LEÇON N^{O} 7

Congruences dans $\mathbb{Z}$. Applications.

Clément BOULONNE

Session 2020

Préambule

Niveau de la leçon

Terminale S Spé Maths

Prérequis

Multiples et diviseurs dans $\mathbb{Z}$.

Références

— X. DELAHAYE, *Congruences, Terminale S*. URL : https://xmaths.free.fr.
— J.-P. QUELEN, *Petit théorème de Fermat et codage RSA*, 15 janvier 2011.
— Manuel Sesamaths, Terminale S Spé, Editions Magnard, 2016. URL : https://mep-outils.sesamath.net/manuel_numerique/index.php?ouvrage=mstsspe_2016
— A. BODIN & al., *Algèbre, Cours de mathématiques de première année*, 2016. URL : http://exo7.emath.fr/cours/livre-algebre-1.pdf
— C. BOULONNE, *Ateliers Mathématiques*. Notes de cours de première année de Licence, 2006-2007. URL : https://cboumaths.files.wordpress.com/2012/04/ateliersmath.pdf
— C. BOULONNE, *M101 : Fondements de l'algèbre*. Notes de Cours de première année de Licence, 2006-2007. URL : https://cboumaths.files.wordpress.com/2010/01/m101.pdf.
— C. BOULONNE, *Promenades sur un cercle*. Exposé donné au collège Voltaire de Wattignies. 30 juin 2015. URL : https://cboumaths.files.wordpress.com/2015/06/promenadescerc
maj_20150630.pdf
— Contributeurs à Wikipedia, *Théorème des restes chinois*. (2020, février 4). Wikipédia, l'encyclopédie libre. Page consultée le 16 :51, février 4, 2020 à partir de http://fr.wikipedia.org/w/index.php?title=Théorème_des_restes_chinois&oldid=167070477.
— P. JAMMES, *C5 : Relations*. Université d'Avignon, faculté de sciences. Licence M-I et C-SP, S1-algèbre. URL : https://math.unice.fr/~pjammes/enseignement/relations.pdf

Table des matières

1 Division euclidienne

Définition 1.1. Soit a un entier relatif et b un entier naturel non nul. On appelle *division euclidienne* de a par b, l'opération qui, au couple $(a; b)$, associe l'unique couple $(q; r)$ tel que :

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

a s'appelle le *dividende*, b le *diviseur*, q le *quotient* et r le *reste*.

Démonstration. $\Diamond$

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

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

On définit alors $r = a - qb$, r vérifie alors $0 \leq r = a - qb < b$.

Unicité Supposons que q', r' soient deux entiers qui vérifient les conditions du théorème. Tout d'abord, $a = bq + r = bq' + r'$ et donc $b(q - q') = r' - r$. D'autre part $0 \leq r' < b$ et $0 \leq r < b$ donc $-b < r' - r < b$. Mais $r' - r = b(q - q')$ donc on obtient $-b < b(q - q') < b$<; on peut

diviser par $b > 0$ pour avoir $-1 < q - q' < 1$. Comme $q' - q$ est un entier, la seule possibilité est $q - q' = 0$ et donc $q = q'$. En repartant de $r' - r = b(q - q')$, on obtient maintenant $r = r'$.

□

Exemples 1.2. ◊

1. La division euclidienne de 114 par 8 correspond à :

$$114 = 8 \times 14 + 2.$$

2. Pour avoir un reste positif dans la division euclidienne de -114 par 8, on écrit : $-2 = 6 - 8$. On obtient alors :

$$-114 = 8 \times (-14) - 2 = 8 \times (-14) - 8 + 6 = 8 \times (-15) + 6.$$

Ainsi $q = -15$ et $r = 6$.

Remarques 1.3.
— Le reste est toujours un entier naturel inférieur au diviseur. Par conséquent, dans la division par 7, par exemple, il existe 7 restes possibles : 0, 1, 2, 3, 4, 5 et 6.
— On peut schématiser la division euclidienne comme on pose une division :

$$\begin{array}{r|l} a & b \\ \hline r & q \end{array}$$

Exercice 1.4. Lorsqu'on divise a par b, le reste est 8 et lorsqu'on divise $2a$ par b, le reste est 5. Déterminer le diviseur b.

Solution. ◊ On écrit chacune des deux divisions euclidiennes, en notant q et q' les quotients respectifs :

$$\begin{cases} a = bq + 8 \text{ avec } b > 8 \\ 2a = bq' + 5 \text{ avec } b > 5 \end{cases}$$

En multipliant la première division par 2 et en égalisant avec la deuxième, on obtient :

$$\begin{aligned} 2bq + 16 &= bq' + 5 \text{ avec } b > 8 \\ b(2q - q') &= -11 \\ b(q' - 2q) &= 11 \end{aligned}$$

b est donc un multiple positif non nul de 11, supérieur à 8, donc $b = 11$. □

2 Congruences

2.1 Premiers résultats

Définition 2.1 (Congruence). Soient $n \in \mathbb{Z}$ et $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo n si $n \mid a - b$. On note alors $a \equiv b \pmod{n}$.

Exemples 2.2.
1. $11 \equiv 1 \pmod{5}$ car $5 \mid 11 - 1$.
2. $25 \equiv 4 \pmod{7}$ car $7 \mid 25 - 4$.

Définition 2.3. Soient $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo p, si a et b ont le même reste dans la division euclidienne par b.

Exemple 2.4.

$$2008 \equiv 8 \pmod{10} \text{ car } 2008 = 10 \times 200 + 8.$$

Démonstration de l'équivalence de deux définitions. — Supposons que a et b ont le même reste r dans la division euclidienne par n. On peut donc écrire :

$$a = p \times k + r \quad \text{et} \quad b = p \times k' + r \quad \text{avec } k,\, k' \in \mathbb{Z},\, r \in \mathbb{N} \text{ et } 0 \leq r \leq p$$

donc

$$b - a = p \times k' + r - (p \times k + r) = p \times k' - p \times k = p(k' - k).$$

$k' - k$ étant un entier relatif, on en déduit que $b - a$ est multiple de p.

