Propriétés de $\mathbb{Z}/n\mathbb{Z}$

Louis Nebout

Le but de ce cours est de présenter le point du vue moderne sur l'arithmétique, issu de l'algèbre. Rien de ceci n'est officiellement au programme des olympiades et une partie des résultats vous est certainement déjà connue sous une formulation différente, mais une bonne connaissance de cette théorie permet de mieux comprendre ce qui se passe, et de prouver quelques résultats très puissants.

1 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geqslant 2$ un entier naturel. Quelle est précisement la nature de la formule $a \equiv b\,[n]$? Ce n'est pas une vraie égalité : cela veut dire qu'il existe une certaine relation d'équivalence, la relation de congruence, pour laquelle a et b sont en relation. Maintenant, si $a \equiv b\,[n]$ et $c \equiv d\,[n]$, on sait bien que $a + c \equiv b + d\,[n]$, et de même avec la multiplication. Ainsi, cette relation possède en fait des propriétés tout à fait similaires à l'égalité, et on aimerait bien dire que « on peut additionner et multiplier les modulo », mais cette phrase n'a aucun sens mathématique. Pour lui donner du sens, on aimerait bien la « transformer » en une véritable égalité, en « faisant de deux entiers congrus modulo n un seul et même nombre ».

Si x est un entier, on appelle *classe d'équivalence de* x *modulo* n l'ensemble des entiers congrus à x modulo n. On note $\overline{x}$ la classe de x. Attention, si $x \equiv y \pmod{n}$, alors $\overline{x}$ et $\overline{y}$ sont deux notations pour un seul et même objet. On obtient exactement n classes d'équivalence : $\overline{0}$, $\overline{1}$, …, $\overline{n-1}$, et on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble de ces classes d'équivalence. On munit $\mathbb{Z}/n\mathbb{Z}$ de deux opérations $+$ et $\times$ en posant $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x} \times \overline{y} = \overline{x \times y}$. Il y a une subtilité : il faut prouver que ces opérations sont bien définies, c'est-à-dire que les résultats de ces opérations ne dépendent pas des choix des représentants x et y de $\overline{x}$ et $\overline{y}$, par exemple pour $+$, que si $\overline{x} = \overline{x'}$ at $\overline{y} = \overline{y'}$, alors $\overline{x+y} = \overline{x'+y'}$: c'est une simple reformulation du fait que la relation de congruence est compatible avec les opérations.

La construction de $\mathbb{Z}/n\mathbb{Z}$ peut paraître conceptuellement difficile la première fois qu'on la voit, mais en fait, la manipulation de cet ensemble est très simple en pratique : écrire $\overline{x}+\overline{y} = \overline{z}$ est rigoureusement équivalent à écrire $x+y \equiv z \mod n$, par exemple. Pour passer d'une écriture à l'autre, on enlève les barres et on remplace l'égalité par une relation de congruence. Mais l'énorme avantage conceptuel de l'utilisation de $\mathbb{Z}/n\mathbb{Z}$ est, dans le cas de $\mathbb{Z}/5\mathbb{Z}$ par exemple, le fait que $\overline{2}$ et $\overline{7}$ sont *un seul et même nombre*, et non plus simplement congrus. De plus, $\mathbb{Z}/n\mathbb{Z}$ possède une certaine structure algébrique, qui nous permet de réaliser toutes nos opérations en restant à l'intérieur de $\mathbb{Z}/n\mathbb{Z}$, et donc sans avoir à repasser par les entiers.

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est donc muni de deux opérations, une addition et une multiplication, toutes deux commutatives et associatives, et telles que

— La loi $+$ admet un élément neutre, $\overline{0}$, tel que pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, $x + \overline{0} = x$;
— Tout élément x de $\mathbb{Z}/n\mathbb{Z}$ admet un opposé noté $-x$, tel que $x + (-x) = \overline{0}$ (celui-ci est unique).
— $\times$ est distributive sur $+$ ($(x + y) \times z = x \times z + y \times z$),
— La loi $\times$ admet un élément neutre, $\overline{1}$, tel que pour tout $x \in \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$, $x \times \overline{1} = x$.

En algèbre, on appelle un tel ensemble un *anneau* (commutatif). Les anneaux sont fondamentaux, car ils apparaissent dans bien des domaines, et les mathématiciens ont donc développé une théorie générale traitant de ce type d'objets. Je n'en dirai pas plus pour l'instant.

2 Inversibilité

Proposition 1. On dit que $a \in \mathbb{Z}/n\mathbb{Z}$ est *inversible* s'il existe $b \in \mathbb{Z}/n\mathbb{Z}$, appelé l'*inverse* de a et noté a^{-1}, tel que $a \times b = \overline{1}$. Les inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $\overline{k}$, où k est un entier premier avec n.

Démonstration. C'est une reformulation du théorème de Bézout, en effet on a les équivalences suivantes.

Il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \mod n$
$\Leftrightarrow$ il existe $b \in \mathbb{Z}$ et $k \in Z$ tels que $ab = kn + 1$
$\Leftrightarrow$ a est premier avec n. □

Remarque 2. Si on sait que $ab = ac$ dans $\mathbb{Z}/n\mathbb{Z}$, on peut donc conclure $b = c$ **dans le cas où** a **est premier avec** n : il suffit de multiplier des deux côtés par l'inverse de a. C'est faux en général. Par exemple, $\overline{2} \times \overline{1} = \overline{2} \times \overline{3} = \overline{2}$ dans $\mathbb{Z}/4\mathbb{Z}$ mais il est faux que $\overline{1} = \overline{3}$.

