S2). Donc $x_0 = 3y_1 + 4y_2 = -11$ est une solution particulière de (S). Comme $7 \times 15 = 105$, l'ensemble des solutions de (S) est l'ensemble des $x \equiv -11\ (105)$. □

[9] Ce problème apparaît dans un livre chinois datant du IIIe siècle.

[10] Le théorème des restes chinois figure dans un livre du mathématicien chinois Qin Jiushao du XIIIe siècle.

Le théorème 38 se généralise pour un système de k équations :

Théorème 39. Si $n_1, n_2, \ldots, n_k$ sont des entiers positifs 2 à 2 premiers entre eux, alors, pour tous $a_1, \ldots, a_k \in \mathbb{Z}$, le système

$$\begin{cases} x & \equiv & a_1 \ (n_1) \\ x & \equiv & a_2 \ (n_2) \\ & \vdots & \\ x & \equiv & a_k \ (n_k) \end{cases}$$

a des solutions et, si x_0 est une solution particulière, l'ensemble des solutions est $\{x \in \mathbb{Z} \mid x \equiv x_0 \ (n_1 n_2 \ldots n_k)\}$.

Pour trouver une solution particulière, on commence par résoudre les systèmes élémentaires. Par exemple, pour $k = 3$, il y a 3 systèmes élémentaires :

$$(S1) \begin{cases} x & \equiv & 1 \ (n_1) \\ x & \equiv & 0 \ (n_2) \\ x & \equiv & 0 \ (n_3) \end{cases} \quad (S2) \begin{cases} x & \equiv & 0 \ (n_1) \\ x & \equiv & 1 \ (n_2) \\ x & \equiv & 0 \ (n_3) \end{cases} \quad (S3) \begin{cases} x & \equiv & 0 \ (n_1) \\ x & \equiv & 0 \ (n_2) \\ x & \equiv & 1 \ (n_3) \end{cases}$$

Comment trouver une solution particulière de (S1) ?
x est solution de (S1) si et seulement si $x \equiv 1 \ (n_1)$ et x est divisible par n_2 et n_3. Or n_2 et n_3 sont premiers entre eux, donc x est divisible par n_2 et n_3 si et seulement si x est divisible par $n_2 n_3$. Donc (S1) est équivalent au système

$$(S1') \quad \begin{cases} x & \equiv & 1 \ (n_1) \\ x & \equiv & 0 \ (n_2 n_3) \end{cases}$$

Comme n_1 est premier avec n_2 et n_3, n_1 n'a aucun facteur premier commun avec n_2 et n_3, donc n_1 et $n_2 n_3$ sont premiers entre eux. Pour trouver une solution du système à 2 équations (S1'), on peut donc appliquer la méthode vue précédemment. On fait de même pour les systèmes (S2) et (S3).
Une fois qu'on a trouvé y_1, y_2, y_3 des solutions particulières de (S1), (S2), (S3), on vérifie facilement que $x_0 = a_1 y_1 + a_2 y_2 + a_3 y_3$ est une solution de

$$\begin{cases} x & \equiv & a_1 \ (n_1) \\ x & \equiv & a_2 \ (n_2) \\ x & \equiv & a_3 \ (n_3) \end{cases}$$

Le théorème affirme alors que l'ensemble des solutions est l'ensemble des entiers $x \equiv x_0 \ (n_1 n_2 n_3)$.

Exemple. Revenons au problème de l'armée chinoise. Le nombre de soldats est solution du système

$$(S) \quad \begin{cases} x & \equiv & 2 \ (3) \\ x & \equiv & 3 \ (5) \\ x & \equiv & 2 \ (7) \end{cases}$$

3, 5 et 7 n'ont pas de facteur premier commun, donc ils sont 2 à 2 premiers entre eux.
Le premier système élémentaire est $(S1) \begin{cases} x & \equiv & 1 \ (3) \\ x & \equiv & 0 \ (5) \\ x & \equiv & 0 \ (7) \end{cases} \iff (S1') \begin{cases} x & \equiv & 1 \ (3) \\ x & \equiv & 0 \ (35) \end{cases}$

Cherchons une relation de Bézout entre 3 et 35. Algorithme d'Euclide :
$35 = 11 \times 3 + 2$
$3 = 2 + 1$.
Relation de Bézout entre 3 et 35 : $1 = 3 - 2 = 3 - (35 - 11 \times 3) = 12 \times 3 - 35$. On en déduit que $y_1 = -35$ est une solution de (S1'), donc de (S1).