— Supposons que $b - a$ est multiple de p, on peut écrire $b - a = k \times p$ avec $k \in \mathbb{Z}$.

□

PROPRIÉTÉS 2.5. — $a \equiv 0 \pmod{n}$ si et seulement si a est un multiple de n ou n est un diviseur de a.

— La congruence est une relation d'équivalence, c'est-à-dire, pour tous entiers a, b et c, on a :

1. $a \equiv a \pmod{n}$ (réflexivité)
2. Si $a \equiv b \pmod{n}$ alors $b \equiv a \pmod{n}$ (symétrie)
3. Si $a \equiv b \pmod{n}$ et si $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$ (transitivité).

Démonstration. ◊ On utilise la définition 2.1 pour démontrer que la relation « Congru modulo n » est une relation d'équivalence dans $\mathbb{Z}$.

— On a bien $n \mid 0$ (pour $n \neq 0$) car 0 est divisible par n'importe quel nombre non nul (prendre $k = 0$ dans la définition de divisibilité).

— Si $a \equiv b \pmod{n}$ alors $n \mid a - b$, il existe donc un entier relatif k tel que $(b - a) = nk$ ou encore $-(b - a) = -nk$ soit donc $-(b - a) = n \times -k$. Comme $-k \in \mathbb{Z}$, on peut en déduire que n divise $-(b - a)$, c'est-à-dire n divise $a - b$ ou encore $b \equiv a \pmod{n}$.

— Si $a \equiv b \pmod{n}$ alors il existe un entier relatif k tel que $(b - a) = nk$ (1). On sait de plus que $b \equiv c \pmod{n}$ donc il existe un entier relatif k' tel que $(c - b) = nk'$. (2) En additionnant les égalités (1) et (2), on trouve :

$$(b - a) + (c - b) = nk + nk' \Leftrightarrow -a + c = n(k + k') \Leftrightarrow c - a = n(k + k').$$

Comme k et k' appartiennent à $\mathbb{Z}$, la somme $k + k'$ est un nombre entier relatif. On a donc : $n \mid c - a$ d'où $a \equiv c \pmod{n}$.

□

Remarque 2.6. La démonstration est encore plus triviale en prenant la définition 2.3.

THÉORÈME 2.7. Soit n un entier naturel ($n \geq 2$), a et b deux entiers relatifs.

$$a \equiv b \pmod{n} \Leftrightarrow a - b \equiv 0 \pmod{n}.$$

Démonstration. ◊

($\Rightarrow$) On sait que $a \equiv b \pmod{n}$. Il existe donc des entiers q, q' et r tels que :

$$a = nq + r \quad \text{et} \quad b = nq' + r \text{ avec } 0 \leq r < n.$$

On obtient : $a - b = n(q - q')$. $a - b$ est alors un multiple de n, et son reste dans la division par n est nul, d'où $a - b \equiv 0 \pmod{n}$.

($\Leftarrow$) On sait que $a - b \equiv 0 \pmod{n}$. Il existe k tel que : $a - b = kn$ (1). Si l'on effectue la division de a par n, on a : $a = nq + r$ avec $0 \leq r < n$ (2). De (1) et (2), on obtient :

$$\begin{aligned} nq + r - b &= kn \\ -b &= kn - nq - r \\ b &= (q - k)n + r \end{aligned}$$

a et b ont le même reste dans la division par n, donc $a \equiv b \pmod{n}$.

□

2.2 Compatibilité de la congruence avec l'addition et la multiplication

THÉORÈME 2.8. Soit n un entier naturel ($n \geq 2$) et a, b, c et d des entiers relatifs vérifiant :

$$a \equiv b \pmod{n} \quad \text{et} \quad c \equiv d \pmod{n}.$$

La relation de congruence est compatible avec :

1. l'addition : $a + c \equiv b + d \pmod{n}$
2. la multiplication : $ac \equiv bd \pmod{n}$
3. les puissances : pour tout entier naturel k, $a^k \equiv b^k \pmod{n}$.

Démonstration. ◊

1. **Compatibilité avec l'addition.** On sait que : $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, donc $(a-b)$ et $(c-d)$ sont des multiples de n. Il existe donc deux entiers relatifs k et k' tels que : $a-b = kn$ et $c - d = k'n$.
   En additionnant ces deux égalités, on obtient :
   $$a - b + c - d = kn + k'n \Leftrightarrow (a + c) - (b + d) = (k + k')n.$$
   Donc $(a + c) - (b - d)$ est un multiple de n, d'où $a + c \equiv b + d \pmod{n}$.
2. **Compatibilité avec la multiplication.** On sait que : $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, donc, il existe deux entiers relatifs k et k' tels que : $a = b + kn$ et $c = d + k'n$.
   En multipliant ces deux égalités, on obtient :
   $$\begin{aligned} ac &= (b + kn)(d + k'n) \\ ac &= bd + k'bn + kdn + kk'n^2 \\ ac &= bd + (k'b + kd + kk'n)n \\ ac - bd &= (k'b + kd + kk'n)n \end{aligned}$$
   Donc $(ac - bd)$ est un multiple de n, d'où $ac \equiv bd \pmod{n}$.
3. On considère, pour $n \in \mathbb{N}^*$, la proposition $P(n)$: « $a^n \equiv b^n \pmod{p}$ ». Pour $n = 1$, on $a^1 = 1$ et $b^1 = b$ et on sait que $a \equiv b \pmod{p}$ donc $P(1)$ est vraie. Supposons $P(n)$ vraie pour un entier $n \geq 1$ alors $a^n \equiv b^n \pmod{p}$ et comme on a aussi $a \equiv b \pmod{p}$, on peut en utilisant la propriété précédente justifier que $a^n \times a \equiv b^n \times b \pmod{p}$, soit $a^{n+1} \equiv b^{n+1} \pmod{p}$, c'est-à-dire la proposition $P(n + 1)$ est vraie. On a donc démontré par récurrence que $P(n)$ est vraie pour tout entier $n \geq 1$.

