NOM : POSTIC Prénom : Mickaël.

Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications (n° 120).

Réf : Perrin, Monier, FGN Alg 1.

I. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Proposition 1. Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, où $n \in \mathbb{N}$.

Remarque 2 : Comme $(\mathbb{Z}, +)$ est abélien, les $(n\mathbb{Z}, +)$ sont des sous-groupes distingués.

Déf 3 : On définit $(\mathbb{Z}/n\mathbb{Z}, +)$ comme le quotient de $\mathbb{Z}$ par $n\mathbb{Z}$. Puisque $(n\mathbb{Z}, +)$ est un sous-groupe distingué, $(\mathbb{Z}/n\mathbb{Z}, +)$ est muni d'une structure de groupe. C'est un groupe fini à n éléments.

Ex 4 : Cas $n=1$ et $n=0$. Si $n=1$, $n\mathbb{Z} = \mathbb{Z}$ et donc $\mathbb{Z}/1\mathbb{Z} = \{0\}$. Si $n=0$, $n\mathbb{Z} = \{0\}$ et donc $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$.
Ces cas étant triviaux, on considèrera maintenant $n \geq 2$.

Prop 5 : $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique.

Corollaire 6 : On a un isomorphisme naturel entre un groupe cyclique G d'ordre n et $(\mathbb{Z}/n\mathbb{Z}, +)$: $\phi : G = \langle a \rangle \to \mathbb{Z}/n\mathbb{Z}$, $a^k \mapsto \bar{k}$.

Exemple 7 : $\phi : \mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\} \to \mathbb{Z}/n\mathbb{Z}$, $e^{i\frac{2\pi}{n}k} \mapsto \bar{k}$

Prop 8 : On a l'équivalence suivante pour $k \in \mathbb{Z}$:
$$(k \wedge n = 1) \iff (\bar{k} \text{ générateur de } (\mathbb{Z}/n\mathbb{Z}, +))$$

Déf 9 : Indicatrice d'Euler φ : $\varphi(n) = \#$ générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$
$= \# k,\ 0 \leq k < n,\ k \wedge n = 1$.

Ex 10 : $\varphi(p) = p-1$ et $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ pour $\alpha \in \mathbb{N}^*$, p premier.

2. Sous-groupes

Prop 11 : Les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont cycliques. De plus, si d divise n, il existe un unique sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ d'ordre d, donné par $\langle \frac{n}{d} \rangle$. Ce groupe est isomorphe à $\mathbb{Z}/d\mathbb{Z}$.

Exemple 12 : $\mathbb{Z}/18\mathbb{Z}$ admet 3 sous-groupes stricts non triviaux, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$.

Application 13 : $n = \# \mathbb{Z}/n\mathbb{Z} = \sum_{d|n} \varphi(d)$ (Gauss).

Application 14. Si K est un corps, alors tout sous-groupe fini de K^* est cyclique.

3. Produit direct et semi-direct.

Th 15 (Lemme Chinois)
$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z} \iff n \wedge m = 1.$$

Application 16 : • Si $n \wedge m = 1$, $\varphi(nm) = \varphi(n)\varphi(m)$
• Si $n = \prod p_i^{\alpha_i}$, $\varphi(n) = \prod \varphi(p_i^{\alpha_i}) = n \prod (1 - \frac{1}{p_i})$.

Définition 17 : L'exposant d'un groupe G est le plus petit $n \in \mathbb{N}^*$ vérifiant $g^n = 1$ $\forall g \in G$.

Remarque 18 : • L'exposant divise l'ordre du groupe par le théorème de Lagrange.
• Si le groupe est abélien, on peut trouver un élément d'ordre égal à l'exposant.

DVP 1

Lemme 19 : Pour tout groupe abélien fini G d'exposant e, tout nombre premier p divisant e est l'ordre d'un sous-groupe cyclique de G et facteur direct dans G.

Lemme 20 : Soit $n \in \mathbb{N}^*$ tout diviseur d de n, et H un sous-groupe du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$. Tout morphisme $\varphi : H \to \mathbb{Z}/d\mathbb{Z}$ s'étend en un morphisme $\varphi' : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$

Théorème 21 : Soit G un groupe abélien fini.
Il existe une unique suite $(a_1, \dots, a_s)$ d'entiers ≥ 1 tels que G soit isomorphe au produit direct

$$G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \dots \times \mathbb{Z}/a_s\mathbb{Z}$$

avec $a_s \mid a_{s-1} \mid \dots \mid a_1$.
Les a_i sont les facteurs invariants de G.

II. L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

1. Anneau et corps $\mathbb{Z}/n\mathbb{Z}$.

Prop 22 : A un anneau commutatif, $\mathcal{R}$ une relation d'équivalence sur A. On note $A/\mathcal{R}$ l'ensemble des classes d'équivalence. Alors $A/\mathcal{R}$ est un anneau ssi $(x \mathcal{R} y \iff x - y \in I)$ où I est un idéal de A. On note alors $A/\mathcal{R} = A/I$. Intègre ssi I premier. Corps commutatif ssi I maximal.

