TD Arithmétique

Arithmétique élémentaire

TL3 **Exercice 1** 🍃 Soit $a \in \mathbb{Z}$ et $p \geq 5$ premier. 1. Montrer que $30 \mid a^5 - a$. 2. Montrer que $24 \mid p^2 - 1$.

F9I **Exercice 2** 🍃 1. Soit $n \geq 1$. Montrer que si $2^n - 1$ est un nombre premier, alors n est premier.

2. ★ Montrer que si $2^n + 1$ est un nombre premier, alors n est une puissance de 2.

P6U **Exercice 3** Montrer que pour tout $n \in \mathbb{N}$, la fraction $\frac{21n+4}{14n+3}$ est irréductible.

139 **Exercice 4** Soit $n \in \mathbb{N}^*$, on note N le nombre de ses diviseurs et P leur produit. Trouver une relation entre n, N et P.

Pgcd et Bézout

1WR **Exercice 5** 🍃🏠 Montrer que $\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{n \wedge m}$.

F6U **Exercice 6** 🍃🏠 Soient $a, b \in \mathbb{Z}$. **Indication** : *Commencer par montrer que* $(a+b) \wedge a = 1$.

1. On suppose $a \wedge b = 1$. Montrer que $(a+b) \wedge (ab) = 1$. 2. Dans le cas général, déterminer $(a+b) \wedge \mathrm{ppcm}(a,b)$.

NNG **Exercice 7** Soit $a \geq 2$, ainsi que $n \geq p$ et $n = qp + r$ la division euclidienne de n par p.

1. Montrer que si p divise $u - v$, alors $a^p - 1$ divise $a^u - a^v$.
2. Montrer que le reste de la division euclidienne de $a^n - 1$ par $a^p - 1$ est $a^r - 1$.
3. En déduire que $\mathrm{pgcd}(a^n - 1, a^p - 1) = a^{\mathrm{pgcd}(n,p)} - 1$.

71W **Exercice 8** ★ Problème de Frobénius Soit a, b deux entiers premiers entre eux ≥ 2. On considère $F = \{ax + by,\ (x,y) \in \mathbb{N}^2\}$.

1. ♣ Soit $n \geq ab$. Montrer que $n \in F$.
2. Soit $a \leq n < ab$, montrer que si $n \in F$, l'écriture $n = ax + by$, $x, y \in \mathbb{N}^2$ est unique.
3. Dénombrer l'ensemble des $(x,y) \in \mathbb{N}^2$ tels que $ax + by < ab$. **Ind** : *Pour* $n \in F$, *considérer* $ab - n$.

ODM **Exercice 9** ★ ★ Soient $a, b, c, d \in \mathbb{Z}$. Donner une CNS pour qu'il existe une infinité d'entiers naturels n tels que $an + b \wedge cn + d = 1$.

Congruence et ordre d'un élément

S97 **Exercice 10** 🍃 1. Soient $a_1, \ldots, a_n$ premiers deux à deux. On note $A = \prod a_i$, $b_i = \frac{A}{a_i}$ et $\mathcal{P}_i$ l'ensemble des div. premiers de a_i.

a) Que dire des ensembles $\mathcal{P}_1, \ldots, \mathcal{P}_n$? Que dire de l'ensemble des diviseurs premiers de b_i ?

b) Montrer que $\mathrm{pgcd}(b_1, \ldots, b_n) = 1$.

2. Soient $c_1, \ldots, c_n \in \mathbb{Z}$

a) Montrer que pour tout $i \in [\![1, n]\!]$, il existe $m_i \in \mathbb{Z}$ tel que $m_i b_i \equiv c_i [a_i]$.

b) Montrer qu'il existe $x \in \mathbb{Z}$ tel que $\forall i,\ x \equiv c_i [a_i]$.

3. Soit $k \in \mathbb{N}^*$. Montrer qu'il existe k entiers consécutifs dont aucun n'est une puissance d'un nombre premier.

LIQ **Exercice 11** Théorème de Wilson Montrer que n est premier si et seulement si $(n-1)! \equiv -1 [n]$.

QKG **Exercice 12** 🍃 Théorème de Fermat Soit p un nombre premier.

1. Pour $k \in [\![1, p-1]\!]$, montrer que p divise $\binom{p}{k}$.
2. En déduire par récurrence que pour tout $m \in \mathbb{N}^*$, $m^p \equiv m [p]$.
3. En déduire que si p ne divise pas m, on a $m^{p-1} \equiv 1 [p]$.

4SL **Exercice 13** Quel est le chiffre des unités de $2023^{2023^{2023}}$?

