109: Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

Pierre Lissy

December 18, 2009

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

1.1 Définition.[2]

Définition-proposition 1. *Considérons l'anneau des entiers $\mathbb{Z}$. Ses seuls idéaux sont les ensembles $n\mathbb{Z}$, avec $n \in \mathbb{N}$. On peut donc s'intéresser à l'anneau quotient $\mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z} | a \in \mathbb{Z}\} = \{a + n\mathbb{Z} | a \in \{0, \dots, n-1\}\}$, ces n dernières classes étant distinctes. C'est donc un ensemble à n éléments. La classe de a modulo n sera notée $C_n(a)$.*

Remarque 1. *Cet anneau n'est pas intègre en général.*

Exemple 1. $C_6(0) = C_6(2)C_6(3)$.

1.2 Structure de groupe de $\mathbb{Z}/n\mathbb{Z}$.[1]

Proposition 1. *Soit $n \in \mathbb{N}$. Dans $\mathbb{Z}/n\mathbb{Z}$, $o(C_n(m)) = \frac{n}{n \wedge m}$. Donc $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique et ses générateurs sont les m tels que $n \wedge m = 1$.*

Définition 1. *On pose $\varphi(n)$ le nombre d'entiers naturels $k \leqslant n$ tels que $k \wedge n = 1$. C'est donc aussi le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Exemple 2. *Si p est premier, tous les éléments à part 0 sont d'ordre p. Donc $\varphi(p) = p - 1$.*

Proposition 2. *[1]Soit d un diviseur naturel de n. Alors $\mathbb{Z}/n\mathbb{Z}$ a exactement un seul sous-groupe d'ordre d, qui est $< C_n(\frac{n}{d}) >$.*

On peut calculer φ de manière récursive pas la formule suivante:

Proposition 3. $n = \sum_{d|n} \varphi(d)$.

Exemple 3. $\varphi(1) = 1$. $\varphi(2) = 2 - \varphi(1) = 1$. $\varphi(3) = 3 - \varphi(1) = 1$. $\varphi(4) = 4 - \varphi(2) - \varphi(1) = 2$. $\varphi(5) = 5 - \varphi(1) = 4$. $\varphi(6) = 6 - \varphi(1) - \varphi(2) - \varphi(3) = 3$. *Et ainsi de suite.*

1.3 Eléments inversibles.[1]

Proposition 4. *$C_n(k)$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, *) \Leftrightarrow k \wedge n = 1 \Leftrightarrow k$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$. Il y a donc exactement $\varphi(n)$ éléments inversibles.*

Remarque 2. *Pour calculer explicitement l'inverse d'un élément modulo n, on peut appliquer l'algorithme d'Euclide étendu.*

Exemple 4. *Un inverse de 47 modulo 111 est 26.*

Corollaire 1 (Théorème d'Euler)**.** *Si $x \wedge n = 1$, $x^{\varphi(n)} \equiv 1[n]$.*

Corollaire 2. *$\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow$ n est premier $\Leftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre. De plus $\mathbb{Z}/p\mathbb{Z}$ est l'unique corps (à isomorphisme près) de cardinal p.*

1.4 Nilpotents. Idempotents.

Proposition 5. *Tout élément tel que $x \wedge n = 1$ est idempotent dans $\mathbb{Z}/n\mathbb{Z}$. Les nilpotents de $\mathbb{Z}/n\mathbb{Z}$ sont les $C_n(d)$ où d est tel que tout nombre premier divisant n divise aussi d.*

2 Lemme chinois et applications.

2.1 Lemme chinois.[1]

Théorème 1. *Soient $p_1, \ldots, p_n$ des entiers premiers entre eux deux à deux. Alors en tant qu'anneaux, $\mathbb{Z}/p_1p_2 \ldots p_n \simeq \mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \ldots \times \mathbb{Z}/p_n\mathbb{Z}$. Inversément, si $\mathbb{Z}/p_1p_2 \ldots p_n \simeq \mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \ldots \times \mathbb{Z}/p_n\mathbb{Z}$ alors les nombres $p_1, \ldots, p_n$ sont premiers entre eux deux à deux.*

Exemple 5. $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Corollaire 3. *Soient $p_1, \ldots, p_n$ des entiers premiers entre eux deux à deux. Alors en tant que groupes, $(\mathbb{Z}/p_1p_2 \ldots p_n)^* \simeq (\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \ldots \times \mathbb{Z}/p_n\mathbb{Z})^*$*

2.2 Résolution de systèmes de congruences.[6]

On cherche à résoudre le système de congruence suivant:

$$\begin{cases} x \equiv a[n] \\ x \equiv b[m] \end{cases}$$

avec $n \wedge m$=1. Le lemme chinois nous assure qu'il existe une solution x_0. De plus, toutes les autres solutions du système sont alors de la forme $x_0 + nmt$ avec $t \in \mathbb{Z}$. Il reste donc à trouver une solution particulière: si u est un inverse de n modulo m (que l'on peut calculer explicitement avec l'algorithme d'Euclide étendu), on peut montrer que $a + n(b-a)u$ convient.