Le deuxième système élémentaire est $(S2) \begin{cases} x & \equiv & 0 \ (3) \\ x & \equiv & 1 \ (5) \\ x & \equiv & 0 \ (7) \end{cases} \iff (S2') \begin{cases} x & \equiv & 1 \ (5) \\ x & \equiv & 0 \ (21) \end{cases}$

Algorithme d'Euclide pour 21 et 5 : $21 = 4 \times 5 + 1$.
Relation de Bézout entre 5 et 21 : $1 = 21 - 4 \times 5$.
On en déduit que $y_2 = 21$ est une solution de (S2).

Le troisième système élémentaire est $(S3)$ $\left\{\begin{array}{rcl} x & \equiv & 0\ (3) \\ x & \equiv & 0\ (5) \\ x & \equiv & 1\ (7) \end{array}\right. \iff (S3')\ \left\{\begin{array}{rcl} x & \equiv & 1\ (7) \\ x & \equiv & 0\ (15) \end{array}\right.$

Algorithme d'Euclide pour 15 et 7 : $15 = 2 \times 7 + 1$. Relation de Bézout entre 15 et 7 : $1 = 15 - 2 \times 7$.
On en déduit que $y_3 = 15$ est une solution de (S3).

$x_0 = 2y_1 + 3y_2 + 2y_3 = 23$ est donc une solution particulière du système initial (S). L'ensemble des solutions est donc l'ensemble des $x \equiv 23\ (105)$ (car $3 \times 5 \times 7 = 105$). Donc la seule solution $x \leq 100$ est $x = 23$.

Remarque.
Une fois qu'on a trouvé y_1, y_2, y_3, on peut résoudre sans calcul supplémentaire tous les systèmes de la forme :

$$\left\{\begin{array}{rcl} x & \equiv & a\ (3) \\ x & \equiv & b\ (5) \\ x & \equiv & c\ (7) \end{array}\right.$$

Les solutions sont les $x \equiv ay_1 + by_2 + cy_3\ (105)$.

11 Petit théorème de Fermat

Théorème 40 (petit théorème de Fermat[11]). Soit p un nombre premier et x un entier. Alors :
• $x^p \equiv x\ (p)$,
• si p ne divise pas x, alors $x^{p-1} \equiv 1\ (p)$.

Lemme 41. Soit p un nombre premier et un k un entier tel que $1 \leq k \leq p-1$. Alors p divise C_p^k.

Preuve. $C_p^k = \frac{p!}{k!(p-k)!}$ *donc* $p! = k!(p-k)!C_p^k$. *Or* $p! = 1 \times 2 \times \cdots \times p$, *donc* p *divise* $k!(p-k)!C_p^k$. *Comme* p *est premier, ceci implique que* p *divise soit* $k!$, *soit* $(p-k)!$, *soit* C_p^k.
• *Si* p *divise* $k! = 1 \times \cdots \times k$, *alors* p *divise un des facteurs (*p *est premier), autrement dit il existe* $i \in \{1, \ldots, k\}$ *tel que* p *divise* i. *Or* $1 \leq i \leq k < p$, *donc c'est impossible.*
• *De même,* p *ne peut pas diviser* $(p-k)! = 1 \times \cdots \times (p-k)$ *car* $(p-k) < p$.
• *Par conséquent,* p *divise* C_p^k. □

Preuve du théorème de Fermat.
On traite à part le cas $p = 2$. *Soit* $x \in \mathbb{Z}$. *Si* 2 *divise* x *alors* $x \equiv 0\ (2)$ *et* $x^2 \equiv 0\ (2) \equiv x\ (2)$. *Si* 2 *ne divise pas* x, *alors* $x \equiv 1\ (2)$ *et* $x^2 \equiv 1\ (2) \equiv x\ (2)$. *Ceci prouve le théorème pour* $p = 2$.

