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

I) Généralités sur l'anneau $\mathbb{Z}/n\mathbb{Z}$

1) Le groupe $\mathbb{Z}/n\mathbb{Z}$

Définition 1 : Le groupe $\mathbb{Z}/n\mathbb{Z}$ est le groupe quotient de $\mathbb{Z}$ par $n\mathbb{Z}$, $n \in \mathbb{N}$.

Propriété 2 : $\mathbb{Z}/n\mathbb{Z}$ est de cardinal n.

Proposition 3 : Si un groupe G est cyclique et de cardinal n, alors il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Prop 4 : $\mathbb{Z}/n\mathbb{Z}$ possède $\varphi(n)$ générateurs ($\varphi(n) := |\{m \in \mathbb{N}^*, m \leq n, m \wedge n = 1\}|$)

Prop 5 : Si $d | n$, il existe un unique sous groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$. C'est le groupe engendré par la classe de $\frac{n}{d}$.

Exemple 6 : Les sous groupes de $\mathbb{Z}/6\mathbb{Z}$ sont $\{0\}$, $2\mathbb{Z}/6\mathbb{Z}$: $3\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$

Théorème 7 : (de structure) Soit G un groupe abélien fini. Il existe des uniques $n_r | n_{r-1} | \dots | n_1 > 1$ tels que

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$$ (les $(n_i)_i$ sont les invariants)

Corollaire 8 : Le théorème se généralise aux groupes abéliens de type fini.

Ex 9 : Puisque $600 = 2^3 \times 5^2 \times 3$, il y a 6 groupes abéliens d'ordre 600. Leurs invariants sont (600), $(5;120)$, $(2;300)$, $(10;60)$, $(2;2;150)$, $(2;10;30)$ (à isomorphisme près).

2) L'anneau $\mathbb{Z}/n\mathbb{Z}$

Déf 10 : L'anneau $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.

Ptés 11 : Si $s \in \mathbb{Z}$, alors $\bar{s}$ inversible dans $\mathbb{Z}/n\mathbb{Z}$ $\Leftrightarrow$ $s \wedge n = 1$.

Notation 12 : Le groupe multiplicatif des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté $(\mathbb{Z}/n\mathbb{Z})^*$

Pté 13 : Le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$ est $\varphi(n)$.

Pté 14 : Pour $s \in \mathbb{Z}$, $\bar{s} \in (\mathbb{Z}/n\mathbb{Z})^*$ $\Leftrightarrow$ $\bar{s}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$ $\Leftrightarrow$ $s \wedge n = 1$.

Prop 15 : $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ est intègre $\Leftrightarrow$ n premier.

Cor 16 : Pour p premier, $\varphi(p) = p - 1$.
et $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$

Prop 17 : Les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $p\mathbb{Z}/n\mathbb{Z}$, avec $p | n$ premier.

II) Théorème chinois

Déf 18 : Un morphisme d'anneaux est une application $f : A \to B$ tels que $f(1_A) = 1_B$ et est compatible avec les opérations $+$ et $\times$.

Prop 19 : (Lemme chinois) : Soient n, m premiers entre eux. Alors $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ par $f : \bar{s} \in \mathbb{Z}/nm\mathbb{Z} \mapsto (\bar{s}, \bar{s}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

Th 20 : (Théorème chinois général) :
Soient $n_1, \dots n_k \in \mathbb{N}$ premiers entre eux, $n = n_1 \dots n_k$.
Alors $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$.

Application 21: Il existe une unique solution modulo nm à $\begin{cases} x \equiv a\ [n] \\ x \equiv b\ [m] \end{cases}$ pour $n \wedge m = 1$. (se généralise à k équations)

Exemple 22: $\begin{cases} x \equiv 4\ [15] \\ x \equiv 3\ [4] \end{cases} \iff x \equiv 19\ [60]$

App 23: • Si p premier, alors $\varphi(p^k) = (p-1)p^{k-1}$,

• Si $p_1 \cdots p_r$ premiers distincts, alors $\varphi(p_1^{k_1} \cdots p_r^{k_r}) = \prod_{i=1}^{r} (p_i - 1) p_i^{k_i - 1}$.

III) Résultats arithmétiques

Th 24: (petit théorème de Fermat) Si p premier et $a \wedge p = 1$, alors $a^p \equiv a\ [p]$.

Cor 25: Ce théorème donne un test de primalité sur p : $\exists a < p,\ a^p \not\equiv a\ [p] \Rightarrow p$ non premier.
Les p rendant fausse la réciproque sont appelés nombre de Carmichaël.