Si p désigne un nombre premier, on a ainsi que tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ autres que $\overline{0}$ sont inversibles. On appelle *corps* un anneau vérifiant cette propriété. Dans un corps, on dispose donc d'une opération fondamentale qui n'existe pas dans les anneaux : la division. Ainsi, les corps sont des objets algébriques beaucoup plus riches. Par exemple, la théorie des polynômes fonctionne très bien sur les corps, et nous allons donc étudier les polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Noter que de tels polynômes seraient délicats à définir sans l'introduction de $\mathbb{Z}/p\mathbb{Z}$:

3 Polynômes sur $\mathbb{Z}/p\mathbb{Z}$

Définition 3. Un polynôme sur $\mathbb{Z}/p\mathbb{Z}$ est une expression de la forme :

$$a_0 + a_1X + a_2X^2 + ... + a_dX^d$$

avec les a_i dans $\mathbb{Z}/p\mathbb{Z}$.

On note $\mathbb{Z}/p\mathbb{Z}[X]$ l'ensemble de ces polynômes.

Remarque 4. Sur $\mathbb{R}$, on peut assimiler un polynôme et la fonction de $\mathbb{R}$ dans $\mathbb{R}$ qui lui correspond. Sur $\mathbb{Z}/p\mathbb{Z}$ il faut être plus prudent. Par exemple, $a^p - a = \overline{0}$ pour tout a donc la fonction correspondant au polynôme $X^p - X$ est la fonction nul. En revanche, ce n'est pas le polynôme nulle : un polynôme est défini par ses coefficients.

Lemme 5. Soient a et b dans $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$, alors $a \times b$ est dans $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$.

Remarque 6. On dit que $\mathbb{Z}/p\mathbb{Z}$ est *intègre*.

Démonstration. Si on avait $a \times b = \overline{0}$, en multipliant par a^{-1} et b^{-1} on obtiendrait $\overline{1} = \overline{0}$, c'est absurde. □

Ce lemme facile nous permet de définir une notion satisfaisante de degré sur $\mathbb{Z}/p\mathbb{Z}[X]$, l'ensemble des polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. En effet, si P et Q ont pour termes dominants $a \cdot X^k$ et $b \cdot X^l$, alors $ab \cdot X^{k+l}$ sera non nul, et sera le terme dominant de $P \cdot Q$. Nous sommes maintenant en mesure de prouver :

Proposition 7. Il y a une notion de division euclidienne sur $\mathbb{Z}/p\mathbb{Z}[X]$: soient A et B dans $\mathbb{Z}/p\mathbb{Z}[X]$ avec B non nul, alors il existe un unique couple (Q, R) de polynômes de $\mathbb{Z}/p\mathbb{Z}[X]$ tels que $A = Q \cdot B + R$, avec $\deg(R) < \deg(B)$.

Démonstration. La preuve est la même que dans $\mathbb{R}[X]$. Pour l'unicité, soit (Q', R') un deuxième tel couple, alors $B \cdot (Q - Q') = R' - R$, puis $Q = Q'$ en examinant les degrés.

Pour l'existence, on vérifie que l'algorithme usuel fonctionne, car le coefficient dominant de B est inversible. Par exemple, pour diviser $A = \overline{5} \cdot X^3 + \overline{2} \cdot X^2 + \overline{5} \cdot X$ par $B = \overline{3} \cdot X^2 + \overline{6} \cdot X + \overline{2}$ dans $\mathbb{Z}/7\mathbb{Z}$, on commence par retrancher $\overline{5} \cdot \overline{3}^{-1} \cdot X \cdot B$ à A, le coefficient dominant de Q doit donc être $\overline{5} \cdot \overline{3}^{-1} \cdot X = \overline{5} \cdot \overline{5} \cdot X = \overline{4} \cdot X$. Il reste $A - \overline{4} \cdot X \cdot B = \overline{6} \cdot X^2 + \overline{4} \cdot X$. On retranche donc $\overline{6} \cdot \overline{3}^{-1} \cdot B$. Au final, on obtient $A = Q \cdot B + R$ avec $Q = \overline{4} \cdot X + \overline{2}$ et $R = \overline{6} \cdot X + \overline{3}$. □

Corollaire 8. Soit P dans $\mathbb{Z}/p\mathbb{Z}[X]$, et a une racine de P. Alors P est divisible par $(X - a)$, i.e. il existe Q dans $\mathbb{Z}/p\mathbb{Z}[X]$ tel que $P = (X - a) \cdot Q$.

Démonstration. Soit $P = (X - a) \cdot Q + R$ la division euclidienne de P par $(X - a)$. Alors R est de degré inférieur strictement à 1, donc constant, et l'évaluation de l'expression précédente en a nous donne $R = \overline{0}$. □

Corollaire 9. Un polynôme de degré n dans $\mathbb{Z}/p\mathbb{Z}[X]$ a au plus n racines.

Démonstration. Soit P de degré n dans $\mathbb{Z}/p\mathbb{Z}[X]$. Supposons qu'il admette n racines $a_1, a_2, \ldots, a_n$. D'après le corollaire précédent, il existe une constante c non nulle tel que

$$P = c \cdot \Pi_{i=1}^{n}(X - a_i).$$

Soit alors a une racine de P. On a

$$\overline{0} = c \cdot \Pi_{i=1}^{n}(a - a_i),$$

et, d'après le lemme, un des $(a - a_i)$ est nul, donc a est l'un des a_i. □

Soit a dans $\mathbb{Z}/p\mathbb{Z}$, en appliquant cela au polynôme $X^k - a$, on obtient un résultat important : a a au plus k racines k-ièmes ! La section suivante en donne une importante application.

