MP*2 LLG
2024/2025

Arithmétique de $\mathbb{Z}$

Exercices de révisions pour s'entraîner

Exercice 1 Démontrer que pour tout entier $n \in \mathbb{N}^*$, $3^{2n} - 2^n$ est divisible par 7, $2^{4^n} + 5$ est divisible par 21, $3^{2n} + 2^{6n-5}$ est divisible par 11.

Exercice 2 *(CCP)* Résoudre : $\begin{cases} x \equiv 2[3] \\ x \equiv 3[5] \end{cases}$, $\begin{cases} x \equiv 6[17] \\ x \equiv 4[15] \end{cases}$ et $\begin{cases} x \equiv 2[11] \\ x \equiv 7[13] \end{cases}$ et $\begin{cases} x \equiv 2[11] \\ x \equiv 7[13] \end{cases}$.

Exercice 3

1. Déterminer l'ensemble des entiers naturels p, tels que les trois nombres p, $p+2$, $p+4$, soient des nombres premiers.
2. Déterminer l'ensemble des entiers naturels premiers qui sont à la fois somme et différence de deux entiers naturels premiers.

Exercice 4 *(CCP)* Résoudre dans $\mathbb{Z}$: $2x + 3y = 1$; $14x - 18y = 2$. Quelles sont les solutions de cette deuxième dans $\mathbb{N}$?

Exercice 5 *(TPE)* Montrer : $\forall (a, b) \in \mathbb{Z}^2$, $\forall n \in \mathbb{N}$, $a \equiv b[n] \Rightarrow a^n \equiv b^n[n^2]$.

Exercice 6 *(Mines)* Montrer que l'ensemble des nombres premiers est infini. Montrer que l'ensemble des nombres premiers congrus à -1 modulo 4 est infini.

Exercice 7 Montrer qu'il existe des intervalles de $\mathbb{N}$ aussi longs que l'on veut qui ne contiennent aucun nombre premier.

Exercice 8 *(Mines)* Résoudre dans $\mathbb{Z}$ la congruence $9x \equiv 6$ [24].

Exercice 9 Soient $a \geq 2$ et $r \geq 2$ des entiers. Montrer que si $(a^r - 1)$ est premier alors $a = 2$ et r est premier.
Montrer que si $a^n + 1$ est premier, avec $n \geq 1$ et $a \geq 2$, alors a est pair et n est une puissance de 2.

Exercice 10 Pour tout $n \in \mathbb{N}$, on pose $M_n = 2^n - 1$. (M_n est appelé nombre de Mersenne).

1. Montrer que si $n \geq 2$, et si M_n est premier, alors n est premier.
2. Etudier la réciproque de cette propriété.

Exercice 11 *(TPE)* Déterminer les nombres premiers tels que p divise $2^p + 1$.

Exercice 12 *(Mines)* Déterminer l'ensemble des entiers relatifs n tels que $n^{13} \equiv n$ modulo 42.

Exercices à corriger

Exercice 13 * Soit p un nombre premier. Pour tout $n \in \mathbb{N}^*$, notons $v_p(n!)$ l'exposant de p dans la décomposition en facteurs premiers de $n!$. Montrer que $v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$.
En déduire le nombre de zéros à la fin de l'écriture décimale de 2025!

Exercice 14 *(Mines-X)** Pour tout $n \in \mathbb{N}$, on note $F_n = 2^{2^n} + 1$.

1. Montrer que, pour tout $k \in \mathbb{N}^*$: $(F_n - 1)^{2^k} + 1 = F_{n+k}$.
2. Montrer qu'il existe $q \in \mathbb{N}$ tel que $F_{n+k} = qF_n + 2$.
3. En déduire que pour $n \neq m$, F_n et F_m sont premiers entre eux.
4. Soit p un diviseur premier de F_k. Montrer que p est premier avec 2. Trouver l'ordre de 2 dans le groupe $(\mathbb{Z}/p\mathbb{Z})^*$.
5. Soit $t \in [\![1, k+1]\!]$. Quelle est la classe de p modulo 2^t ?
6. Montrer que pour tout $t \in \mathbb{N}^*$, il existe une infinité de nombres premiers congrus à 1 modulo 2^t.

Exercice 15 *(Mines)* Montrer que 2021 a un multiple dont tous les chiffres en base 10 valent 1.

Exercice 16 *(X)* Quel est le chiffre des unités de $23^{23^{23^{23}}}$?

Exercice 17 *(Mines)* Quel est le chiffre des unités de $2022^{2022^{2022}}$?