□

Exercice 2.9. On veut déterminer le reste dans la division euclidienne par 7 du nombre $50^{100} + 100^{100}$.

Solution. $\Diamond$ On a tout d'abord $50 \equiv 1 \pmod 7$ car $50 = 7 \times 7 + 1$. D'après la compatibilité avec les puissances, on a : $50^{100} \equiv 1^{100} \equiv 1 \pmod 7$.

De plus $100 = 50 \times 2$. On utilise la compatibilité avec la multiplication pour en déduire que $100 \equiv 2 \pmod 7$. □

Exercice 2.10.
1. Déterminer suivant les valeurs de l'entier relatif n, le reste de la division de n^2 par 7.
2. En déduire alors les solutions de l'équation $x^2 \equiv 2 \pmod 7$.

Solution. $\Diamond$

1. Si on veut trouver la solution par une méthode exhaustive, on peut construire un tableau de congruence :

Reste de la ÷ de n par 7	0	1	2	3	4	5	6
Reste de la ÷ de n^2 par 7	0	1	4	2	2	4	1

   Les restes possibles de n^2 par 7 sont donc 0, 1, 2 et 4.
2. Pour résoudre $x^2 \equiv 2 \pmod 7$, on recherche dans le tableau les valeurs de n pour lesquelles on obtient un reste de 2 quand n est au carré. Il est obtenu pour les restes 3 et 4 dans la division de n par 7.

   Les solutions de l'équation sont donc : $x \equiv 3 \pmod 7$ et $x \equiv 4 \pmod 7$.

□

3 Applications

3.1 Petit théorème de Fermat

THÉORÈME 3.1 (PETIT THÉORÈME DE FERMAT). Soit p un nombre premier et a un entier naturel premier avec p alors a^{p-1} est divisible par p. En d'autres termes, $a^{p-1} \equiv 1 \pmod p$.

Démonstration. $\Diamond$ p ne divise aucun nombre de la suite a, $2a$, …, $(p-1)a$. En effet, d'après le théorème de Gauss, si p divisait un de ces produits ka, p diviserait k puisque a et p sont premiers entre eux. Ceci est impossible puisque $1 < k < p$.

De plus, les restes des divisions a, $2a$, …, $(p-1)a$ par p sont tous différents. Si on trouvait des restes identiques pour ka et $k'a$ $(k > k')$ alors le reste $(k-k')a$ par p serait nul, ce qui est impossible d'après ce qui précède. Donc, à l'ordre près des facteurs les restes de a, $2a$, …, $(p-1)$a par p sont 1, 2, …, $p-1$.

Par conséquent, la division du produit $a \times 2a \times \cdots \times (p-1)a$ par p a pour reste le produit $1 \times 2 \times \cdots \times (p-1)$ et donc $a \times 2a \times \cdots \times (p-1)a$ qui s'écrit encore :

$$a^{p-1} \times 2 \times \cdots \times (p-1) \equiv 2 \times 3 \times \cdots \times (p-1) \pmod p.$$

Il existe donc un entier relatif k tel que :

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

Comme p est premier avec $1 \times 2 \times \cdots \times (p-1)$ d'après le théorème de Gauss, p divise $a^{p-1} - 1$. Ainsi, a^{p-1} est congru à 1 modulo p. □

Corollaire 3.2. Soit p un nombre premier et a un entier quelconque alors $a^p \equiv a \pmod{p}$.

Démonstration. $\Diamond$ D'après ce qui précède, si a et p sont premiers entre eux, $a^{p-1} - 1$ est congru à 0 modulo p. Sinon, p étant premier, a est congru à 0 modulo p. On a donc soit $a^{p-1} \equiv 1 \pmod{p}$, soit $a^p \equiv a \equiv 0 \pmod{p}$ et par conséquent, dans les deux cas, $a^p \equiv a \pmod{p}$. □

Exemple 3.3. 7 est un nombre premier et 7 ne divise par $10^{10^{10}}$ puisque $10^{10^{10}}$ s'écrit sous la forme $2^\alpha \times 5^\beta$ avec $\alpha, \beta \in \mathbb{N}^*$. Don d'après le corollaire du petit théorème de Fermat :

$$(10^{10^{10}})^6 \equiv 1 \pmod{7}.$$

3.2 Construction de nouveaux ensembles : $\mathbb{Z}/n\mathbb{Z}$

On rappelle que la relation $a \equiv b \pmod{n}$ est une relation d'équivalence sur $\mathbb{Z}$.

Définition 3.4 ($\mathbb{Z}/n\mathbb{Z}$). Soit $\mathcal{R}$ la relation d'équivalence définie par :

$$a\mathcal{R}b \Leftrightarrow a \equiv b \pmod{n}.$$

La classe de a associée à $\mathcal{R}$ est :

$$\overline{a} = \{x \in \mathbb{Z},\ a \equiv x \pmod{n}\} = \{x \in \mathbb{Z},\ n \mid a - x\}.$$

On note donc :

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\mathcal{R} = \{\overline{a},\ a \in \mathbb{Z}\}.$$

On définit des opérations sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$. Tout d'abord, l'addition :

Définition 3.5 (Addition dans $\mathbb{Z}/n\mathbb{Z}$). L'opération $\oplus$ correspond à l'addition dans $\mathbb{Z}/n\mathbb{Z}$:

$$\begin{array}{rccc} \oplus & : & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & & (\overline{a}, \overline{b}) & \mapsto & \overline{a} \oplus \overline{b} = \overline{a+b} \end{array}.$$

Remarque 3.6. Cette opération est bien définie, c'est-à-dire qu'elle est indépendante du choix d'un représentant :

$$\begin{aligned} \overline{a} = \overline{a'} \quad \text{et} \quad \overline{b} = \overline{b'} &\Rightarrow a \equiv a' \pmod{n} \quad \text{et} \quad b \equiv b' \pmod{n} \\ &\Rightarrow a + b \equiv a' + b' \pmod{n} \Rightarrow \overline{a+b} = \overline{a'+b'}. \end{aligned}$$

Exemple 3.7. On se place dans $\mathbb{Z}/4\mathbb{Z}$:

1. $\overline{3} \otimes \overline{2} = \overline{3+2} = \overline{5} = \overline{1}$.
2. $\overline{7} \otimes \overline{3} = \overline{7+3} = \overline{10} = \overline{2}$.