6P8 **Exercice 14** Soit n est premier avec 10. Montrer qu'il existe un multiple de n qui ne s'écrit qu'avec le chiffre 1.

DHP **Exercice 15** ★ [Oral X] 1. Montrer que pour n impair, n divise $\sum_{k=1}^{n-1} k^n$.

2. Trouver les entiers $n \geq 1$ pour lesquels $n \mid 1^n + 2^n + \cdots + (n-1)^n$.

Nombres premiers

8H2 **Exercice 16** 🍃 1. Montrer que si $N \equiv 3 [4]$, alors N admet un diviseur premier congru à $3 [4]$.

2. Montrer qu'il existe une infinité de nombres premiers de la forme $4n + 3$.

LG0 **Exercice 17** ♣ Théorème de Legendre

1. Soit p un nombre premier. Montrer que $v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$.
2. Déterminer le nombre de zéros à la fin de l'écriture décimale de 100!.
3. Montrer que $\frac{(2n)!(2m)!}{n!m!(n+m)!} \in \mathbb{N}$.

LJB **Exercice 18** Soit p un nombre premier impair, et $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$. On dit que $a \in \mathbb{K}$ est un carré s'il existe $x \in \mathbb{K}$ tel que $a = x^2$.

1. Déterminer les carrés de $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$.
2. Soit $a \in \mathbb{K}$ non nul. Montrer que l'équation $x^2 = a$ admet 0 ou 2 solutions. En déduire qu'il existe exactement $\frac{p-1}{2}$ carrés non nuls dans $(\mathbb{Z}/p\mathbb{Z})^*$.
3. En utilisant le théorème de Fermat, factoriser le polynôme $X^{p-1} - 1$ dans $\mathbb{K}[X]$. Montrer que si a est un carré non nul, alors a est racine de $X^{(p-1)/2} - 1$. En déduire que les carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont exactement les racines de $X^{(p-1)/2} - 1$.
4. Montrer que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si p est congru à 1 modulo 4.
5. Soit $k \geq 2$ pair. Montrer que les facteurs premiers de $k^2 + 1$ sont congrus à 1 modulo 4. En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

0CL **Exercice 19** ★ 1. Montrer que les points rationnels du cercle unité sont les $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$, pour $t \in \mathbb{Q}$, et le point $(-1, 0)$.

2. Déterminer le nombre de solutions de l'équation $x^2 + y^2 = 1$ dans $\mathbb{Z}/p\mathbb{Z}$.

P3J **Exercice 20** ★ Un classique Soit $p > 3$ premier. On écrit $1 + \frac{1}{2} + \cdots + \frac{1}{p-1} = \frac{a}{(p-1)!}$. Montrer que $p \mid a$, puis $p^2 \mid a$.

Équations diophantiennes

ZZ4 **Exercice 21** 1. Soient n, m deux entiers premiers entre eux tels que nm est un carré. Montrer que n et m sont des carrés.

2. Soit $k \geq 2$. Résoudre l'équation $x^2 + x = y^k$, d'inconnues $x, y \in \mathbb{Z}$.

297 **Exercice 22** Résoudre $2^m - 3^n = 1$. **Ind** : *Commencer par étudier la relation modulo* 8.

Fonctions arithmétiques

FQG **Exercice 23** ♣ Fonction indicatrice d'Euler Pour $n \geq 1$ on note $\varphi(n)$ le nombre d'entiers de $[\![1, n]\!]$ premiers avec n.

1. Déterminer $\varphi(p)$ pour p premier, puis $\varphi(p^\alpha)$.
2. Montrer que si n, m sont premiers entre eux, $\varphi(nm) = \varphi(n)\varphi(m)$.
3. En déduire une expression de $\varphi(n)$ en fonction de sa décomposition en facteurs premiers.
4. Montrer que $\sum_{d|n} \varphi(d) = n$. **Indication** : *Réduire les n fractions $\frac{i}{n}$, pour $i \in [\![1, n]\!]$ sous forme irréductible.*

XTT **Exercice 24** Inversion de Möbius On munit $\mathcal{F}(\mathbb{N}^*, \mathbb{C})$ de l'addition usuelle et du produit $f \star g \colon n \mapsto \sum_{d|n} f(d)g(\frac{n}{d})$.

1. Montrer que cela en fait un anneau commutatif. En caractériser les éléments inversibles.
2. Soit μ la fonction associant 0 aux multiples de carrés et $(-1)^r$ à tout entier qui s'écrit $p_1 \dots p_r$, où les p_i sont premiers distincts. Calculer $\mu \star (n \mapsto 1)$ et en déduire que si $f(n) = \sum_{d|n} g(d)$, alors $g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$.