Exercice 18 *(Mines)* Trouver tous les entiers naturels $n \geq 2$ tels que $\phi(n)$ divise n (ϕ représente l'indicatrice d'Euler).

Exercice 19 *(Centrale)** Soient $a \geq 2$, n et $m \geq 1$ des entiers.

1. Rappeler la définition du pgcd et la méthode de calcul par l'algorithme d'Euclide.
2. Montrer que si $m|n$ alors $(a^m - 1)|(a^n - 1)$.
3. Montrer que $(a^m - 1) \wedge (a^n - 1) = (a^{m \wedge n} - 1)$

Exercice 20 *(Mines)* * Soit $(a, b) \in (\mathbb{N}^*)^2$. Montrer que a et b sont premiers entre eux si et seulement si tout entier supérieur ou égal à $(a-1)(b-1)$ est de la forme $au + bv$ pour un couple $(u, v) \in \mathbb{N}^2$.

Exercice 21 *(X)** Soit A une partie de $\mathbb{N}$ contenant 0, non réduite à 0 et stable par somme. On note $d = \mathrm{pgcd}(A)$.

1. Montrer que $\{x - y,\ (x, y) \in A^2\} = d\mathbb{Z}$.
2. On suppose que $d = 1$. Montrer que $\mathbb{N} \setminus A$ est fini.
3. Soient a et b deux entiers naturels premiers entre eux. Quel est le plus grand entier n'appartenant pas à $a\mathbb{N} + b\mathbb{N}$.

Exercice 22 *(X)* Soit $a \in \mathbb{Z}$ impair. Existe-t-il $f : \mathbb{Z} \to \mathbb{Z}$ telle que, pour tout $n \in \mathbb{Z}$, $f \circ f(n) = n + a$?

Exercice 23 *(ENS)** Si $n \in \mathbb{N}^*$, soit $\sigma(n)$ la somme des diviseurs de n dans $\mathbb{N}^*$. On dit qu'un élément $P \in \mathbb{N}^*$ est parfait si $\sigma(P) = 2P$.

1. Soit $p \in \mathbb{N}^*$ tel que $2^p - 1$ est premier. Montrer que p est premier.
2. Montrer que, si p est un élément de $\mathbb{N}^*$ tel que $2^p - 1$ est premier, alors $2^{p-1}\,(2^p - 1)$ est parfait.
   On admet dans la suite que tout nombre parfait pair est de la forme précédente. On considère un nombre parfait pair, que l'on écrit donc sous la forme $P = 2^{p-1}\,(2^p - 1)$ où $p \in \mathbb{N}^*$ est tel que $2^p - 1$ est premier. Dans les questions (3), (4) et (5), on suppose $p \neq 2$.
3. Déterminer la classe de P modulo 12.
4. Montrer que $P - 1$ et $P + 1$ ne sont pas des carrés.
5. En considérant la classe de $P - 1$ modulo 4 et celle de $P + 1$ modulo 3, montrer que $P - 1$ et $P + 1$ ne sont pas parfaits.
6. Montrer qu'il n'existe pas de couple de nombres parfaits consécutifs.
7. Prouver le résultat admis.

Exercice 24 *(Mines-Ponts)**

1. Calculer l'intégrale $\displaystyle\int_0^1 t^p(1-t)^q \,\mathrm{d}t$ (avec $(p, q) \in \mathbb{N}^2$) de deux manières différentes.
2. En déduire que pour tout $(a, b) \in \mathbb{N}^* \times \mathbb{N}$, $a\dbinom{a+b}{a}$ divise $ppcm(b + 1, \ldots, b + a)$.

Exercice 25 *(ENS)** Quels sont les éléments n de $\mathbb{N}^*$ tels que $\sqrt{n} \in \mathbb{Q}$?

Exercice 26 *(Lyon)* Soit φ l'indicatrice d'Euler.

1. Montrer que $\forall n \in \mathbb{N}^*$, $\varphi(n) \geq \dfrac{\sqrt{n}}{2}$.
2. Existe-t-il $C \in \mathbb{R}^{+*}$ tel que $\forall n \in \mathbb{N}^*, \varphi(n) \geq Cn$?

Exercice 27 *(ENS Lyon)* On munit $E = \mathbb{Z}^{\mathbb{N}}$ de sa structure de groupe additif : $a + b = (a_n + b_n)_{n \in \mathbb{N}}$. On note E^* l'ensemble des morphismes de groupes de E dans $\mathbb{Z}$. On note $(e_k) = (\delta_{k,n})_{n \in \mathbb{N}}$. Montrer que si un élément f de E^* s'annule en chaque e_k alors f est nulle. *Indication :* On pourra considérer des suites du type $(p^n a_n)_n$.

