120

NOM : Prénom : Jury :

Algèbre ← Entourez l'épreuve → Analyse

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

Autre sujet :

[ARN] p119

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

1 Structure de groupe

DEF 1 Soit $n \in \mathbb{N}$. On dit que a et b sont congrus modulo n si $n \mid b-a$. On note $a \equiv b\ [n]$.

PROP 2 La congruence est une relation d'équivalence sur $\mathbb{Z}$. On note $\mathbb{Z}/n\mathbb{Z}$ ses classes d'équivalence et $\mathbb{Z}/n\mathbb{Z} = [\![\overline{0}; \overline{n-1}]\!]$.

Rq 3 L'addition sur $\mathbb{Z}$ est compatible avec la relation de congruence.

PROP 4 $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.

PROP 5 Tout groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. ?

PROP 6 Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$, $d \mid n$. ?

DEV 1

[ULM] p107 [CoL] p252

TH 7 Soit G un groupe abélien fini. Il existe $n_i \geq 2$, $i \in [\![1; r]\!]$ tels que $G \simeq \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$.

~~Ok est écrit~~

2 Structure d'anneaux

[ARN] p122

DEF/PROP 9 L'addition et la multiplication sur $\mathbb{Z}$ est compatible avec la relation de congruence.

On transporte la structure de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.

Ainsi $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

PROP 10 Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont ses sous-groupes additifs. ?

PROP 11 Les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $p\mathbb{Z}/n\mathbb{Z}$ avec p premier divisant n. ?

3 Éléments inversibles et fonction indicatrice d'Euler

DEF 12 $(\mathbb{Z}/n\mathbb{Z})^\times$ est le groupe multiplicatif des inversibles de $\mathbb{Z}/n\mathbb{Z}$. [ARN] p135

PROP 13 Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. $\overline{a}$ est inversible $\Leftrightarrow \operatorname{pgcd}(a, n) = 1$.

DEF 14 L'indicateur d'Euler de n, noté $\varphi(n)$, est le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$.

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

COR 16 Pour tout premier $p \geq 2$, $\varphi(p) = p-1$.

TH 17 Pour tout premier $p \geq 2$, $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})^*$ est cyclique. [PER] p74

TH 18 $\forall n \geq 2$, $n = \sum_{d \mid n} \varphi(d)$.

120

NOM : Prénom : Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi :

Autre sujet :

[DEK] 46, 111

II Théorème chinois et résolution d'équations

DEF19 Une équation diophantienne est une équation algébrique comportant une ou plusieurs inconnues et pour laquelle on cherche à connaître, s'il y en a, des solutions entières.

TH20 Soient $a,b,c \in \mathbb{Z}$. On note $d = \text{pgcd}(a,b)$.
L'équation diophantienne $ax+by=c$ possède des solutions entières ssi $d|c$. Les solutions sont alors les entiers $\left(x_0+\frac{b}{d}k, y_0-\frac{a}{d}k\right)$, $k \in \mathbb{Z}$ où (x_0,y_0) est une solution particulière

EX21 $9x+15y=33$

TH22 Soient $a,b,m \in \mathbb{Z}$. On note $d = \text{pgcd}(a,m)$.
La congruence $ax \equiv b\ [m]$ possède des solutions entières ssi $d|b$. Les solutions sont alors les entiers $x_0+\frac{m}{d}k$, $k \in \mathbb{Z}$ où x_0 est une solution particulière.

EX23 $17x \equiv 30\ [49]$

TH24 [th des restes chinois]
Soient $m_1 \dots m_n \in \mathbb{Z}$ deux à deux premiers entre eux.
Soient $a_1 \dots a_n \in \mathbb{Z}$.
Le système de congruences
"$\forall i \in [\![1;n]\!],\ x \equiv a_i\ [m_i]$"
admet une solution.
De plus toutes les solutions sont congrues modulo $m_1 \dots m_n$.

TH25 [th chinois] [PER] p25
Soient $m_1 \dots m_n \in \mathbb{Z}$ deux à deux premiers entre eux.
Alors $\mathbb{Z}/m_1 \dots m_n\mathbb{Z} \simeq (\mathbb{Z}/m_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/m_n\mathbb{Z})$.

EX26 [DEK]
$$\begin{cases} x \equiv 2\ [3] \\ x \equiv 3\ [5] \\ x \equiv 4\ [7] \end{cases}$$

APP27 ? $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/\text{pgcd}(m,n)\mathbb{Z}) \times (\mathbb{Z}/\text{ppcm}(m,n)\mathbb{Z})$

PROP28 Soient $m,n \in \mathbb{Z}$ premiers entre eux. [PER] p25
Alors $(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$

COR29 Soient $m,n \in \mathbb{Z}$ premiers entre eux. [PER] p25
Alors $\varphi(mn) = \varphi(m)\varphi(n)$.

LEM30 Soit p premier, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$

PROP31 Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.
Alors $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i-1}(p_i-1)$
$= n \prod_{i=1}^{r} \left(1-\frac{1}{p_i}\right)$.

120

NOM : Prénom : Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi :

Autre sujet :

[PER] 76

III Applications

1 Irréductibilité des polynômes

TH32 [Critère d'Eisenstein]
Soit $n \geq 2$. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$.
DEV2 Soit p premier. On suppose :
- $p \nmid a_n$
- $\forall i \in [\![0; n-1]\!]$, $p \mid a_i$
- $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{Q}[X]$.

p 77 **TH33** Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$.
Soit p premier tel que $p \nmid a_n$.
Si $\bar{P} \in (\mathbb{Z}/p\mathbb{Z})[X]$ est irréductible alors P est irréductible dans $\mathbb{Q}[X]$.

OX] 173 **EX34** $\forall n \geq 1$, $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$.

2 Applications à l'arithmétique

[DEK] ou [ARN] **TH35** [Th d'Euler]
Soient $a, n \in \mathbb{N}^*$ tels que $\text{pgcd}(a,n) = 1$.
Alors $a^{\varphi(n)} \equiv 1 [n]$.

TH36 [Th Fermat]
Soit $a \in \mathbb{N}^*$, soit $p \in \mathcal{P}$.
Alors $a^{p-1} \equiv 1 [n]$.

TH37 [Th Wilson] Soit $p > 1$.
$p \in \mathcal{P} \iff (p-1)! \equiv -1 [p]$.

PROP39 [Caractérisation des carrés] [PER]
Soit $p > 2$. $q = p^n$, $n \geq 1$.
$x \in (\mathbb{F}_q^\times)^2 \iff x^{\frac{q-1}{2}} = 1$.
Si $p = 2$, $(\mathbb{F}_q^\times)^2 = \mathbb{F}_q^*$.

DEF38 On note $\mathbb{F}_q$ le corps à $q = p^n$ éléments
On note $(\mathbb{F}_q^\times)^2 = \{x \in \mathbb{F}_q^\times / \exists y \in \mathbb{F}_q^\times, x = y^2\}$.

DEV3 **TH40** Soit $p \in \mathcal{P}$,
p est une somme de carrés ou $p \in \Sigma$
$\iff p = 2$ ou $p \equiv 1 [4]$

Refs

[ARN] ARNAUDIES, FRAYSSE, Algèbre
[COL] COLMEZ, Éléments d'analyse et d'algèbre
[ULM] ULMER, Théorie des groupes
[PER] PERRIN, Cours d'algèbre
[DEK] DE KONINCK, MERCIER, Introduction à la théorie des nombres