PROPOSITION 3.8. $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ est un groupe abélien avec $e = \overline{0}$ (élément neutre) et $\overline{a}^{-1} = -\overline{a}$ (élément inversible).

Démonstration. $\Diamond$ En exercice. □

On définit ensuite la multiplication dans $\mathbb{Z}/n\mathbb{Z}$.

Définition 3.9 (Multiplication dans $\mathbb{Z}/n\mathbb{Z}$). On définit une multiplication dans $\mathbb{Z}/n\mathbb{Z}$:

$$\begin{array}{rccc} \otimes & : & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & & (\overline{a}, \overline{b}) & \mapsto & \overline{a} \otimes \overline{b} = \overline{a \cdot b} \end{array}.$$

Remarque 3.10. Cette opération est bien définie car si $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$ alors :

$$a \equiv a' \pmod{n} \quad \text{et} \quad b \equiv b' \pmod{n} \Rightarrow ab \equiv a'b' \pmod{n} \Rightarrow \overline{ab} = \overline{a'b'}.$$

Mais $(\mathbb{Z}/n\mathbb{Z}, \otimes)$ n'est pas un groupe car il existe des éléments non inversibles. Par exemple, on se place dans $\mathbb{Z}/4\mathbb{Z}$ et on regarde la classe $\overline{2} \in \mathbb{Z}/4\mathbb{Z}$:

$$\begin{aligned}
\overline{2} \otimes \overline{0} &= \overline{2 \times 0} = \overline{0} \\
\overline{2} \otimes \overline{1} &= \overline{2 \times 1} = \overline{2} \\
\overline{2} \otimes \overline{2} &= \overline{2 \times 2} = \overline{0} \\
\overline{2} \otimes \overline{3} &= \overline{2 \times 3} = \overline{2}
\end{aligned}$$

La classe de $2 \in \mathbb{Z}/4\mathbb{Z}$ n'est donc pas inversible.

Pour cela, on va réduire l'ensemble $\mathbb{Z}/n\mathbb{Z}$ en son ensemble des éléments inversibles pour l'opération $\otimes$.

Définition 3.11 ($(\mathbb{Z}/n\mathbb{Z})^\times$). On définit l'ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$, l'ensemble de toutes les classes $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ inversibles par la multiplication $\otimes$.

Exemple 3.12. On se place dans l'ensemble $\mathbb{Z}/4\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\right\}$. On veut déterminer $(\mathbb{Z}/4\mathbb{Z})^\times$. On a vu que $\overline{2}$ n'est pas inversible pour $\otimes$, et évidemment, $\overline{0}$ n'est pas inversible pour $\otimes$. On cherche donc les inverses des éléments $\overline{1}$ et $\overline{3}$, on a :

$$\overline{1}^{-1} = \overline{1}, \ \overline{3}^{-1} = \overline{3}.$$

D'où :

$$(\mathbb{Z}/4\mathbb{Z})^\times = \left\{\overline{1}, \overline{3}\right\}$$

et c'est un groupe pour la multiplication.

PROPOSITION 3.13. $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible pour la multiplication si et seulement si $\mathrm{PGCD}(a, n) = 1$.

Démonstration. $\Diamond$

($\Rightarrow$) On suppose $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ inversible donc il existe $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{a} \otimes \overline{b} = \overline{1}$. On traduit cela en terme de la relation « congru modulo » :

$$ab \equiv 1 \pmod{n},$$

il existe donc $k \in \mathbb{Z}$ tel que $ab - nk = 1$, d'où $\mathrm{PGCD}(a, n) = 1$.

($\Leftarrow$) On suppose que $\mathrm{PGCD}(a, b) = 1$, il existe donc $u, v \in \mathbb{Z}$ tel que $au + bv = 1$, c'est-à-dire :

$$\overline{au + nv} = \overline{1}.$$

Or $\overline{nv} = \overline{0}$, ainsi :

$$\overline{au} = \overline{1}.$$

Donc $\overline{u}$ est inversible d'inverse $\overline{u}$.

□

Définition 3.14 (Fonction indicatrice d'Euler). L'indicatrice d'Euler $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ est une fonction telle que :

$$\varphi(1) = 1, \ \varphi(n) = \mathrm{card}\left\{k \in \{1, \ldots, n\}, \ \mathrm{PGCD}(k, n) = 1\right\}, \ \text{ pour } n > 1.$$

C'est-à-dire $\varphi(n)$ est le nombre d'entiers positifs et premiers à n.

Corollaire 3.15. L'ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$ est l'ensemble des classes $\overline{a}$ tels que $\mathrm{PGCD}(a,b) = 1$. Donc, d'après la définition 3.14, $(\mathbb{Z}/n\mathbb{Z})^\times$ a pour cardinal $\varphi(n)$.

PROPOSITION 3.16. Si p est un nombre premier alors $\varphi(p) = p - 1$.

Exemple 3.17. Pour $n = 5$, $(\mathbb{Z}/5\mathbb{Z})^\times = \left\{\overline{1}, \overline{2}, \overline{3}, \overline{4}\right\}$. On a : $\varphi(5) = 4$ et pour $1 \leq k \leq 5$, on obtient $\mathrm{PGCD}(k,5) = 1$ si $k \neq 5$.

Pour $n = 9$, on obtient :

$$(\mathbb{Z}/9\mathbb{Z})^\times = \left\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\right\}.$$

D'où $\varphi(9) = 6$.

3.3 Cryptographie

3.3.1 Le code César

Avant de décrire le procédé du « Code César », on fait un petit rappel historique.