Exercice 28 *(X)* Soient a et b dans $\mathbb{N}^*$, $(x_n)_{n \in \mathbb{Z}}$ et $(y_n)_{n \in \mathbb{Z}}$ deux suites à valeurs dans un ensemble E, respectivement a-périodique et b-périodique. On suppose qu'il existe $a + b - a \wedge b$ entiers relatifs consécutifs tels que $x_n = y_n$. Montrer que $(x_n)_{n \in \mathbb{Z}} = (y_n)_{n \in \mathbb{Z}}$.

Exercice 29 *(X)** Pour $n \in \mathbb{N}^*$, on note $C_n = \{(x, y) \in (\mathbb{Q}^*)^2, x^2 + y^2 = n\}$.

1. Montrer que C_1 est non vide.
2. Montrer que C_7 est vide.
3. Soit $n \in \mathbb{N}^*$. On suppose que C_n est non vide. Montrer que C_n est infini.

Exercice 30 *(X)* * Soient $x,\ y,\ z \in (\mathbb{N}^*)^3$ tels que : $x^2 + y^2 = z^2$ et $\mathrm{PGCD}(x,\ y,\ z) = 1$.

1. Montrer qu'il existe $n > m$ entiers premiers entre eux tels que, à permutation près de x et y, on ait : $x = 2nm$, $y = n^2 - m^2$, $z = n^2 + m^2$.

2. En déduire que l'aire du triangle de côté x, y et z n'est pas le carré d'un entier.

Exercice 31 *(Lyon)**

1. Soit α un nombre réel irrationnel. Montrer que, pour tout $n \in \mathbb{N}^*$, il existe (p, q) de $\mathbb{Z} \times [\![1, n]\!]$ tel que $\left|\alpha - \frac{p}{q}\right| < \frac{1}{qn}$.
2. Soit $d \in \mathbb{N}^*$. On suppose que d n'est pas un carré parfait.
   Montrer que l'équation $a^2 - db^2 = 1$ possède une solution $(a, b) \in \mathbb{Z}^2$ telle que $b \neq 0$.

Exercice 32 *(X)**

1. Montrer que l'équation $a^2 - 2b^2 = 1$ admet une infinité de solutions $(a, b) \in \mathbb{N}^2$. Déterminer l'ensemble des solutions.
2. Que dire de l'ensemble des solutions de $a^2 - 2b^2 = -1$?

Exercice 33 *(X)** Soit $x \in \mathbb{R} \setminus \mathbb{Q}$. Montrer qu'il existe une suite de rationnels $(r_n)_{n \in \mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ telle que : pour tout $n \in \mathbb{N}$, $r_n = \frac{p_n}{q_n}$ avec $p_n \wedge q_n = 1$, $\left|x - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n^2}$ et $\lim_{n\to\infty} q_n = +\infty$.

Exercice 34 *(Lyon)* Montrer que, si m et n sont dans $\mathbb{N}^*$, n divise $\displaystyle\sum_{k=1}^{n} m^{k\wedge n}$.

Exercice 35 *(Paris)* Soient $m, M, r \in \mathbb{N}$, avec $r \geq 3$, $k_0, \ldots, k_M \in \mathbb{Z}$ tels que $\displaystyle\sum_{i=0}^{M} k_i r^i = \sum_{i=0}^{m} r^i$. Montrer que $\displaystyle\sum_{i=0}^{M} |k_i| \geq m + 1$.

Exercice 36 *(X)* Soit p un nombre premier congru à 1 modulo 4. On considère l'ensemble

$$S = \left\{(a, b, c) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{Z}^*,\ 4ab + c^2 = p\right\}.$$

1. Montrer que S est fini non vide.
   Soient $S_1 = \{(a, b, c) \in S,\ a > b + c\}$ et $S_2 = \{(a, b, c) \in S,\ a < b + c\}$.
2. Montrer que S est l'union disjointe de S_1 et S_2. Montrer que S_1 et S_2 ont le même cardinal.
3. Soit $g : S_1 \to S_1$ définie par $g(a, b, c) = (a - b - c, b, -2b - c)$. À l'aide de g, montrer S_1 a un cardinal impair.
4. Soit $S_0 = \{(a, b, c) \in S,\ a \neq b\}$. À l'aide de S_0, montrer que p est somme de deux carrés.
5. Montrer qu'un nombre premier impair s'écrivant comme la somme de deux carrés est congru à 1 modulo 4
6. Montrer qu'un entier naturel non nul dont tous les diviseurs premiers sont congrus à 1 modulo 4 est somme de deux carrés d'entiers.