UCT **Exercice 25** Une fonction $f \colon \mathbb{N} \to \mathbb{R}$ est dite multiplicative si pour tous m, n premiers entre eux, $f(mn) = f(m)f(n)$.

1. Montrer que f est multiplicative si et seulement si $m \mapsto g(m) = \sum_{d|m} f(d)$ est multiplicative.
2. En déduire que les fonctions indicatrice d'Euler, somme des diviseurs et nombre de diviseurs sont multiplicatives.

72H **Exercice 26** ★ Théorème d'Erdös Soit $f \colon \mathbb{N}^* \to \mathbb{N}^*$ multiplicative strictement croissante.

1. Montrer que pour p premier et $n \in \mathbb{N}$, $f(p^n) = f(p)^n$.
2. En déduire qu'il existe $\alpha \in \mathbb{R}$ tel que $f(n) = n^\alpha$.
3. Montrer que α est entier.

Polynômes et arithmétique sur $\mathbb{Z}$

6P1 **Exercice 27**

1. Soit $P = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X]$ de degré n, et $r = \frac{p}{q}$ une racine rationnelle de P, avec $p \wedge q = 1$. Montrer que $p \mid a_0$ et $q \mid a_n$.
2. On suppose que P est unitaire. Montrer que ses racines rationnelles sont entières.
3. Montrer que $P = 1 - 2X - X^2 + X^3$ est scindé sur $\mathbb{R}[X]$ mais irréductible sur $\mathbb{Q}[X]$.

WTG **Exercice 28** Soit P un polynôme à coefficients entiers non constant, montrer que l'ensemble des nombres premiers p qui divisent un des $P(n)$, $n \in \mathbb{N}$ est infini.

ETE **Exercice 29** 1. Pour $n \in \mathbb{N}$, montrer qu'il existe un polynôme $P_n \in \mathbb{Z}[X]$ unitaire tel que $\forall \theta \in \mathbb{R},\ P_n(2\cos\theta) = 2\cos(n\theta)$.

2. ★ Déterminer dans $\mathbb{C}$ toutes les racines de l'unité qui sont à coordonnées rationnelles.

DDN **Exercice 30** ★ Soit $n \geq 2$ et $a_1, \dots, a_n$ des éléments de $\mathbb{Z}$ deux à deux distincts. Montrer que $P = (X - a_1) \dots (X - a_n) - 1$ est irréductible dans $\mathbb{Z}[X]$.

Arithmétique des polynômes

FDL **Exercice 31** Pour $n \geq 2$, montrer que $X^n - X + 1$ est scindé à racines simples dans $\mathbb{C}[X]$.

LQM **Exercice 32** Soient A, B deux polynômes de $\mathbb{K}[X]$ non constants et premiers entre eux.

1. On considère (U_0, V_0) tels que $AU_0 + BV_0 = 1$. Montrer que (U, V) est un couple de Bezout de (A, B) si et seulement s'il existe $Q \in \mathbb{K}[X]$ tel que $(U, V) = (U_0 - BQ, V_0 + AQ)$.
2. Montrer que (A, B) admet un unique couple de Bezout (U, V) tel que $\deg U < \deg B$ et $\deg V < \deg A$.

M3H **Exercice 33** Soit $P \in \mathbb{C}[X]$. On note $D = \operatorname{pgcd}(P, P')$.

1. Exprimer $\deg D$ en fonction de $n = \deg P$ et du nombre r de racines distinctes de P.
2. En déduire quels sont les polynômes unitaires $P \in \mathbb{C}[X]$ tels que $P' \mid P$.

K6U **Exercice 34** Soient $A, B, P \in \mathbb{Z}[X]$.

1. Pour $a, b \in \mathbb{Z}$ mq $a - b \mid P(a) - P(b)$. 2. Mq $A - B$ divise $P \circ A - P \circ B$. 3. Montrer que $P - X$ divise $P \circ P - X$.

KBH **Exercice 35** Polynôme minimal Soit $\theta \in \mathbb{C}$ racine d'un polynôme $P \in \mathbb{Q}[X]$.

1. Montrer qu'il existe un polynôme $P_{min} \in \mathbb{Q}[X]$ unitaire de degré minimal dont θ est racine. Montrer que $P_{\min}$ est irréductible dans $\mathbb{Q}[X]$ et scindé à racines simples sur $\mathbb{C}$.
2. Soit $P \in \mathbb{Q}[X]$ de degré 5 qui admet une racine multiple dans $\mathbb{C}$. Montrer que P admet une racine dans $\mathbb{Q}$.