Exercice 1

Résoudre dans $\mathbb{Z}/12\mathbb{Z}$ l'équation $x^2 + \overline{3}x + \overline{2} = 0$.

Exercice 2 (Théorème de Wilson)

Soit $p \geqslant 2$ un entier naturel. Montrer que p est premier si et seulement si $(p-1)! \equiv -1 \mod p$.

Exercice 3

Soit $p \geqslant 5$ un nombre premier. Soient $a, b \in \mathbb{Z}$ tels que $1 + \frac{1}{2} + ... + \frac{1}{p-1} = \frac{a}{b}$. Montrer que $p^2 \mid a$.

4 Carrés dans $\mathbb{Z}/p\mathbb{Z}$

Définition 10. Soit $x \in \mathbb{Z}$. On dit que x est un résidu quadratique modulo p (ou encore que $\overline{x}$ est un résidu quadratique dans $\mathbb{Z}/p\mathbb{Z}$) si x n'est pas divisible par p et si $\overline{x}$ est le carré d'un élément de $\mathbb{Z}/p\mathbb{Z}$.

On note :

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ est un résidu quadratique modulo } p \\ 0 & \text{si } p \mid x \\ -1 & \text{sinon} \end{cases}$$

Le symbole $\left(\frac{x}{p}\right)$ s'appelle le symbole de Legendre.

Théorème 11 (Critère d'Euler)**.** Soit p un nombre premier impair, et $x \in (\mathbb{Z}/p\mathbb{Z})^*$. Alors x est un résidu quadratique si et seulement si $x^{\frac{p-1}{2}} = \overline{1}$. Sinon, on a $x^{\frac{p-1}{2}} = -\overline{1}$.

Autrement dit, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ pour tout $x \in \mathbb{Z}/p\mathbb{Z}$

Démonstration. Commençons par dénombrer les résidus quadratiques de $(\mathbb{Z}/p\mathbb{Z})^*$. Soit a un résidu quadratique, disons que $a = y^2$ avec $y \in (\mathbb{Z}/p\mathbb{Z})^*$. On a alors aussi $a = (-y)^2$, or $y \neq -y$ puisque p est impair, donc a est le carré d'au moins deux éléments de $(\mathbb{Z}/p\mathbb{Z})^*$. En fait, c'est le carré d'exactement deux éléments, car le polynôme $X^2 - a$ est de degré 2, donc admet au plus deux racines dans $\mathbb{Z}/p\mathbb{Z}$. Puisque $(\mathbb{Z}/p\mathbb{Z})^*$ possède $p-1$ éléments, et puisque chaque résidu quadratique est le carré d'exactement deux de ces éléments, on en déduit qu'il y a exactement $\frac{p-1}{2}$ résidus quadratiques.

Tous ces résidus quadratiques vérifient $x^{\frac{p-1}{2}} = \overline{1}$, puisqu'en les écrivant $x = y^2$, on obtient $x^{\frac{p-1}{2}} = y^{p-1} = \overline{1}$, par petit Fermat. Il s'agit de montrer que c'est les seuls. Mais le polynôme $X^{\frac{p-1}{2}} - \overline{1}$ a au plus $\frac{p-1}{2}$ racines dans $\mathbb{Z}/p\mathbb{Z}$, et tous les résidus quadratiques, qui sont au nombre de $\frac{p-1}{2}$, en sont racines. Donc ce sont les seules, ce qui conclut la première affirmation du théorème.

Pour démontrer la seconde partie, il suffit de montrer que la fonction $f(x) = x^{\frac{p-1}{2}}$ ne prend que les valeurs $\overline{1}$ et $-\overline{1}$ lorsque x parcourt $(\mathbb{Z}/p\mathbb{Z})^*$. Mais $f(x)^2 = x^{p-1} = \overline{1}$, donc les valeurs prises par f sur $(\mathbb{Z}/p\mathbb{Z})^*$ sont des racines carrées de 1 : ce sont donc $\overline{1}$ et $-\overline{1}$.

□

Cette preuve, ou du moins le premier paragraphe, est à connaître, car elle donne des informations sur la répartition des résidus quadratiques : leur nombre, et le fait que chacun soit le carré d'exactement deux éléments *opposés*. On peut en déduire, par exemple, que 1^2, 2^2, ..., $\left(\frac{p-1}{2}\right)^2$ forme un système complet de représentants des résidus quadratiques de $\mathbb{Z}/p\mathbb{Z}$, car ils sont au nombre de $\frac{p-1}{2}$ et sont deux-à-deux non-opposés.

Une autre remarque importante est que le critère d'Euler peut se reformuler de la façon suivante à l'aide du symbole de Legendre : pour tout nombre premier impair p et pour tout $x \in \mathbb{Z}$, on a $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \mod p$ (on remarquera que ceci marche *même* si $p \mid x$). On en déduit immédiatement que le symbole de Legendre est *complètement multiplicatif* par rapport à son

argument supérieur, autrement dit, pour tous $x, y \in \mathbb{Z}$, on a $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$. En particulier, le produit de deux résidus quadratiques est un résidu quadratique, et l'inverse d'un résidu quadratique est un résidu quadratique (on dit que l'ensemble des résidus quadratiques est un *sous-groupe* de $(\mathbb{Z}/p\mathbb{Z})^*$), mais aussi, le produit de deux non-résidus quadratiques est un résidu quadratique, et le produit d'un résidu quadratique et d'un non-résidu quadratique n'est pas un résidu quadratique.

