Def 1: On note $n\mathbb{Z}$ l'ensemble des entiers multiples de n, avec $n \in \mathbb{N}^*$. Pour $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, on dit que a est congru à b modulo n si $a - b \in n\mathbb{Z}$. On note alors $a \equiv b \ [n]$.

Def 2: Pour $n \in \mathbb{N}^*$, on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour la relation de congruence modulo n.

I Structures de $\mathbb{Z}/n\mathbb{Z}$

1) Structure de groupe

Prop 3: Soit $n \in \mathbb{N}^*$. Alors $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. Donc $\mathbb{Z}/n\mathbb{Z}$ est muni d'une structure de groupe.

Prop 4: Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique engendré par $\overline{1}$, pour tout $n \in \mathbb{N}^*$.

Prop 5: Soit G un groupe cyclique de cardinal n. Alors $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Ex 6: Soit $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ le groupe des racines n-ièmes de l'unité. On a $U_n \simeq \mathbb{Z}/n\mathbb{Z}$.

Prop 7: Soit $n \in \mathbb{N}^*$, $m \in \mathbb{Z}$. Alors $\overline{m}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si m et n sont premiers entre eux.

Ex 8: $\overline{5}$ est un générateur de $\mathbb{Z}/6\mathbb{Z}$, mais pas $\overline{2}$.

Prop 9: Soit $n \in \mathbb{N}^*$ et d un diviseur de n. Alors il existe un unique sous-groupe d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$. Il est engendré par $\overline{\frac{n}{d}}$.

TH 10: Théorème de structure des groupes abéliens de type fini:
Tout groupe abélien G de type fini est isomorphe à un groupe de la forme:

$$\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^r$$

avec $r, k \in \mathbb{N}$, $m_1 \dots m_k \in \mathbb{N}^*$ et $\forall i \leq k-1$, $m_i \mid m_{i+1}$
les entiers $r, k, m_1 \dots m_k$ sont déterminés de manière unique par G.

2) Structure d'anneau

Prop 11: Soit $n \in \mathbb{N}^*$. Alors $n\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$. Donc $\mathbb{Z}/n\mathbb{Z}$ est muni d'une structure d'anneau.

Prop 12: Soit $n \in \mathbb{N}^*$, $m \in \mathbb{Z}$. Alors $\overline{m}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si m et n sont premiers entre eux.

Ex 13: Dans $\mathbb{Z}/10\mathbb{Z}$, $\overline{3}$ est inversible d'inverse $\overline{7}$, mais $\overline{5}$ n'est pas inversible.

Def 14: On définit l'indicatrice d'Euler, notée φ, par $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ pour $n \in \mathbb{N}^*$.

Rq 15: On a également $\varphi(n) = |\{x \in \mathbb{Z}/n\mathbb{Z} \mid \langle x \rangle = \mathbb{Z}/n\mathbb{Z}\}|$

Prop 16: Soit $n \in \mathbb{N}^*$. Alors $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Ex 17: $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z}$ sont des corps, mais pas $\mathbb{Z}/6\mathbb{Z}$.

Cor 18: Soit $p \in \mathbb{N}^*$ premier. Alors $\varphi(p) = p - 1$

Ex 19: Les premières valeurs de φ sont:
$\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$

Prop 20: Soit $n \in \mathbb{N}^*$. Alors $n = \sum_{d \mid n} \varphi(d)$.

TH 21: Soit K un corps fini. Alors $K^\times$ est cyclique.

Ex 22: Pour $p \in \mathbb{N}^*$ premier, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

Def 23: Soit A un anneau, et $f : \mathbb{Z} \to A$.
Si f est injective, on dit que A est de caractéristique nulle. Sinon, soit $n > 0$ tel que $\ker f = n\mathbb{Z}$. On dit alors que A est de caractéristique n.

Prop 24: Soit K un corps commutatif de caractéristique $p>0$. Alors $f: \begin{cases} K \to K \\ x \mapsto x^p \end{cases}$ est un morphisme de corps.

3) Théorème chinois et application.

Th 25: Soit $m, n \in \mathbb{N}^*$ premiers entre eux. Alors
$f: \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est un isomorphisme
$k \bmod mn \to (k \bmod m, k \bmod n)$
d'anneaux.

Rq 26: On peut calculer f^{-1} en utilisant une relation de Bézout entre m et n.

Cor 27: Soit $m, n \in \mathbb{N}^*$ premiers entre eux. Alors
$\varphi(mn) = \varphi(m)\varphi(n)$.
Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $p_1 \dots p_r$ premiers distincts,
$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$

II Arithmétique

1) Nombres premiers et applications en cryptographie

Th 28: Petit théorème de Fermat:
Soit $p \in \mathbb{N}^*$ premier, $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Alors $a^{p-1} = \overline{1}$.

Cex 29: La réciproque est fausse : pour $n = 561 = 3 \times 11 \times 17$, pour tout $a \in [\![1, \dots, 560]\!]$, $a^{n-1} \equiv 1 \ [\text{mod } 561]$

Th 29: Soit $p \in \mathbb{N}^*$. Alors p est premier si et seulement si $(p-1)! \equiv -1 \ [\text{mod } p]$

Rq 30: Cet algorithme demande trop de calculs pour être utilisable en pratique.

TR 31: Théorème RSA
Soit p et q deux nombres premiers. Soit $n = pq$ et e premier avec $(p-1)(q-1)$. Alors il existe $d > 0$ tel que $ed \equiv 1 \ [\text{mod } (p-1)(q-1)]$ et pour tout $a \in \mathbb{Z}$ premier avec n, $a^{ed} \equiv a \ [\text{mod } n]$.