On suppose dans la suite de la preuve que $p > 2$. *Montrons par récurrence sur* $x \in \mathbb{N}$ *que* $x^p \equiv x\ (p)$.
• *Si* $x = 0$, *alors* $x^p \equiv 0\ (p) \equiv x\ (p)$.
• *Supposons que* $x^p \equiv x\ (p)$ *pour* $x \in \mathbb{N}$. *Par la formule du binôme,*

$$(x+1)^p = x^p + C_p^{p-1}x^{p-1} + \cdots + C_p^k x^k + \cdots + C_p^1 x + 1.$$

Par le lemme 41, $C_p^k \equiv 0\ (p)$ *pour tout* $k \in \{1, \ldots, p-1\}$, *donc* $(x+1)^p \equiv x^p + 0 + \cdots + 0 + 1\ (p)$. *Or* $x^p \equiv x\ (p)$ *par hypothèse de récurrence, donc* $(x+1)^p \equiv x+1\ (p)$, *ce qui est la propriété au rang* $x+1$.
• *Conclusion :* $x^p \equiv x\ (p)$ *pour tout* $x \in \mathbb{N}$.

Si $x \in \mathbb{Z}$, $x < 0$, *on pose* $y = -x$. *Comme* p *est premier et différent de* 2, p *est impair et* $x^p = (-y)^p = -y^p$. *Par ce qui précède,* $y^p \equiv y\ (p)$, *donc* $x^p \equiv -y\ (p) \equiv x\ (p)$. *Ceci termine la preuve du premier point du théorème.*

Si x *n'est pas un multiple de* p, *alors* $\overline{x}$ *est inversible dans* $\mathbb{Z}/p\mathbb{Z}$ *(théorème 37). Si* $\overline{u}$ *est son inverse dans* $\mathbb{Z}/p\mathbb{Z}$, *alors* $ux \equiv 1\ (p)$. *Par le premier point du théorème,* $x^p \equiv x\ (p)$ *donc, en multipliant par* u, *on trouve* $x^{p-1} \equiv 1\ (p)$. *Ceci prouve le second point du théorème.* □

Exemple. Quel est le reste de la division euclidienne de 42^{2006} par 5 ?
2 est le reste de la division euclidienne de 42 par 5, autrement dit $42 \equiv 2\ (5)$. Donc $42^{2006} \equiv 2^{2006}\ (5)$.
Par le théorème de Fermat, $2^4 \equiv 1\ (5)$, donc $2^{4k} \equiv 1\ (5)$ pour tout entier $k \in \mathbb{N}$. Effectuons la division euclidienne de 2006 par 4 : $2006 = 4 \times 501 + 2$. On en déduit que $2^{2006} \equiv 2^{4\times 501} \cdot 2^2\ (5) \equiv 1 \times 4\ (5)$. Donc $42^{2006} \equiv 4\ (5)$, ce qui signifie exactement que 4 est le reste de la division euclidienne de 42^{2006} par 5.

Pour calculer $x^n\ (p)$ quand $x \not\equiv 0\ (p)$, on utilise souvent le théorème de Fermat comme dans l'exemple : si on écrit $n = q(p-1) + r$ (division euclidienne de n par $p-1$), alors $x^n \equiv (x^{p-1})^q.x^r\ (p) \equiv x^r\ (p)$ car $x^{p-1} \equiv 1\ (p)$.

[11] Pierre de Fermat est un mathématicien français du XVIIe siècle.

12 Cryptographie

La cryptographie désigne les méthodes de codage permettant de transmettre des messages de telle manière que seule le destinataire peut lire le message. Ainsi, si une tierce personne intercepte le message, elle ne peut pas le comprendre.

a) Cryptographie à clé secrète

Dans la cryptographie à clé secrète, l'algorithme de décodage se déduit facilement de l'algorithme de codage. L'algorithme de codage doit donc être gardé secret, il est connu uniquement de l'expéditeur et du destinataire.

Exemple élémentaire : cryptage par décalage
On remplace chaque lettre du message par la lettre suivante dans l'alphabet.
MARS $\longrightarrow$ NBST
On décode en remplaçant chaque lettre par la lettre précédente dans l'alphabet.