Voici enfin un célèbre résultat dû à Gauss, peu utile en pratique dans les exercices mais qu'il est toujours bon de connaître :

Théorème 12 (Loi de réciprocité quadratique)**.** Soient p et q deux nombres premiers impairs.

- Si au moins un des deux nombres p et q est congru à 1 modulo 4, alors q est un résidu quadratique modulo p si et seulement si p est un résidu quadratique modulo q ;
- Si les deux nombres p et q sont congrus à 3 modulo 4, alors q est un résidu quadratique modulo p si et seulement si p n'est pas un résidu quadratique modulo q.

À l'aide du symbole de Legendre, on peut reformuler ce résultat de la manière suivante : pour tous nombre premiers impairs p et q, on a :

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

Ce théorème ne dit rien du cas où $p = 2$. Pour cela, on a la proposition suivante :

Proposition 13. Soit p un nombre premier impair. Alors 2 est un résidu quadratique modulo p si et seulement si p est congru à 1 où à -1 modulo 8. Autrement dit, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Avec la loi de réciprocité quadratique ainsi que la proposition précédente, on peut déterminer très rapidement si un entier est où non un résidu quadratique modulo un nombre premier p. On peut aussi, pour simplifier les calculs (même si ce n'est en réalité pas nécessaire), utiliser le fait que -1 est un résidu quadratique modulo p si et seulement si p est congru à 1 où 2 modulo 4, autrement dit $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Exercice 4

(1) Trouver tous les nombres premiers p vérifiant la propriété suivante : pour tous entiers $a, b \in \mathbb{Z}$, si $p \mid (a^2 + b^2)$ alors $p \mid a$ et $p \mid b$.

(2) Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

Exercice 5

219 est-il un résidu quadratique modulo 383 ?

5 Ordre dans $(\mathbb{Z}/n\mathbb{Z})^*$

Passons à une étude plus poussée de l'opération la plus intéressante dans $\mathbb{Z}/n\mathbb{Z}$: la multiplication. Seulement, cette multiplication possède quelques propriétés pénibles, comme le fait que le produit de deux éléments non nuls puisse être nul, qui empêchent de dire grand chose d'intéressant. Ainsi, il est naturel de restreindre notre étude à l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, que l'on notera $(\mathbb{Z}/n\mathbb{Z})^*$. Attention ! $(\mathbb{Z}/n\mathbb{Z})^*$ n'est pas l'ensemble des éléments non nuls !

Algébriquement, cet ensemble est muni d'une opération, la multiplication, qui possède un élément neutre $\overline{1}$, et chaque élément possède un inverse. Un tel ensemble s'appelle un groupe, une structure mathématique très importante. Un autre exemple de groupe est $\mathbb{Z}/n\mathbb{Z}$ tout entier, muni de son addition. Nous prouverons plus loin que dans certains cas ces groupes ont en fait une structure très proche.

J'insiste sur ces questions de structure, car elles sont fondamentales. Selon les ensembles ou les opérations intervenant dans un problème donné, le cadre naturel dans lequel se place le problème change. Ainsi, un problème ne faisant intervenir que des multiplications modulo n « vit » dans $(\mathbb{Z}/n\mathbb{Z})^*$, et les outils que l'on peut utiliser pour aborder le problème seront ceux de la théorie des groupes, qui sont très différents de ceux de la théorie des corps par exemple.

Commençons par un rappel : la forme générale du petit théorème de Fermat.

Théorème 14. Soit a dans $(\mathbb{Z}/n\mathbb{Z})^*$. Alors $a^{\varphi} = 1$. (On rappelle que φ désigne l'indicatrice d'Euler, et que $\varphi(n)$ est le nombre d'entiers inférieurs à n et premiers avec n, qui est aussi le cardinal de $\mathbb{Z}/n\mathbb{Z}^*$, d'après notre reformulation du théorème de Bézout).

Démonstration. L'idée est d'utiliser le fait que la multiplication par a est une bijection. Appelons $x_1, x_2, \ldots, x_{\varphi(n)}$ les éléments de $(\mathbb{Z}/n\mathbb{Z})^*$: si $ax_i = ax_j$, comme a est premier avec n on peut multiplier par son inverse. On obtient $x_i = x_j$ d'où l'injectivité. De plus, $a(a^{-1}x_i) = x_i$ avec $a^{-1}x_i \in (\mathbb{Z}/n\mathbb{Z})^*$ d'où la surjectivité.

La multiplication par a est donc une bijection de $(\mathbb{Z}/n\mathbb{Z})^*$ dans lui-même donc :

$$\{x_1, x_2, \ldots, x_{\varphi(n)}\} = \{ax_1, ax_2, \ldots, ax_{\varphi(n)}\},$$

Le produit des éléments à gauche vaut $\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^*} x$ et à droite :

$$\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^*} (ax) = a^{\varphi(n)} \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^*} x$$

On obtient le résultat en simplifiant par $\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^*} x$, ce qu'on peut faire car ce nombre est inversible. □

Proposition 15. Soit x dans $(\mathbb{Z}/n\mathbb{Z})^*$. La suite $(x^k)_{k\in\mathbb{Z}}$ est périodique. Appelons $\omega(x)$ sa période. Alors $x^l = 1 \Leftrightarrow \omega(x)|l$.