Exemple 6.

$$\begin{cases} x \equiv 10[47] \\ x \equiv 5[111] \end{cases}$$

Les solutions sont de la forme $4334 + 5217t$.

2.3 Calcul de $\varphi(n)$.[1]

Lemme 1. *φ est une fonction multiplicative, ie. $\forall (m,n) \in \mathbb{N}^2$, $\varphi(mn) = \varphi(n)\varphi(m)$*

Théorème 2. *Soit $n \in \mathbb{N}^*$. On décompose n en facteurs premiers: $n = \prod_i p_i^{\alpha_i}$. Alors $\varphi(n) = \prod(p_i^{\alpha_i} - p_i^{\alpha_i - 1})$.*

Exemple 7. $\varphi(21060) = \varphi(4*13*5*81) = (2^2-2)(13-1)(5-1)(3^4-3^3) = 2*12*4*54 = 5184$.

2.4 Automorphismes de $\mathbb{Z}/n\mathbb{Z}$.[1]

Théorème 3. *$Aut(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.*

Lemme 2. *Si p est un nombre premier impair et $\alpha \in \mathbb{N}^*$), on a $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z}$.*

Lemme 3. $(\mathbb{Z}/2\mathbb{Z})^* \simeq 1$. *Pour $\alpha \geqslant 2$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-1}\mathbb{Z}$.*

On en déduit par le Corollaire 3 les automorphismes de $\mathbb{Z}/n\mathbb{Z}$.

Corollaire 4. *[3] $Aut(\mathbb{Z}/n\mathbb{Z})$ (ie. $(\mathbb{Z}/n\mathbb{Z})^*$) est cyclique si et seulement si $n = 2$, $n = 4$, $n = p^\alpha$ ou $n = 2p^\alpha$ avec p premier impair et $\alpha \in \mathbb{N}$.*

3 Applications.

3.1 Critères de divisibilité[2]

Théorème 4. *Soit n un entier naturel que l'on écrit sous forme décimale $a_k a_{k-1} \dots a_0$. Alors*

1. *n est congru à a_0 modulo 2,*
2. *n est congru à $a_0 + a_1 + \dots + a_k$ modulo 3,*
3. *n est congru à a_0 modulo 5,*
4. *n est congru à $a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + \dots$ modulo 7,*
5. *n est congru à $a_0 + a_1 + \dots + a_k$ modulo 9,*
6. *n est congru à $a_0 - a_1 + \dots + (-1)^k a_k$ modulo 11„*
7. *n est congru à $a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 2a_5 + a_6 + \dots$ modulo 7,.*

3.2 Caractéristique d'un anneau. Sous-corps premier. Corps finis.[5]

Définition 2. *Soit A un anneau. Soit le morphisme d'anneaux*

$$\begin{array}{rccc} f: & \mathbb{Z} & \to & A \\ & n & \mapsto & n1_A \end{array}.$$

Alors Le noyau de f étant un idéal de $\mathbb{Z}$, on a $Im(f) \simeq \mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}$. Cet entier n est appelé la caractéristique de l'anneau A. Si $n = 0$, f est injectif, et nécessairement A est de cardinal infini (car il contient un sous-anneau isomorphe à $\mathbb{Z}$), de plus $k1_A = 0 \Leftrightarrow k = 0$. Si $n \neq 0$, le morphisme est non injectif, A contient un sous-anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et $k1_A = 0 \Leftrightarrow n|k$. Dans les deux cas, $\mathbb{Z}/n\mathbb{Z}$ est le plus petit sous-anneau inclus dans A.

Exemple 8. *La caractéristique de $M_{n,m}(\mathbb{Z}/n\mathbb{Z}) =$ est n.*

Proposition 6. *Si A est un anneau intègre, alors la caractéristique de A est 0 ou un nombre premier*

Corollaire 5. *Si k est un corps, sa caractéristique est 0 ou un nombre premier. De plus, si sa caractéristique est nulle, k contient un sous-corps isomorphe à $\mathbb{Q}$. Si sa caractéristique est un nombre premier p, k contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Dans les deux cas, ce sous-corps est le plue petit sous-corps inclus dans k. Il est appelé sous-corps premier de k.*

Théorème 5. *Soit k un corps fini de caractéristique p premier. Alors $\exists n \in \mathbb{N}^*$ tel que $|k| = p^n$.*

Remarque 3. *La notion de sous-corps premier est invariante par extension de corps: si $k \subset L$ est une extension de corps, le sosu-corps premier de L est le même que celui de k.*

3.3 Détermination de tous les groupes abéliens finis.[4]

Théorème 6. *Soit G un groupe abélien fini (de cardinal au moins 2). Alors il existe une unique suite d'entiers $\geqslant 2$ vérifiant $a_1|a_2|\dots|a_n$ tels que $G \simeq \prod_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z}$.*

Exemple 9. *Les sous-groupes de cardinal 8 sont : $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

3.4 Quelques équations diophantiennes.[2]

Définition 3. *On appelle équation diophantienne une équation de la forme $P(x,y,z)=0$ avec P un polynôme à trois variables, et (x,y,z) un triplet d'entiers.*