Cryptage affine
On choisit des entiers a et b avec a premier avec 26.

Codage : on remplace chaque lettre par son rang dans l'alphabet, puis on remplace chaque entier x associé à une lettre par l'entier y tel que $y \equiv ax + b\ (26)$, avec $1 \leq y \leq 26$.

Décodage : Par hypothèse, $\overline{a}$ est inversible dans $\mathbb{Z}/26\mathbb{Z}$, on note $\overline{u}$ son inverse, c'est-à-dire $ua \equiv 1\ (26)$. Alors $u(y-b) \equiv uax\ (26) \equiv x\ (26)$.
Pour décoder, on calcule donc $x' \equiv u(y-b)\ (26)$, en choisissant x' tel que $1 \leq x' \leq 26$. Alors $x' = x$, et on a retrouvé la lettre de départ.

Exemple : $a = 3, b = 5$.
Pour trouver u, on applique l'algorithme d'Euclide à 3 et 26 :
$26 = 3 \times 8 + 2$
$3 = 2 + 1$
Relation de Bézout entre 3 et 26 : $1 = 3 - 2 = 3 - (26 - 3 \times 8) = 9 \times 3 - 26$. On peut donc prendre $u = 9$.

Codage : MARS $\longrightarrow (13, 1, 18, 19) \longrightarrow (18, 8, 7, 10)$
car $3 \times 13 + 5 \equiv 18\ (26)$, $3 \times 1 + 5 \equiv 8\ (26)$, $3 \times 18 + 5 \equiv 7\ (26)$, $3 \times 19 + 5 \equiv 10\ (26)$,

Décodage : on vérifie qu'en calculant $x' \equiv 9(y-5)\ (26)$ pour chaque entier du message codé $(18, 8, 7, 10)$, on retrouve le message d'origine $(13, 1, 18, 19)$.

Dans les algorithmes à clés secrètes, le problème le plus important réside dans l'échange de la clé entre l'expéditeur et le destinataire. Si quelqu'un intercepte la clé de codage, il peut décoder n'importe quel message.

b) Cryptographie à clé publique

Dans la cryptographie à clé publique, l'algorithme de codage est connu de tout le monde. L'algorithme de décodage, connu uniquement du destinataire, ne peut pas se déduire de l'algorithme de codage.

Système de cryptographie RSA[12]
– p et q sont 2 nombres premiers différents (très grands) et $n = pq$.
– On choisit un entier positif e premier avec $m = (p-1)(q-1)$.
– On détermine un entier positif d tel que $ed \equiv 1\ (m)$ ($\overline{d}$ est l'inverse de $\overline{e}$ dans $\mathbb{Z}/m\mathbb{Z}$).

le couple (n, e) est la **clé publique** : on la communique à tout le monde.
Les entiers p, q et d sont gardés secrets par le destinataire.

Codage
Le message est un entier M avec $0 \leq M \leq n-1$
(si on veut envoyer un message plus long, on le découpe en plusieurs blocs).
L'expéditeur calcule l'entier $C \equiv M^e\ (n)$ avec $0 \leq C \leq n-1$. Il envoie le message codé C.

Décodage
Le destinataire calcule $M' \equiv C^d\ (n)$ avec $0 \leq M' \leq n-1$.
Propriété : $M' = M$.

[12] Le système RSA date de 1978, son vient des initiales de ses trois auteurs : Rivest, Shamir, Adleman

Lemme 42. Soit p et q deux nombres premiers différents et $k \in \mathbb{N}$ tel que $k \equiv 1\ ((p-1)(q-1))$. Alors, pour tout entier $x \in \mathbb{Z}$, $x^k \equiv x\ (pq)$.