Démonstration. La seule chose à prouver est la périodicité. Or la suite $(x^k)_{k\in\mathbb{N}}$ prend ses valeurs dans un ensemble fini, il existe donc par principe des tiroirs $p > q$ tels que $x^p = x^q$, et alors $x^{p-q} = 1$ (on simplifie par x^q qui est inversible), et la suite est $p - q$ périodique. □

Attention, dans cette preuve $p - q$ n'est pas nécessairement l'ordre de x. Calculer l'ordre d'un élément x n'est pas un problème facile : en général, il n'y a pas de méthode plus beaucoup plus intelligente que le calcul des puissances de x. Introduire cet ordre peut pourtant s'avérer très fructueux. Il y a un cas particulièrement agréable : si on dispose d'une relation de type $x^l = 1$: on saura alors que l'ordre divise à la fois l et $\varphi(n)$, ce qui peut permettre de le déterminer.

6 $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique

Étudier les ordres est plus agréable dans $(\mathbb{Z}/p\mathbb{Z})^*$, grâce aux bonnes propriétes des polynômes de la forme $X^k - 1$ montrées dans la troisième partie.

Définition 16. Un *générateur* de $(\mathbb{Z}/n\mathbb{Z})^*$ est un élément x de $(\mathbb{Z}/n\mathbb{Z})^*$ tel que la suite des puissances de x recouvre tout $(\mathbb{Z}/n\mathbb{Z})^*$.

Théorème 17. Pour tout p premier, $(\mathbb{Z}/p\mathbb{Z})^*$ possède un générateur. On dit aussi que $(\mathbb{Z}/p\mathbb{Z})^*$ est *cyclique*.

Pour prouver ce théorème, il faut trouver un moyen de construire des éléments d'ordre donnés. Je commence par un lemme allant dans ce sens. il est vrai de manière générale sur $(\mathbb{Z}/n\mathbb{Z})^*$, je l'énonce donc dans ce cadre.

Lemme 18. Soient a et b dans $(\mathbb{Z}/n\mathbb{Z})^*$ tels que $\omega(a) \wedge \omega(b) = 1$. Alors $\omega(ab) = \omega(a)\omega(b)$.

Démonstration. Tout d'abord, $(ab)^{\omega(a)\omega(b)} = 1$, donc $\omega(ab)|\omega(a)\omega(b)$. Pour terminer, il suffit de prouver que si k est tel que $(ab)^k = 1$, alors k est multiple de $\omega(a)$ et de $\omega(b)$. Or, si $(ab)^k = 1$, en élevant à la puissance $\omega(a)$ on trouve que $b^{k\omega(a)} = 1$, donc que $\omega(b)$ divise $k\omega(a)$, donc $\omega(b)$ divise k par lemme de Gauss. □

Lemme 19. Posons $m := \text{PPCM}((\omega(x))_{x\in(\mathbb{Z}/n\mathbb{Z})^*})$. Alors il existe dans $(\mathbb{Z}/n\mathbb{Z})^*$ un élément d'ordre m.

Démonstration. Décomposons m en facteurs premiers : $m = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$. Soit x_i un élément dont l'ordre est un multiple de $p_i^{\alpha_i}$: $\omega(x_i) = k_i p_i^{\alpha_i}$ (un tel x_i existe par définition du PPCM). Posons $y_i := x_i^{k_i}$. On vérifie que y_i est d'ordre $p_i^{\alpha_i}$ et, en utilisant de façon répétée notre lemme précédent, le produit des y_i est d'ordre m. □

Démonstration. Il est temps de finir la preuve du théorème annoncé. Appliquons donc les lemmes à $(\mathbb{Z}/p\mathbb{Z})^*$. Soit donc x un élément d'ordre m. On sait que $p - 1$ est multiple de tous les ordres des éléments de $(\mathbb{Z}/p\mathbb{Z})^*$, il est donc multiple de leur PPCM : m, et donc $m \leqslant p - 1$. Or, on sait que le polynôme $X^m - 1$ a au plus m racines, et que les $p - 1$ éléments de $\mathbb{Z}/p\mathbb{Z}^*$ sont racines de ce polynôme (car m est multiple de tous les ordres), donc on a $p - 1 \leqslant m$, puis $p - 1 = m$, et notre élément d'ordre m est notre générateur recherché. □

Que veut dire ce théorème ? Choisissons x un générateur. Alors

$$(\mathbb{Z}/p\mathbb{Z})^* = \{1, x, x^2, \dots, x^{p-2}\}.$$

La multiplication de telles puissances de x est très facile : il suffit d'ajouter les exposants modulo $p - 1$. En fait, ce choix de x permet même d'identifier $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ avec $(\mathbb{Z}/p\mathbb{Z}^*, \times)$,

via la fonction $k \mapsto x^k$. Ainsi, la structure multiplicative du groupe $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ n'est pas plus compliquée que la structure additive du groupe $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$. Attention, tout n'est pas si rose, car trouver un générateur x n'est pas facile. Toutefois, l'introduction d'un générateur peut faire des miracles dans un problème plutôt théorique. Mentionnons, enfin, qu'il existe des résultats plus généraux, plus difficiles, explicitant pour tout n la structure de $(\mathbb{Z}/n\mathbb{Z})^*$. En particulier, on a :

Théorème 20. Le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ possède un générateur si et seulement si n vaut 2, 4, p^k ou $2p^k$, où p est un nombre premier plus grand que 3.

- Quelques exercices -

Exercice 6 Combien y a-t-il de classes a modulo 343 telles que $a^{70} \equiv 1[343]$?