Jules César (en latin, *Caius Iulius Caesar IV*) était un général romain, né à Rome en 100 av. J.-C. et mort à Rome en 44 av. J.-C. Il fut ambitieux et brillant, repoussa les frontières romaines jusqu'au Rhin et à l'océan Atlantique en conquérant la Gaule.

Pour crypter les messages qu'ils envoient à ces centurions, Jules César appliqua une méthode de chiffrement très simple que l'on va décrire maintenant.

Le chiffre de César consiste à décaler les lettres de quelques rangs vers la droite ou vers la gauche de l'alphabet. Par exemple, historiquement, Jules César les lettres de 3 rangs vers la droite.

Remarque 3.18. On se contentera dans cette partie, d'un cryptage avec un décalage de lettres de 3 à droite.

On peut dresser le tableau de cryptage suivant :

message clair	A	B	C	D	E	F	G	H	I	J	K	L	M
numéro clair NCl	1	2	3	4	5	6	7	8	9	10	11	12	13
décalage	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3
numéro crypté NCr	4	5	6	7	8	9	10	11	12	13	14	15	16
message crypté	D	E	F	G	H	I	J	K	L	M	N	O	P

message clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
numéro clair NCl	14	15	16	17	18	19	20	21	22	23	24*	25*	26*
décalage	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3
numéro crypté NCr	17	18	19	20	21	22	23	24	25	26	1	2	3
message crypté	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Remarque 3.19. Pour calculer le numéro crypté NCr des nombres NCl avec un astérisque, on doit calculer le reste de la division suivante $(NCl + 3) \div 26$ (ou prendre le reste de $NCl + 3$ congru modulo 26).

Cryptage d'un message. On veut crypter le message « ZEN » avec le « Code César ». On part d'un message clair à un message crypté : le décalage de lettres est donc de $+3$.

— $Z \to 26 \overset{+3}{\to} 29 \overset{29>26}{\to} 3 \to C$

— $E \to 5 \overset{+3}{\to} 8 \to H$

— $N \to 19 \overset{+3}{\to} 22 \to Q$.

Le message crypté est donc « CHQ ».

Décryptage d'un message. Avant de décrypter un message crypté, on doit remarquer quelque chose.

Remarque 3.20. Pour décrypter un message codé par le « Code César », on décale toutes les lettres du message crypté de trois rangs vers la gauche de -3.

On veut décrypter le message « FHVDU » par le « Code César » :
— $F \to 6 \overset{-3}{\to} 3 \to C$
— $H \to 8 \overset{-3}{\to} 5 \to E$
— $V \to 22 \overset{-3}{\to} 19 \to S$
— $D \to 4 \overset{-3}{\to} 1 \to A$
— $U \to 21 \overset{-3}{\to} 18 \to R$
Le message clair est donc « CESAR »

Remarque 3.21. Si on veut décrypter le message « CRR » crypté avec le « Code César », on fait comme ceci :
— $C \to 3 \overset{-3}{\to} 0 \overset{0<1}{\to} 26 \to Z$
— $R \to 17 \overset{-3}{\to} 14 \to O$
— $R \to 17 \overset{-3}{\to} 14 \to O$
Le message clair est donc « ZOO ».

Exercice 3.22.
1. Décrypter le message « ERQMRXU ! » crypté avec le « Code César ».
2. Crypter un message court avec le « Code César »

3.3.2 Le cryptage RSA

Le cryptage RSA (du nom des inventeurs, Ronald Rivest, Adi Shamir et Leonard Adleman) est intéressant car la clé de cryptage est publique et il n'a donc pas de risques liés à l'envoi de la clé et au procédé de codage des données. Bon, comme tout le monde, peut crypter et envoyer un message. Par contre, seul la destinataire, Alice, qui connaît la clé privée correspondante pourra reconstituer le message initial.

Alice, la destinataire rend publique deux nombres n et c où n est le produit de deux grands nombres premiers p et q qu'elle est seule à connaître, où c est un entier premier avec le produit $(p-1)(q-1)$ compris entre 2 et $(p-1)(q-1)$.

Pour coder le message « Bonjour », par exemple, on commence par remplacer les lettres par leurs positions dans l'ordre alphabétique, ce qui donne :

$$02\ 15\ 14\ 10\ 15\ 21\ 18.$$

Si on utilise $n = 10573 = 97 \times 109$, on peut regrouper les chiffres par 4 sans risquer de dépasser n. Ce qui donne $0215\ 1410\ 1521\ 0018$. Pour chaque nombre a de la série, on déterminer alors b, reste de la division de a^c par n. On obtient alors dans ce cas avec $c = 5$ la série :

$$9131\ 7391\ 0690\ 7574.$$

C'est cette série de nombres qu'envoie Bob à Alice.

Alice qui connaît les deux facteurs premiers de n (ici $p = 97$ et $q = 109$) déterminer alors le nombre entier d vérifiant $1 < d < (p-1)(q-1)$ et tel que :

$$cd \equiv 1 \pmod{(p-1)(q-1)}.$$

Ici, $d = 6221$.

Alice peut alors retrouver la série initiale de nombres car, pour chaque entier b de cette série, on démontre que b^d est congrue à a modulo n.

L'intérêt pour Alice est bien sûr d'avoir un nombre n produit de deux nombres premiers très grands de façon à ce que les calculateurs même les plus rapides ne puissent pas trouver en un temps suffisamment court les deux facteurs premiers nécessaires pour calculer d.

On note, d'autre part, que c et d jouent le même rôle et sont interchangeables. Ainsi Alice peut décider de coder elle-même un message en utilisant sa clé privée $d = 6621$. Bob décryptera alors aisément ce message avec la clé publique c. Le message envoyé à Bob constitue en fait une signature du message d'Alice. En effet, si Bob réussit à décrypter sans problème le message à l'aide de la clé c, c'est que ce message a été codé avec la clé privée d connue d'Alice seule et cela suffit pour en garantir l'authenticité.

On donne quelques propriétés permettant de justifier la robustesse de la méthode RSA.