Preuve. On écrit $k = i(p-1)(q-1)+1$. L'entier i est positif car $p-1 \geq 1, q-1 \geq 1$ et $k \geq 0$. Montrons d'abord que $x^k \equiv x\ (p)$.
• *Si p divise x, alors $x \equiv 0\ (p)$ donc $x^k \equiv 0\ (p) \equiv x\ (p)$.*
• *Si p ne divise pas x, alors $x^{p-1} \equiv 1(p)$ par le petit théorème de Fermat.*
$x^k = x^{i(p-1)(q-1)+1} = (x^{p-1})^{i(q-1)}.x$ donc $x^k \equiv 1^{i(q-1)}.x\ (p) \equiv x\ (p)$.
Pour tout $x \in \mathbb{Z}$, on a donc $x^k \equiv x\ (p)$.
Le même argument montre que

$$\forall x \in \mathbb{Z},\ x^k \equiv x\ (q).$$

Ceci montre que, pour tout entier x, p et q divisent $x^k - x$. Comme p et q sont premiers entre eux, le produit pq divise $x^k - x$, autrement dit $x^k \equiv x\ (pq)$. □

Preuve de la propriété permettant le décodage de RSA.
Par définition, $M' \equiv C^d\ (pq) \equiv M^{ed}\ (pq)$, et $ed \equiv 1\ ((p-1)(q-1))$. Par le lemme 42 (appliqué à $x = M$ et $k = ed$), $M^{ed} \equiv M\ (pq)$. Par conséquent, $M' \equiv M\ (pq)$. Or $0 \leq M < pq$ et $0 \leq M' < pq$, donc nécessairement $M' = M$. □

Pourquoi ne peut-on pas décrypter le cryptage RSA ?

L'efficacité du cryptage RSA réside dans le fait que décoder sans connaître la clé secrète demanderait des calculs beaucoup trop importants.
Pour retrouver le message initial M à partir du message codé C, on a besoin de connaître d. L'entier d se calcule facilement à partir de e si on connaît p et q (à l'aide de l'algorithme d'Euclide appliqué à e et $m = (p-1)(q-1)$). Tout le monde connaît l'entier n, donc, en théorie, on peut retrouver p et q en décomposant n en facteurs premiers. En pratique, la décomposition en facteurs premiers est très difficile et prend énormément de temps quand les entiers sont grands. À l'inverse, multiplier les entiers p et q pour obtenir n est très facile. De plus, on dispose d'algorithmes assez rapides pour trouver de grand nombres premiers.
On utilise actuellement des nombres premiers p, q d'environ 100 chiffres, le produit $n = pq$ a donc environ 200 chiffres. Même les ordinateurs les plus puissants sont incapables de mener à bien la décomposition en facteurs premiers d'un entier aussi grand.

Table des matières

1 Les ensembles $\mathbb{N}$ et $\mathbb{Z}$ **1**

2 Divisibilité dans $\mathbb{Z}$ **1**
a) Diviseurs et multiples . . . 1
b) Propriétés . . . 1

3 Nombres premiers **2**
a) Reconnaître un nombre premier . . . 2
b) Ensemble des nombres premiers . . . 2
c) Décomposition en produit de facteurs premiers . . . 3
d) Crible d'Ératosthène . . . 4

4 Division euclidienne **5**

5 PGCD et PPCM **5**
a) PGCD . . . 5
b) Algorithme d'Euclide . . . 6
c) Nombres premiers entre eux . . . 7
d) PPCM . . . 7

6 Théorèmes de Bézout et de Gauss **8**
a) Théorème de Bézout . . . 8
b) Comment trouver une relation de Bézout . . . 9
c) Théorème de Gauss . . . 9
d) Résoudre l'équation $ax + by = c$ . . . 9
e) Unicité de la décomposition en facteurs premiers . . . 10

7 Congruences **11**
a) Définition et propriétés . . . 11
b) Compatibilité avec les opérations . . . 11
c) Critères de divisibilité . . . 12

8 $\mathbb{Z}/n\mathbb{Z}$ **12**
a) Définition . . . 12
b) Opérations dans $\mathbb{Z}/n\mathbb{Z}$ . . . 12
c) Éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$ . . . 13

9 Résoudre l'équation $ax \equiv b\ (n)$ **14**

10 Théorème des restes chinois **15**

11 Petit théorème de Fermat **17**

12 Cryptographie **18**
a) Cryptographie à clé secrète . . . 18
b) Cryptographie à clé publique . . . 18