Exercice 7 Soit n un entier naturel. Montrer que les diviseurs premiers du $n^{\text{ième}}$ nombre de Fermat $2^{2^n} + 1$ sont tous de la forme $k \cdot 2^{n+1} + 1$.

Exercice 8 Soit p un nombre premier. Trouver tous les entiers k tels que p divise $1^k + 2^k + \ldots + (p-1)^k$.

Exercice 9 Combien y-a-t'il d'élements d'ordre k dans $(\mathbb{Z}/p\mathbb{Z})^*$?

Exercice 10 Soit p un nombre premier impair. Prouver que si q est un diviseur premier de $x^{p-1} + x^{p-2} + \cdots + 1$ alors $p = q$ ou p divise $q - 1$.

Exercice 11 Soit n divisible par deux premiers impairs distincts. Montrer que $\mathbb{Z}/n\mathbb{Z}$ n'est pas cyclique, i.e n'a pas de générateur.

Exercice 12 Trouver tous les entiers $n \geqslant 1$ impairs tels que n divise $3^n + 1$.

Exercice 13 Trouver tous les p, q premiers tels que pq divise $2^p + 2^q$.

7 Solutions des exercices

Solution de l'exercice 1 En factorisant, on obtient $(x + \overline{1})(x + \overline{2}) = 0$. Mais attention, on ne peut pas en déduire que $x = -\overline{1}$ ou $x = -\overline{2}$, car l'anneau $\mathbb{Z}/12\mathbb{Z}$ n'est pas intègre ! Dans un tel anneau, un polynôme de degré 2 peut avoir bien plus de deux racines. Il faut éviter d'essayer d'utiliser des résultats classiques sur les polynômes dans un anneau non intègre, car en général, très peu sont vrais. Ici, le seul moyen de résoudre l'équation est de tester tous les cas possibles, et de cette façon on obtient que l'ensemble des solutions est $\{\overline{2}, -\overline{5}, -\overline{2}, -\overline{1}\}$.

Solution de l'exercice 2

Si p est composé, on choisit $a \in [\![1, p-1]\!]$ divisant p. p et $(p-1)!$ ont alors a pour facteur commun, donc ne sont pas premiers entre eux. p n'est donc pas premier, sinon il diviserait $(p-1)!$ donc aussi un entier inférieur à $p - 1$.

Réciproquement, supposons p premier. Il existe alors deux méthodes pour obtenir la congruence demandée.

Première méthode. On va partitionner $(\mathbb{Z}/p\mathbb{Z})^*$ en paires d'éléments deux à deux inverses. Pour cela, il faut connaître les $x \in (\mathbb{Z}/p\mathbb{Z})^*$ qui sont leur propre inverse ; ceux-là sont racines du polynôme $X^2 - \overline{1}$, de degré 2, donc il y en a au plus deux : ce sont donc $\overline{1}$ et $-\overline{1} = \overline{p-1}$.

On regroupe les autres par paires d'inverses $\{x_i, x_i^{-1}\}$, de sorte que $\{\overline{1}\}$, $\{\overline{p-1}\}$ et les $\{x_i, x_i^{-1}\}$ forment une partition de $(\mathbb{Z}/p\mathbb{Z})^*$.

En réorganisant l'ordre des facteurs du produit, on a alors

$$\overline{(p-1)!} = \overline{1} \cdot \overline{p-1} \cdot (x_1 x_1^{-1}) \cdot ... \cdot (x_r x_r^{-1}) = \overline{p-1} = -\overline{1}.$$

Seconde méthode. Pour $p = 2$, le résultat est vrai. Supposons maintenant que $p \geqslant 3$. Considérons le polynôme $P(X) = X^{p-1} - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$. Il est unitaire et de degré $p-1$, et par le petit théorème de Fermat, tous les $p-1$ éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ en sont racines. Par la remarque précédant l'exercice, on en déduit que $P(X) = (X-\overline{1})(X-\overline{2})...(X-\overline{p-1})$. Le polynôme P étant de degré pair, son coefficient constant est produit de ses racines, autrement dit $\overline{(p-1)!} = -\overline{1}$.

<u>*Solution de l'exercice 3*</u> L'égalité de l'énoncé se réécrit $(p-1)! \cdot a = bc_1$, où $c_1 = 2 \cdot 3 \cdot ... \cdot ... \cdot (p-1) + 1 \cdot 3 \cdot ... \cdot (p-1) + ... + 1 \cdot 2 \cdot ... \cdot (p-2)$ est le coefficient du terme en X du polynôme $P(X) = (X-1)...(X-(p-1))$. Pour résoudre le problème, il suffit de montrer que $p^2 \mid c_1$, car alors comme p^2 est premier avec $(p-1)!$, on en déduit par Gauss que $p^2 \mid a$.

Si on tente d'appliquer directement une méthode simillaire à la seconde méthode du problème précédent, on obtiendra, en réduisant P modulo p que $c_1 \equiv 0 \mod p$, ce qui n'est pas suffisant pour résoudre le problème. On va en fait utiliser une autre méthode : si on note $P(X) = \sum_{k=0}^{p-1} c_k X^k$, en évaluant P en p, on obtient $(p-1)! = \sum_{k=0}^{p-1} c_k p^k$, en remarquant que $c_0 = (p-1)!$ et simplifiant par p, on obtient $\sum_{k=1}^{p-1} c_k p^{k-1} = 0$. En réduisant modulo p^2, on obtient $c_2 p + c_1 \equiv 0 \mod p^2$. Il suffit donc de montrer que c_2 est divisible par p, mais ceci est clair en réduisant P modulo p.