PROPRIÉTÉ 3.23. Soient p et q deux nombres premiers. Si c, tel que $1 < c < (p-1)(q-1)$, est premier avec le produit $(p-1)(q-1)$ alors il existe un unique d tel que $1 < d < (p-1)(q-1)$ et vérifiant

$$cd \equiv 1 \pmod{(p-1)(q-1)}.$$

PROPRIÉTÉ 3.24. Dans les conditions précédentes, si p et q sont différents et si $b \equiv a^c \pmod{pq}$ alors $b^d \equiv a \pmod{pq}$.

3.3.3 Le numéro INSEE

Le numéro INSEE ou numéro de Sécurité Sociale est formé de 15 chiffres déterminés pour chaque individu de la façon suivante :

- 1 chiffre pour le sexe : Homme (1) et Femme (2) ;
- 2 chiffres correspondant aux deux derniers chiffres de l'année de naissance ;
- 2 chiffres correspondant au mois de naissance ;
- 2 chiffres correspondant au département de naissance ;
- 3 chiffres correspondant à la commune de naissance ;
- 3 chiffres correspondant au numéro d'inscription sur le registre des naissances ;
- 2 chiffres correspondant à une clé de contrôle. La clé de contrôle est ainsi déterminée de la manière suivante : « *On prend le nombre formé par les 13 premiers chiffres, on cherche son reste r dans la division par 97, la clé est alors égale au nombre $97 - r$ écrit avec deux chiffres (le premier étant éventuellement un 0).* »

Exercice 3.25.

1. Vérifier la clé de contrôle associée au numéro 2 85 05 33 565 001 89.
2. On change le dixième chiffre « 5 » par le chiffre « 9 ». Montrer qu'alors la clé de contrôle permet de détecter l'erreur.

Solution. ♢

1. On fait la division euclidienne de 2 850 533 565 001 par 97. On trouve un reste de 8. Ainsi, $97 - 8 = 89$, ce qui est bien notre clé de contrôle.
2. Si on change le dixième chiffre « 5 » par le chiffre « 9 », on obtient le nombre 2 850 533 569 001. On effectue la division euclidienne de ce nombre par 97 et on trouve un reste de 31. Ainsi, on peut constater que la clé de contrôle change car $97 - 31 = 66 \neq 89$.

□

3.4 D'autres problèmes pour introduire la notion de congruences à des collégiens

3.4.1 Promenade sur un cercle

Deux promeneurs, Matt et Matic se promènent sur un cercle. Le cercle parcouru est jalonné de 3 plots : le plot $\overline{0}$, le plot $\overline{1}$ et le plot $\overline{2}$.

Matt et Matic se promène sur le cercle, ils démarrent du plot $\overline{0}$ pour aller au plot $\overline{1}$... puis continuent leur chemin du plot $\overline{1}$ pour aller au plot $\overline{2}$ puis du plot $\overline{2}$ pour arriver au point de départ, le plot $\overline{0}$.

1. Matt et Matic se promènent sur le cercle. Ils affirment qu'après 23 tours de cercle, ils se retrouvent sur le plot $\overline{1}$. Combien de plots ont-ils rencontrés durant leur parcours ?
2. Matt et Matic se promènent de nouveau sur le cercle. Ils affirment qu'ils ont rencontré 125 plots durant leur trajet. Combien ont-ils fait de tours de cercle ? À quel plot ont-ils terminé leur trajet ?

Solutions. ♢

1. Le nombre de plots rencontrés durant leur parcours est :
$$23 \times 3 + 1 = 69 + 1 = 70.$$
2. On fait la division euclidienne de 125 par 3. On trouve un quotient de 41 et un reste 2. Ainsi, Matt et Matic ont fait 41 tours de cercle et s'arrêtent au plot $\overline{2}$.

□

Exercice 3.26. Sur un cercle de 7 plots :

1. Matt et Matic ont fait 12 tours et sont arrivés sur le plot $\overline{5}$. Combien de plots ont-ils rencontrés sur leur route ?
2. Ils ont rencontré sur leur trajet, 801 plots. Combien ont-ils fait de tours de cercle ? À quel plot ont-ils terminé leur trajet ?
3. Reprendre les questions 1 et 2 avec un cercle de 13 plots.

3.4.2 Partage de bonbons

Lola veut partager le plus équitablement possible ses 84 bonbons avec ses 5 amis. Elle mangera ainsi les bonbons qui lui reste.

1. Combien de bonbons recevront chacun des amis de Lola ?
2. Combien de bonbons mangera-t-elle au final ?

♢

On peut voir une similitude avec le problème de la « Promenade sur un cercle ».

Promenade circulaire	Partage de bonbons
Nombre de plots par tour	Nombre d'amis
Nombre de plots rencontrés	Nombre total de bonbons
Nombre de tours de cercle	Nombre de bonbons donnés à chacun
Numéro du plot final	Nombre de bonbons mangés par Lola

Le problème peut être reformulé en terme de promenade circulaire : « Sur un cercle de 5 plots, Matt et Matic ont rencontré sur leur trajet, 84 plots. Combien ont-ils fait de tours de cercle ? À quel plot ont-ils terminé leur trajet ? »

Solution. On fait la division euclidienne de 84 par 5. On trouve un quotient de 16 et un reste de 4.
Lola devra donner à chacun de ses amis, 16 bonbons. Elle mangera les 4 restants. □

Remarque 3.27. On peut donner une variante plus difficile à ce problème : « Martin a un certain nombre de bonbons qu'il veut partager équitablement avec ses 10 amis. Après le partage, il mange les bonbons qu'il n'a pas pu partagé.