Application 32: Chiffrement RSA.
Alice souhaite communiquer avec Bob. Bob a choisi p et q premiers, e et il a calculé d. Bob publie $n = pq$ et e.
Si Alice veut envoyer $a < n$ à Bob, elle calcule puis envoie $b = a^e$. Pour déchiffrer le message, Bob a juste à calculer b^d.
Pour un observateur extérieur qui ne connait que n, e et b, il est difficile de calculer a ! il faut qu'il trouve p et q).

2) Résidus quadratiques

Def 33: Soit p premier et $a \in \mathbb{Z}$. On définit le symbole de Legendre de a sur p comme :
$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a = 0 \\ 1 & \text{si } a \neq 0 \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z} \\ -1 & \text{si } a \neq 0 \text{ n'est pas un carré dans } \mathbb{Z}/p\mathbb{Z}. \end{cases}$

Ex 34: $\left(\frac{-1}{5}\right) = 1$, $\left(\frac{2}{5}\right) = -1$

Prop 35: Soit $p \neq 2$ premier et $n \in \mathbb{Z}$. Alors $\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \ [\text{mod } p]$

Cor 36: Soit p premier, $m, n \in \mathbb{Z}$. Alors $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$

Ex 37: $\left(\frac{1764}{1973}\right) = \left(\frac{36}{1973}\right)\left(\frac{49}{1973}\right) = 1$

Th 38: Théorème de Frobenius-Zolotarev :
Soit p premier impair, $n \in \mathbb{N}^*$ et $u \in GL(\mathbb{F}_p)$ (vu comme un élément de $\mathfrak{S}(\mathbb{F}_p^n)$). Alors $\varepsilon(u) = \left(\frac{\det u}{p}\right)$

DEV 1

Ex 39: Soit $\gamma: \begin{cases} \mathbb{F}_p \to \mathbb{F}_p \\ x \mapsto \frac{1}{m} x \end{cases}$ avec $m \in \mathbb{Z}$. Alors $\varepsilon(\gamma) = \left(\frac{m}{p}\right)$

Th 40: Loi de réciprocité quadratique :
Soit p, q premiers impairs distincts. Alors
$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

Ex 41: $\left(\frac{11}{83}\right) = -\left(\frac{83}{11}\right) = -\left(\frac{6}{11}\right) = 1$

Def 42 : Soit $q \in \mathbb{N}^*$. Le q-ième nombre de Mersenne est $M_q = 2^q - 1$.

Rq 43 : Si q n'est pas premier, alors M_q n'est pas premier.

Th 44 : Soit q premier impair tel que M_q est premier. Alors $(2+\sqrt{3})^{2^{q-1}} \equiv -1 \ [\text{mod } M_q]$.

DEV2

Rq 45 : La réciproque est vraie aussi.

Application 46 : Test de Lucas-Lehmer :
Soit $x_0 = 4$ et $\forall n \geq 0$, $x_{n+1} = x_n^2 - 2$.
Alors pour p premier impair, M_p est premier si et seulement si $x_{p-2} \equiv 0 \ [\text{mod } M_p]$

Prop 47 : Test de Pocklington-Lehmer :
Soit $n \in \mathbb{N}^*$, $F, U \in \mathbb{N}^*$ tels que $n-1 = FU$, $\text{pgcd}(F,U)=1$, et $F > \sqrt{n}$. Si pour tout diviseur premier p de F il existe $a_p \in \mathbb{Z}$ tel que $a_p^{n-1} \equiv 1 \ [\text{mod } n]$ et $\text{pgcd}(a_p^{\frac{n-1}{p}} - 1, n) = 1$, alors n est premier. Réciproquement, si n est premier, alors tout élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ vérifie ces relations.

3) Équations diophantiennes

Th 48 : Soient $m_1 \dots m_r \in \mathbb{N}^*$ premiers entre eux deux à deux. Alors le système de congruence :

$$\begin{cases} x \equiv a_1 \ [\text{mod } m_1] \\ \vdots \\ x \equiv a_r \ [\text{mod } m_r] \end{cases}$$

admet une unique solution x modulo $M = m_1 m_2 \dots m_r$ donnée par $x = a_1 M_1 y_1 + \dots + a_r M_r y_r$ où $M_i = \frac{M}{m_i}$ et $y_i M_i \equiv 1 \ [\text{mod } m_i]$

Ex 49 : Le système $\begin{cases} x \equiv 1 \ [6] \\ x \equiv 2 \ [7] \end{cases}$ a pour solution $x \equiv 37 \ [\text{mod } 42]$

Prop 50 : Soit $P \in \mathbb{Z}[X_1, \dots, X_n]$, $m \in \mathbb{N}^*$ et $\overline{P} \in (\mathbb{Z}/m\mathbb{Z})[X_1, \dots, X_n]$ le polynôme obtenu en réduisant les coefficients de P modulo m. Si $P(x_1, \dots, x_n) = 0$ n'a pas de solutions dans $(\mathbb{Z}/m\mathbb{Z})^n$, alors $P(x_1, \dots, x_n)$ n'a pas de solutions dans $\mathbb{Z}^n$.

Ex 51 : L'équation $x^3 + 5 = 153 y^3$ n'admet pas de solution entière car elle n'admet pas de solutions modulo 9.

C-ex 52 : L'équation $2y^2 = x^4 - 17$ admet des solutions modulo N pour tout $N \in \mathbb{N}^*$ mais n'admet pas de solutions rationnelles.

Références :

- Beck, Malick, Peyré, Objectif agrégation
- Cohen, A course in computational number theory
- Gourdon, Algèbre
- Hindry, Arithmétique
- Lamoitier, Arithmétique modulaire
- Saux-Picard, Rannou, Cours de calcul formel, corps finis, systèmes polynomiaux, applications.
- Ulmer, Théorie des groupes.