<u>*Solution de l'exercice 4*</u>

(1) Il est clair que cette propriété n'est pas vérifiée par 2, en prenant par exemple $a = b = 1$. Soit maintenant p un nombre premier impair. On a $(-1)^{\frac{p-1}{2}} = 1$ si $p \equiv 1 \mod 4$ et -1 si $p \equiv 3 \mod 4$, donc par le critère d'Euler, -1 est un résidu quadratique modulo p si et seulement si $p \equiv 1 \mod 4$. Ceci montre immédiatement qu'aucun nombre premier congru à 1 modulo 4 ne vérifie la propriété demandée, car un tel nombre premier divise un entier de la forme $n^2 + 1$ (prendre pour n un représentant de la classe dont le carré vaut $-\overline{1}$).

Montrons maintenant que tout nombre premier congru à 3 modulo 4 vérifie la propriété demandée. Supposons qu'il existe a, $b \in \mathbb{Z}$, avec a non divisible par p, tel que $p \mid (a^2 + b^2)$. Il est alors clair que p ne divise pas b non plus, donc $\overline{a}$ et $\overline{b}$ sont inversibles dans $\mathbb{Z}/p\mathbb{Z}$. On a alors $\overline{a}^2 = -\overline{b}^2$, donc $(\overline{a}\overline{b}^{-1})^2 = -\overline{1}$, ce qui contredit le fait que -1 ne soit pas un résidu quadratique modulo p.

(2) Supposons que l'ensemble des nombres premiers congrus à 1 modulo 4 soit fini et notons-le $\{p_1, ..., p_n\}$. Posons alors $N = (2p_1...p_n)^2 + 1$. Il est clair que ni 2 ni aucun des p_i ne divise N, donc tous ses diviseurs premiers sont congrus à 3 modulo 4. Soit p un des diviseurs premiers de N ; comme p divise $(2p_1...p_n)^2 + 1^2$, alors par la question précédente il divise 1, absurde.

Solution de l'exercice 5 Par multiplicativité du symbole de Legendre, on a $\left(\frac{219}{384}\right) = \left(\frac{3}{383}\right)\left(\frac{73}{383}\right)$. Par deux applications de la loi de réciprocité quadratique, on en déduit que $\left(\frac{219}{383}\right) = -\left(\frac{383}{3}\right)\left(\frac{383}{73}\right)$. Puis en réduisant modulo 3 et 73 respectivement, $\left(\frac{219}{383}\right) = -\left(\frac{-1}{3}\right)\left(\frac{18}{73}\right) = \left(\frac{18}{73}\right)$. Une nouvelle fois par multiplicativité, on a $\left(\frac{219}{383}\right) = \left(\frac{2}{73}\right)\left(\frac{3}{73}\right)^2 = \left(\frac{2}{73}\right)$, puis par la proposition 13, on finit par en déduire que $\left(\frac{2}{73}\right) = 1$, donc que 219 est un résidu quadratique modulo 383.

Solution de l'exercice 6 Tout d'abord, $343 = 7^3$, donc $(\mathbb{Z}/343\mathbb{Z})^*$ est cyclique, de cardinal 294 ($294 = 6 \cdot 7^2$). Soit x une racine primitive et α tel que $a = x^\alpha$:

$$a^{70} \equiv 1[343] \iff 70\alpha \equiv 0[294] \iff 21|\alpha,$$

ce qui nous donne 14 classes d'équivalences mod 294 pour α qui correspondent à 14 classes d'équivalence modulo 343 pour a.

Solution de l'exercice 7 Soit p un diviseur premier de $2^{2^n}+1$. Alors $2^{2^n} \equiv -1 \mod p$ et $2^{2^{n+1}} \equiv 1 \mod p$, donc l'ordre de 2 modulo p divise 2^{n+1} mais pas 2^n, donc c'est 2^{n+1}. Il s'ensuit que $2^{n+1} \mid (p-1)$, ce qui est le résultat voulu.

Solution de l'exercice 8 La somme des puissances k-ièmes va être difficile à manipuler telle quelle. L'idée est d'introduire un générateur x de $\mathbb{Z}/p\mathbb{Z}^*$. En effet,

$$1^k + 2^k + \ldots + (p-1)^k \equiv 1 + x^k + x^{2k} \ldots + x^{(p-2)k} [p].$$

On reconnaît la somme des termes d'une suite géométrique. Ainsi, si $(p-1)|k$, chaque terme de la somme vaut 1, et la somme vaut $p-1$ qui est non nul. Sinon, x^k est différent de 1, $x^k - 1$ est inversible, et la somme vaut $\frac{x^{(p-1)k}-1}{x^k-1}$, qui est nul par théorème de Fermat.

Solution de l'exercice 9 Soit x un générateur de $\mathbb{Z}/p\mathbb{Z}^*$ (le résultat de l'exercice implique l'existence d'un générateur, donc, à moins de vouloir tout reprouver, il faudra de toute façon utiliser ce résultat). Les éléments de $\mathbb{Z}/p\mathbb{Z}^*$ sont donc les x^k avec k entre 0 et $p-2$. Quel est l'ordre d'un tel x^k ? C'est le plus petit a tel que ak soit multiple de $p-1$, c'est donc $\frac{\mathrm{PPCM}(p-1,k)}{k}$, autrement dit $\frac{p-1}{\mathrm{PGCD}(p-1,k)}$. Soit donc d un diviseur de $p-1$. L'élément x^k est d'ordre $\frac{p-1}{d}$ si et seulement si $\mathrm{PGCD}(p-1,k) = d$, donc si k est de la forme αd avec α premier avec $\frac{p-1}{d}$. Il y a $\varphi(\frac{p-1}{d})$ tels k.