Exercice 37 *(Paris)* Pour $n \in \mathbb{N}^*$, $g(n)$ désigne le nombre de diviseurs premiers de n comptés avec multiplicité ; par exemple, $g(5^2) = 2$. Calculer, pour $n \in \mathbb{N}^*$, $\displaystyle\sum_{d|n} (-1)^{g(d)}$.

Exercice 38 *(X)* On définit v_2 la valuation 2-adique sur $\mathbb{Q}$ et on admet que pour tout $(x, y) \in \mathbb{Q}^2$:

— $v_2(xy) = v_2(x) + v_2(y)$

— $v_2(x + y) \geq \min(v_2(x), v_2(y)$ avec égalité si et seulement si $v_2(x) \neq v_2(y)$.

1. Montrer que pour $n \geq 2$, $H_n \notin \mathbb{N}$.
2. Montrer que pour $m \leq n - 2$, $H_n - H_m \notin \mathbb{N}$.

Exercice 39 *(SR)* Si $n \in \mathbb{N}^*$, soit $H_n = \displaystyle\sum_{k=1}^{n} \frac{1}{k}$. Si p est un nombre premier et si $r \in \mathbb{Q}^*$ s'écrit $\frac{a}{b}$ où a et b sont deux entiers premiers entre eux, on définit la p-valuation $v_p(r)$ de r comme la p-valuation de a.

1. Montrer que, si $p \geq 3$ est un nombre premier, $v_p(H_{p-1}) \geq 1$.
2. Montrer que, si $p \geq 5$ est un nombre premier, $v_p(H_{p-1}) \geq 2$.
3. Montrer que, si $p \geq 5$ est un nombre premier, $v_p(H_{(p-1)p}) \geq 1$.

Exercice 40 *(SR)**

1. On note φ la fonction indicatrice d'Euler. Redémontrer que $\varphi(mn) = \varphi(m)\varphi(n)$ pour tous m, n dans $\mathbb{N}^*$ premiers entre eux (on dit que φ est arithmétiquement multiplicative), redonner la formule explicite pour $\varphi(n)$, et enfin calculer $\displaystyle\sum_{d|n} \varphi(d)$ pour tout $n \geq 1$.

2. Soit m, n dans $\mathbb{N}^*$. Exprimer $\varphi(mn)$ en fonction de $\varphi(m)$, $\varphi(n)$, $\varphi(m \wedge n)$ et $m \wedge n$.
3. Pour $n \in \mathbb{N}^*$, on note d_n le nombre de diviseurs premiers de n, puis $\mu(n) := (-1)^{d_n}$ si n n'est pas divisible par le carré d'un nombre premier, et enfin $\mu(n) := 0$ dans le cas contraire. Montrer que μ est arithmétiquement multiplicative, et calculer $\sum_{d|n} \frac{\mu(d)}{d}$ pour tout $n \in \mathbb{N}^*$.

Exercice 41 *(SR)* Si $n \in \mathbb{N}^*$, soit $H_n = \sum_{k=1}^{n} \frac{1}{k}$. Si p est un nombre premier et si $r \in \mathbb{Q}^*$ s'écrit $\frac{a}{b}$ où a et b sont deux entiers premiers entre eux, on définit la p-valuation $v_p(r)$ par $v_p(r) = v_p(a) - v_p(b)$. Si $n \in \mathbb{N}^*$, calculer $v_2(H_n)$.

Exercice 42 *(ENS)*

1. Calculer $\sum_{d|n} \varphi(d)$ où φ est l'indicatrice d'Euler.
2. Calculer $\sum_{d|n} \mu(d)$ où μ est la fonction de Möbius définie par $\mu(1) = 1$, $\mu(p) = -1$, $\mu(p^k) = 0$ pour $k \geq 2$ si p est un nombre premier et $\mu(nm) = \mu(n)\,\mu(m)$ si $n \wedge m = 1$. On pose
$$F : x \in \mathbb{R}^+ \mapsto \left| \left\{ \frac{p}{q} \in [0,1] \ ; \ q \leq x \right\} \right|.$$
3. Montrer que $F(x) \underset{x \to +\infty}{=} \frac{3}{\pi^2} x^2 + O(x \ln x)$.