Quel est le nombre de bonbons que Martin doit posséder pour que le partage soit totalement équitable (c'est-à-dire qu'après partage, Martin doit manger autant de bonbons que chacun de ses amis) ? »

3.4.3 Un Immeuble, des Étages, des Appartements (IEA)

Dans un immeuble, il y a huit étages. Les numéros des appartements sont agencés comme suivant :
— l'appartement n° 1 se trouve à l'étage 1 ;
— l'appartement n° 2 se trouve à l'étage 2 ;
— ...
— l'appartement n° 8 se trouve à l'étage 8 ;
— l'appartement n° 9 se trouve à l'étage 1 ;
— l'appartement n° 10 se trouve à l'étage 2...
À quel étage se trouve l'appartement n° 31 ?
◊
Là encore, on peut trouver des similitudes avec le problème de la « Promenade sur le cercle » :

Promenade circulaire	IEA
Nombre de plots par tour	Nombre d'étages
Nombre de plots rencontrés	Numéro de l'appartement à trouver
Nombre de tours de cercle	Position de l'appartement sur le palier
Numéro du plot final $+1$[1]	Numéro d'étage où se trouve l'appartement

On peut reformulé le problème IEA en terme de promenade circulaire : « Sur un cercle de 8 plots, Matt et Matic ont rencontré sur leur trajet, 31 plots. À quel plot ont-ils terminé leur trajet ? ».

Solution. On fait la division euclidienne de 31 par 8. On trouve un quotient de 3 et un reste de 7. Ainsi, l'appartement n° 31 se trouve au septième étage. □

Remarque 3.28. Bien que la division euclidienne de 32 par 8 donne 0 comme reste, l'appartement n° 32 se situe bien au huitième étage.

3.4.4 Rangement de Boules dans des Urnes (RBU)

On dispose de 9 urnes numérotées de 1 à 9 et 100 boules numérotées de 1 à 100.
— La boule 1 est déposée dans l'urne n° 1 ;
— la boule 2 est déposée dans l'urne n° 2 ;
— ...
— la boule 9 est déposée dans l'urne n° 9 ;
— la boule 10 est déposée dans l'urne n° 1 ;
— la boule 11 est déposée dans l'urne n° 2...
À quelle urne sera déposée la boule 67 ?
◊
Encore une fois, on peut y voir des similitudes avec le problème de la « Promenade sur le cercle ».

Promenade circulaire	RBU
Nombre de plots par tour	Nombre d'urnes
Nombre de plots rencontrés	Numéro de la boule cible
Nombre de tours de cercle	Position de boules par urne
Numéro du plot final $+1$[2]	Numéro d'étage où se retrouve la boule cible

On peut reformuler le problème RBU en terme de promenade circulaire : « Sur un cercle de 9 plots, Matt et Matic ont rencontré sur leur trajet, 67 plots. À quel plot ont-ils terminé leur trajet ? »

Solution. On fait la division euclidienne de 67 par 9. On trouve un quotient de 7 et un reste de 4. Ainsi, la boule 67 sera placée dans l'urne n° 4. □

1. les plots sont numérotés $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{7}$, $\overline{8}$
2. les plots sont numérotés $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{7}$, $\overline{8}$, $\overline{9}$

Remarque 3.29. On peut donner une variante plus difficile au problème RBU. « On dispose de 8 urnes numérotées de 1 à 9 et 100 boules numérotées de 1 à 100.

— La boule 1 est déposée dans l'urne n^o 1 ;
— la boule 2 est déposée dans l'urne n^o 2 ;
— $\ldots$;
— la boule 8 est déposée dans l'urne n^o 8 ;
— la boule 9 est déposée dans l'urne n^o 9 ;
— la boule 10 est déposée dans l'urne n^o 8 ;
— la boule 11 est déposée dans l'urne n^o 7...

À quelle urne sera déposée la boule 67 ? »

3.5 Les soldats chinois

Le mathématicien et astronome chinois Sun Zi (né en Chine entre le III^e et le IV^e siècle) publia dans son livre *Sun Tzu Suan Ching* un théorème qui permet de résoudre le problème suivant (problème de décompte des soldats de l'armée du général Han Xing) :

« Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats, et rangés par 7 colonnes, il reste deux soldats ? »

La résolution proposée par Sun Zin pour ce problème est la suivante : « *Multiplie le reste de la division par 3, c'est-à-dire 2, par 70, ajoute-lui le produit du reste de la division par 5, c'est-à-dire 3, avec 21 puis ajoute le produit du reste de la division par 7, c'est-à-dire 2 par 15. Tant que le nombre est plus grand que 105, retire 105.* ».

On remarque que :

— 70 a pour reste 1 dans la division par 3 et pour reste 0 dans les divisions par 5 et 7 ;
— 21 a pour reste 1 dans la division par 5 et pour reste 0 dans les divisions par 3 et 7 ;
— 15 a pour reste 1 dans la division par 7 et pour reste 0 dans les divisions par 3 et 5.

Le nombre $2\times70+3\times21+2\times15$ a bien alors pour restes respectifs 2, 3 et 2 dans les divisions par 3, 5 et 7. Enfin, comme 105 a pour reste 0 dans les trois types de division, on peut l'ôter ou l'ajouter autant de fois que l'on veut sans changer les valeurs des restes. La plus petite valeur pour le nombre d'objets est alors de 23.

THÉORÈME 3.30 (THÉORÈME DES RESTES CHINOIS). Soient n_1, ..., n_k des entiers deux à deux premiers entre eux, c'est-à-dire que $\mathrm{PGCD}(n_i, n_j) = 1$ lorsque $i \neq j$. Alors pour tous entiers a_1, ..., a_k, il existe un entier x, unique modulo $n = \prod_{i=1}^{k} n_i$, tel que :

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \quad \vdots \\ x \equiv a_k \pmod{n_k}. \end{cases}$$

Méthode 3.31. Une solution x peut être trouvée de la manière suivante. Pour chaque i, les entiers n_i et

$$\tilde{n}_i = \frac{n}{n_i} = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$$

sont premiers entre eux. D'après le théorème de Bachet-Bézout, on peut calculer l'inverse v_i de $\tilde{n}_i$ modulo n_i. Pour cela, on utilise l'algorithme d'Euclide étendu et on peut obtenir des entiers u_i et v_i tels que $u_i n_i + v_i \tilde{n}_i = 1$. Si on pose $e_i = v_i \tilde{n}_i$, alors on a :

$$e_i \equiv 1 \pmod{n_i} \quad \text{et} \quad e_i \equiv 0 \pmod{n_j} \quad \text{pour } j \neq i.$$

Une solution particulière de ce système de congruences est par conséquent :

$$x = \sum_{i=1}^{k} a_i e_i,$$

et les autres solutions sont les entiers congrus à x modulo le produit n.