Théorème 7. *Pour que $(x,y,z)\in\mathbb{N}^3$ soit solution de l'équation diophantienne suivante : $x^2+y^2=z^2$, il faut et il suffit qu'il existe $d\in\mathbb{N}$ et deux entiers naturels u et v premiers entre eux tels que (x,y,z) ou (y,x,z) soit égal à $(d(u^2-v^2),2duv,d(u^2+v^2))$.*

Théorème 8. *Les équations suivantes n'ont pas de solutions non triviales (ie. avec $x=0$ ou $y=0$):*

$$x^4+y^4=z^2$$
$$x^4+y^4=z^4$$
$$x^3+y^3=z^3$$

Remarque 4. *Willes a démontré en 1995 que l'équation diophantienne $x^n+y^n=z^n$ n'a pas de solutions non triviales pour $n\geqslant 3$, ce que Fermat prétendait pouvoir prouver!*

3.5 Système de cryptage RSA.[2]

Ce système repose sur le principe suivant: Si l'on se donne un nombre N grand, (ayant par exemple une écriture décimale à 150 ou 200 chiffres), un ordinateur mettrait des dizaines d'années à calculer les facteurs premiers de N. Soit E un réseau de personnes souhaitant communiquer entre elles. Le chef du réseau choisit deux entiers premiers très grands p et q, pose $N:=pq$ et calcule $\varphi(n)=(p-1)(q-1)$. Pour chaque membre A du réseau, il choisit e_A premier avec $\varphi(N)$ et il calcule un inverse d_A de e_A modulo $\varphi(N)$. Il publie e_A et N mais garde secret $\varphi(N)$. Il communique à chaque membre du réseau son d_A que celui-ci garde secret. Pour envoyer un message, l'expéditeur A (qui souhaite communiquer avec B) code les caractères du message en nombres, puis fabrique des suites de nombres de longueur strictement inférieur à la longueur de p et q (pour assurer que ces suites de nombres soient premières à N). Soit M une telle suite. A calcule le reste X modulo N de M^{e_B} et le transmet à B. Celui-ci peut reconstituer la suite (grâce au théorème d'Euler) en calculant X^{d_B}.

3.6 Loi de réciprocité quadratique et applications

Définition 4.

3.7 Critère d'irréductibilité de polynômes.[1]

Théorème 9 (Critère d'Eisenstein)**.** *Soit $P\in\mathbb{Z}[X]$, $P=a_nX^n+\ldots+a_0$. Soit p un nombre premier. On suppose:*

1. *$p\not| a_n$,*
2. *$p|a_i$, pour $i\leqslant n-1$,*
3. *$p^2\not| a_0$.*

Alors P est irréductible sur $\mathbb{Q}$.(et donc dans $\mathbb{Z}$ pourvu que P soit primitif)

Exemple 10. *Si p est un nombre premier, $X^{p-1}+\ldots+X+1$ est irréductible sur $\mathbb{Z}$.*

Théorème 10 (réduction modulo p)**.** *Soit p un nombre premier et soit $P\in\mathbb{Z}[X]$, $P=a_nX^n+\ldots+a_0$. On pose $\bar{P}=C_p(a_n)X^n+\ldots+C_p(a_0)$. Si $\bar{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors P est irréductible dans $\mathbb{Q}[X]$ (et donc dans $\mathbb{Z}[X]$ si il est primitif).*

Exemple 11. $X^3+462X^2+2433X-67691$ *est irréductible sur $\mathbb{Z}$ (car il l'est sur $\mathbb{Z}/2\mathbb{Z}[X]$)*

Exemple 12. *Soit p un nombre premier. X^p-X-1 est irréductible sur $\mathbb{Z}$ (car il l'est sur $\mathbb{Z}/p\mathbb{Z}$).*

3.8 Tests de primalité.

Théorème 11. *Soit un entier $n \geqslant 2$ vérifiant: $\exists a \in \mathbb{Z}$ tel que $a^{(n-1)} \simeq 1[n]$ et $\forall k < n-1$, $a^k \not\simeq 1[n]$. Alors n est premier.*

Théorème 12. *Soit un entier $n \geqslant 2$ dont la décomposition en facteurs premiers est $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ vérifiant: $\forall i, \exists a_i \in \mathbb{Z}$ tel que $a_i^{(n-1)/p_i} \simeq 1[n]$ et $\forall k < n-1$, $a^k \not\simeq 1[n]$. Alors n est premier.*

Théorème 13. *Soit p un nombre premier. Soit $h \in \{1, \dots, p-1\}$. On pose $n := 1 + hp^2$ et on suppose que $2^{n-1} \simeq 1[n]$ mais $2^h \not\simeq 1[n]$. Alors n est premier.*

Ce dernier test permet d'obtenir des grands nombres premiers.

Exemple 13. *$p = 2^{127} - 1$ est premier et $h = 190$ convient, donc $1 + 190p^2$ est premier).*

Developpements : équations diophantiennes [2], automorphismes de $\mathbb{Z}/n\mathbb{Z}$ [1], tests de primalité [5]

References

[1] Perrin

[2] Combes

[3] Ortiz

[4] Querré

[5] Gourdon algèbre

[6] Itard nombres premiers