Prop 23 : Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$.
Les idéaux premiers de $\mathbb{Z}$ sont les $p\mathbb{Z}$, avec p premier ou $\{0\}$.
Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$, avec p premier.

Déf 24 : On définit $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ comme l'anneau quotient de $\mathbb{Z}$ par $n\mathbb{Z}$.

Proposition 25 : $\mathbb{Z}/p\mathbb{Z}$ corps $\iff$ p premier.

Proposition 26 : Soit $\xi \in \mathbb{Z}$. $\xi \wedge n = 1 \iff \bar{\xi}$ générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$
$\iff \bar{\xi} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Cor 27 : $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$
On retrouve p premier $\iff \mathbb{Z}/p\mathbb{Z}$ corps.

Application 28 : On a un isomorphisme $\mathrm{Aut}\, \mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/n\mathbb{Z})^\times$
et en particulier $\mathrm{Aut}\, \mathbb{Z}/n\mathbb{Z}$ groupe abélien de cardinal $\varphi(n)$.

Application 29 : Formule d'Euler.
1) Si $\xi \wedge n = 1$, $\xi^{\varphi(n)} \equiv 1 \ [n]$.
2) Pour tout $x \in \mathbb{Z}$, $x^p \equiv x \ [p]$ (p premier)
3) $p \neq 2$ est un nombre premier ssi $(p-1)! \equiv -1 \ [p]$.

Exemple 30
La différence des unités de 27^{2016} et 1

2. Théorème chinois (anneaux) et automorphismes de $\mathbb{Z}/n\mathbb{Z}$.

Théorème 31
$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \underset{\text{anneaux}}{\simeq} \mathbb{Z}/nm\mathbb{Z} \iff n \wedge m = 1$$

Prop 32 :
$$\mathrm{Aut}\, \mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{s} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$$
où $n = \prod p_i^{\alpha_i}$

Théorème 33. Cas $p=2$, $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$. $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$

$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$. $(\alpha \geq 3)$

$p \geq 3$. $\mathbb{Z}/p^\alpha\mathbb{Z} = \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z} \simeq \mathbb{Z}/p^{\alpha-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$

Conséquence 34. On a les suites exactes : pour $p=2$, $\alpha \geq 3$

$$1 \to \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \to 1$$

$p \geq 3$

$$1 \to \mathbb{Z}/p^{\alpha-1}\mathbb{Z} \to (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to \mathbb{Z}/(p-1)\mathbb{Z} \to 1$$

3. Corps fini premier.

Déf 35. Soit K un corps fini ; car K est le plus petit entier d tel que $\underbrace{1+\dots+1}_{d \text{ fois}} = 0$.

Proposition 36 Tout corps fini de card p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

III. Applications.

1) Nombres premiers

Test de Fermat 37 Soit $n \in \mathbb{N}^*$. Pour savoir s'il est premier, on prend a au hasard $\leq n$, et on regarde a^{n-1}. Si $a^{n-1} \not\equiv 1 \mod[n]$, alors n n'est pas premier. Marche en général bien, mais pour être sûr il faut le faire avec tous diviseurs de n sont les seuls à ne pas donner 1 si n nb de Carmichael.

Dirichlet faible 37 bis. Il existe une infinité de nb premiers congrus à 1 mod$[n]$ $\forall n \geq 1$.

2.) Théorème de Sylow

Proposition 38 : Soit $G = GL(n, \mathbb{Z}/p\mathbb{Z})$. G groupe fini de card $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$.

Théorème 39 : Soit G un groupe fini et p un diviseur premier de $|G|$. Alors G contient au moins un p-Sylow de card $p^{v_p(n)}$.

3.) Le théorème des 2 carrés

Déf 40. $\Sigma := \{a^2+b^2,\ a,b \in \mathbb{N}\}$.

Th 41 : $(n \in \Sigma) \iff (p=2$ ou $p \equiv 1 \mod[4])$.

Th 42 : $n = \prod_{p \in P} p^{v_p(n)}$. $n \in \Sigma \iff v_p(n)$ pair pour $p \equiv 3 \mod[4]$

4.) Le cryptage RSA.

Th 43 p, q premiers, $n = pq$, $e \wedge (p-1)(q-1) = 1$.

Si $a \wedge n = 1$, $\exists d$ tq $a^{ed} \equiv a \mod[n]$.

Application 44 : RSA.

p, q premiers, puis e premier avec $(p-1)(q-1)$. On calcule l'inverse de e mod $(p-1)(q-1) \to d$. On rend public n et e. L'expéditeur envoie $B = A^e$ (mod$[n]$). Pour avoir A, il suffit de faire B^d.