Exemple 3.32. On peut traduire le problème de comptage des soldats de l'armée du général Han Xing par un système de congruences :

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

on obtient alors :
- $n = 3 \times 5 \times 7 = 105$;
- $n_1 = 3$ et $\tilde{n}_1 = 35$, or $2\tilde{n}_1 \equiv 1 \pmod 3$ donc $e_1 = 70$;
- $n_2 = 5$ et $\tilde{n}_2 = 21$, or $\tilde{n}_2 \equiv 1 \pmod 5$ donc $e_2 = 21$;
- $n_3 = 7$ et $\tilde{n}_3 = 15$, or $\tilde{n}_3 \equiv 1 \pmod 7$ donc $e_3 = 15$.

Une solution pour x est alors :

$$x = 2 \times 70 + 3 \times 21 + 2 \times 15 = 233$$

et les solutions sont tous les entiers congrus à 233 modulo 105, c'est-à-dire 23 modulo 105.

4 Compléments sur les relations

4.1 Relations binaires

Définition 4.1. Une *relation binaire* $\mathcal{R}$ sur un ensemble E est une propriété portant sur les couples d'éléments de E. On notera $a\mathcal{R}b$ le fait que la propriété est vraie pour le couple $(a, b) \in E \times E$.

Exemples 4.2.
- L'inégalité $\leq$ est une relation sur $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$.
- Le parallélisme et l'orthogonalité sont des relations sur l'ensemble des droites du plan ou de l'espace.
- L'inclusion $\subset$ est une relation sur $\mathcal{P}(X)$ où X est un ensemble quelconque.

Définition 4.3. Soit $\mathcal{R}$ une relation sur un ensemble E.
- $\mathcal{R}$ est réflexive si pour tout $x \in E$, on a $x\mathcal{R}x$;
- $\mathcal{R}$ est symétrique si pour tout $x, y \in E$, on a $x\mathcal{R}y \Rightarrow y\mathcal{R}x$;
- $\mathcal{R}$ est antisymétrique si pour tout $x, y \in E$, on a $(x\mathcal{R}y$ et $y\S) \Rightarrow x = y$;
- $\mathcal{R}$ est transitive si pour tout $x, y, z \in E$, $(x\mathcal{R}y$ et $y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.

4.2 Relations d'équivalence

Définition 4.4. Une relation binaire est une *relation d'équivalence* si et seulement si elle est réflexive, symétrique et transitive.

Exemples 4.5.
- Le parallélisme est une relation d'équivalence sur l'ensemble des droites.
- Soit E et F deux ensembles et f une application de E dans F. La relation sur E définie par $a\mathcal{R}b \Leftrightarrow f(a) = f(b)$ est une relation d'équivalence.

Définition 4.6. Soit $\mathcal{R}$ une relation d'équivalence sur E et a un élément de E. On appelle *classe d'équivalence* de a l'ensemble $\mathcal{C}(a) = \{x \in E,\ x\mathcal{R}a\}$.

PROPRIÉTÉ 4.7. Si $\mathcal{R}$ est une relation d'équivalence sur E et que $a, b \in E$ vérifiant $a\mathcal{R}b$, alors a et b ont même classe d'équivalence.

THÉORÈME 4.8. Une relation d'équivalence $\mathcal{R}$ sur un ensemble E définit une partition de E dont les éléments sont les classes d'équivalence de $\mathcal{R}$.

Réciproquement, une partition de E définit sur E une relation d'équivalence dont les classes coïncident avec les éléments de la partition.

Définition 4.9. L'ensemble des classes d'équivalence se nomme *ensemble quotient* de E par $\mathcal{R}$ et se note $E/\mathcal{R}$.

L'application $E \to E/\mathcal{R}$ qui à tout élément x de E associe sa classe d'équivalence se nombre *application* (ou *projection*) *canonique*.

4.3 Relations d'ordre

Définition 4.10. Une relation binaire $\mathcal{R}$ sur E est une relation *d'ordre* si et seulement si elle est réflexive, antisymétrique et transitive. On dit alors que E est un ensemble *ordonné* (par $\mathcal{R}$). Une relation d'ordre est souvent notée $\leq$.

Exemples 4.11.
— L'inégalité $\leq$ est une relation d'ordre sur $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$.
— L'inclusion est une relation d'ordre.

Définition 4.12. Une relation d'ordre sur E est dite *totale* si deux éléments quelconques de E sont toujours comparables : pour tout $x, y \in E$, on a $x\mathcal{R}y$ et $y\mathcal{R}x$.

Dans le cas contraire, on dit que l'ordre est partiel.

Exemples 4.13.
— $\leq$ est un ordre total sur $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{R}$.
— En général, l'inclusion est un ordre partiel.
— La divisibilité dans $\mathbb{N}^*$ est un ordre partiel.

Définition 4.14. Une relation binaire est un ordre strict si elle est transitive et vérifie $x\mathcal{R}y \Rightarrow x \neq y$.

Exemple 4.15. L'inégalité stricte $<$ définit un ordre strict sur $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{R}$.

Définition 4.16. Soit $(E, \leq)$ un ensemble ordonné, et A une partie non vide de E.
— si $a \in E$ vérifie $x \leq a$ (resp. $x \geq a$) pour tout $x \in A$, on dit que a est un *majorant* (resp. *minorant*) de A ;
— si $a \in A$ est un majorant (resp. minorant) de A, on dit que a est un *maximum* (resp. *minimum*) de A. On note $a = \max A$ (resp. $a = \min A$) ;
— Si l'ensemble des majorants de A n'est pas vide et qu'il admet un minimum (resp. maximum), il est appelé *borne supérieure* (resp. *borne inférieure*) de A et se note $\sup A$ (resp. $\inf A$).