Th 26: (d'Euler). On peut généraliser le petit théorème de Fermat à $n \in \mathbb{N}^*$ avec $a^{\varphi(n)} \equiv 1\ [n]$.

Ex 27: $7^4 \equiv 1\ [10]$.

Th 28: (Wilson) $p \in \mathbb{N}^*$ est premier $\iff (p-1)! \equiv -1\ [p]$

Remarque 29: Ce théorème donne un test de primalité parfait (on a une équivalence), mais qui est impraticable pour p très grand.

Th 30: (Format modulaire) Pour tout $n > 0$, il existe $N_n > 0$ tel que pour tout $p > N_n$ premier, $x^n + y^n = z^n$ admet une solution dans $\mathbb{Z}/p\mathbb{Z}$ } DEV 1

Th 31: (deux carrés) p premier impair est somme de deux carrés d'entiers ssi $p \equiv 1\ [4]$.

IV) Applications

1) Résidus quadratiques

Déf 32: Pour p premier, $a \in \mathbb{Z}$, on appelle symbole de Legendre $\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } p \mid a \\ 1 \text{ si il existe } k \in \mathbb{Z} \text{ tel que } a \equiv k^2\ [p] \\ -1 \text{ sinon} \end{cases}$

Thé 33: (critère d'Euler) : $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ [p]$ $(p \neq 2)$

Thé 34: Si $a \wedge b = 1$, $a \wedge p = b \wedge p = 1$, alors $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Ex 35: $\left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = 2^5 3^5\ [11]$
$\equiv -1\ [11]$.

Th 36: (Loi de réciprocité quadratique). Soient p, q deux entiers impairs distincts. Alors : $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$

Ex 37: $\left(\frac{20}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{13}{7}\right)(-1)^{6 \times 3} = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right)$
$= 1 \times \left(\frac{7}{3}\right) \times (-1)^3 = -\left(\frac{1}{3}\right) = -1$.

Rq 38 : La loi de réciprocité quadratique nous donne un critère pour que 3 soit un carré modulo p, qui est utile dans la prochaine partie.

2) Recherche de nombre premiers

Rq 39 : La recherche de grands nombres premiers est un prérequis de la cryptographie à clé publique. On va donc fournir une méthode pour prouver que certains grands nombres sont premier.

Def 40 : Un nombre de Mersenne est de la forme $M_n = 2^n - 1$.

Rq 41 : Si $n = ab$, $M_n = (2^a - 1)(2^{a(b-1)} + \dots + 2^a + 1)$

Donc n composé implique M_n composé.

DEV 2

Th 42 : (critère de primalité des M_q).

Soit q premier impair. Alors :

$$M_q \text{ premier} \iff (2+\sqrt{3})^{2^{q-1}} \equiv -1 \,[M_q]$$

Rq 43 : Ici, la deuxième équation se place dans $\mathbb{Z}/M_q\mathbb{Z}$ si 3 est un carré modulo M_q, $\mathbb{Z}/M_q\mathbb{Z}[X]/\langle X^2-3\rangle$ sinon.

Rq 44 : Cette méthode donne un test de primalité parfait, mais toujours de complexité qui la rend impraticable. Cependant, le test de Lehmer-Lucas, en $O(q^3)$ s'en déduit :

Th 45 : (Test de Lehmer-Lucas). Soit la suite L_n définie par : $\begin{cases} L_0 = 4 \\ L_{n+1} = L_n^2 - 2 \,[M_q] \end{cases}$. Alors M_q premier $\iff L_{q-2} \equiv 0 \,[M_q]$.

3) Cryptographie à clé publique : le système RSA.

Principe 46 :
- Soit p, q premiers distincts, $n = pq$.
- Soit e inversible modulo $\varphi(n) = (p-1)(q-1)$, d'inverse d.
- Soit $M \in \mathbb{Z}/n\mathbb{Z}$ le message à chiffrer. Alors le message chiffré est $C = M^e \,[n]$.

Prop 47 : $C^d = M^{ed} \equiv M \,[n]$

Pcipe 48 : On a donc :
- clé publique : (n, e)
- clé privée : (d)
- chiffrement : $C = M^e \,[n]$
- déchiffrement : $M = C^d \,[n]$.

Rq 49 : En pratique, p et q doivent être très grand, sinon $\varphi(n)$ puis d sont faciles à déduire de (n, e). Ils doivent de plus être aléatoires : on utilise donc une méthode de recherche de premier basée sur le test de Miller-Rabin.