Deux remarques : la notion d'ordre fonctionne aussi dans $(\mathbb{Z}/n\mathbb{Z}, +)$, l'ordre de x étant le plus petit entier n tel que nx soit nul (où nx est défini comme valant $x + x + \ldots + x$ n fois). Un raisonnement identique montre alors que, pour d divisant n, il y a $\varphi(d)$ éléments d'ordre d (moralement, notre preuve consistait à, via le choix d'un générateur, se placer dans $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$. On en déduit en comptant selon leur ordre les éléments de $\mathbb{Z}/n\mathbb{Z}$, la très jolie, et importante, identité combinatoire suivante :

$$\varphi(n) = \Sigma_{d|n}\varphi(d).$$

Solution de l'exercice 10 Un tel diviseur q divise $x^p - 1 = (x-1)\left(x^{p-1} + x^{p-2} + ... + 1\right)$ donc l'ordre de x modulo q divise p premier. Si cet ordre est p, comme d'après le théorème de Fermat il divise également $q-1$, p divise $q-1$. Si l'ordre est 1, pour tout k, $x^k \equiv 1\,[q]$ donc la somme des p termes : $x^{p-1} + x^{p-2} + ... + 1 \equiv p\,[q]$ est divisible par q si et seulement si q divise p, soit $q = p$.

Solution de l'exercice 11 Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ la décomposition en facteurs premiers de n. Je vous laisse utiliser le théorème chinois pour montrer que pour tout a, si on note $\omega_j(a)$ l'ordre de a mod j :

$$\omega_n(a) = ppcm\left(\omega_{p_1^{\alpha_1}}(a), p_2^{\alpha_2}(a), \dots, p_k^{\alpha_k}(a)\right).$$

Comme l'ordre d'un élément mod j divise $\varphi(j)$, on a que

$$\omega_n(a) \,\Big|\, ppcm\left((p_1-1)p_1^{\alpha_1-1}, (p_2-1)p_2^{\alpha_2-1}, \dots, (p_k-1)p_k^{\alpha_k-1}\right)$$

Or on veut un élément dont l'ordre soir $\varphi(n)$, qui est le produit des termes de droite. Le $ppcm$ de ces termes est égal à leur produit ssi ils sont tous premiers entre eux deux à deux, mais il est facile de voir que si n est divisible par deux premiers impairs distincts, deux de ces termes sont pairs. Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas cyclique.

Solution de l'exercice 12 Soit $n > 1$ tel que n divise $3^n + 1$. Une autre façon de le dire est que $3^n \equiv -1\,[n]$, on est donc face à un problème purement multiplicatif. On aimerait bien utiliser le théorème de Fermat, mais il est difficile à exploiter car on contrôle mal $\varphi(n)$. Soit donc p un facteur premier de n, qui est impair. On a $3^{2n} \equiv 1\,[p]$. Soit ω l'ordre de 3 modulo p. Alors ω divise $2n$. D'autre part, d'après le petit théorème de Fermat, $3^{p-1} \equiv 1\,[p]$. Ainsi ω divise $p-1$. On en déduit que ω divise $PGCD(2n, p-1)$.

Comme on est libre de choisir le diviseur premier p de n qu'on veut, il est "assez classique" de choisir un diviseur "extrême". Si on impose donc de plus que p soit le plus petit facteur premier de n, alors nécessairement $\omega = 1$ ou 2 (car un facteur premier de $p-1$ ne peut pas diviser n par minimalité). Dans le premier cas de figure, $3 \equiv 1\,[p]$ et donc $p = 2$, ce qui est exclu. Dans le deuxième cas, $3^2 \equiv 1\,[p]$ et donc p divise 8, ce qui est exclu également. On en déduit que $n = 1$.

Solution de l'exercice 13 Remarquons tout d'abord que si $p = 2$, $2q$ divise $4 + 2^q$ si et seulement si soit $q = 2$, soit $2q$ divise 6, puisque, pour tout q impair, q divise $2^{q-1} - 1$, donc $2q$ divise $2^q - 2$. D'où les solutions : $(p,q) = (2,2), (2,3)$ ou $(3,2)$. On supposera désormais p et q impairs. Appelons ω_p et ω_q les ordres de 2 modulo p et q respectivement. Supposons que p divise $2^p + 2^q$, donc $2^{p-1} + 2^{q-1}$ (car 2 est inversible modulo p, on peut donc diviser par 2), comme p divise $2^{p-1} - 1$, p divise $2^{q-1} + 1$, donc p divise $2^{2(q-1)} - 1$. Dès lors, ω_p divise $p-1$ et $2(q-1)$ mais ne divise pas $q-1$. Appelons ν_2 la valuation 2-adique. Le fait que ω_p divise $p-1$ implique que $\nu_2(\omega_p) \leqslant \nu_2(p-1)$, et le fait que ω_p divise $q-1$ mais pas $2(q-1)$ implique que $\nu_2(\omega_p) = 1 + \nu_2(q-1)$ (pour vous en convaincre, regardez les décompositions en facteurs premiers). Or, symétriquement, on a $\nu_2(\omega_q) \leqslant \nu_2(q-1)$, et donc $\nu_2(\omega_p) = 1 + \nu_2(q-1) > \nu_2(\omega_q)$. Symétriquement, $\nu_2(\omega_q) > \nu_2(\omega_p)$, c'est absurde.