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.

Exercice 13 (Mines) Soit $n \in \mathbb{N} \setminus \{0, 1\}$. Calculer $S_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} (-3)^k$ et $T_n = \sum_{k=0}^{\lfloor \frac{n}{3} \rfloor} \binom{n}{3k}$.

Exercices à corriger

Exercice 14 (Mines) * Soient $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \mathbb{R}^n$. Montrer que l'application définie sur l'ensemble des permutations de $\llbracket 1, n \rrbracket$ par $f(\sigma) = \sum_{i=1}^n a_i b_{\sigma(i)}$ admet un minimum et un maximum à expliciter.

Exercice 15 ***(Toutes) 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 16 (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 $t \in \llbracket 1, k+1 \rrbracket$. 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 17 (*Mines*) Montrer que 2021 a un multiple dont tous les chiffres en base 10 valent 1.

Exercice 18 (*X*) Quel est le chiffre des unités de $23^{23^{23}}$?

Exercice 19 (*Mines*) Quel est le chiffre des unités de $2022^{2022^{2022}}$?

Exercice 20 (*Mines*) Trouver tous les entiers naturels $n \geq 2$ tels que $\phi(n)$ divise n (ϕ représente l'indicatrice d'Euler).

Exercice 21 (*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 22 (*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 23 (*X*)* Soit A une partie de $\mathbb{N}$ contenant 0, non réduite à 0 et stable par somme. On note $d = \text{pgcd}(A)$.

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

Exercice 25 (*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 26 (*Mines-Ponts*)*

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

Exercice 27 (*ENS*)* Quels sont les éléments n de $\mathbb{N}^*$ tels que $\sqrt{n} \in \mathbb{Q}$?

Exercice 28 (*Lyon*) Soit φ l'indicatrice d'Euler.

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

Exercice 29 (*Mines*) On note φ la fonction indicatrice d'Euler.

1. Calculer $\varphi(7)$ et $\varphi(37044)$.
2. Montrer que : $\forall n \in \mathbb{N}^*, \varphi(n) \geq \frac{n \ln 2}{\ln n + \ln 2}$.

Exercice 30 (*Lyon-X*) Soit ϕ un morphisme de groupes de $\mathbb{Z}^{\mathbb{N}}$ dans $\mathbb{Z}$ (pour la structure de groupes additifs). On suppose qu'il s'annule sur l'ensemble $\mathbb{Z}^{(\mathbb{N})}$ des suites presque nulles. Montrer ϕ est nul. *Indication* : On pourra considérer des suites du type $(p^n a_n)_n$.

Exercice 31 (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 32 (X)* Soient $x, y, z \in (\mathbb{N}^*)^3$ tels que : $x^2 + y^2 = z^2$ et $\text{PGCD}(x, y, z) = 1$.

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

Exercice 34 (**PLSR**)

1. Montrer qu'il existe une infinité de nombres premiers p tels que $p \equiv 3 [4]$.
2. Soient p un nombre premier et $n \geq 2$. Soit $k = \frac{(np)^p - 1}{np - 1}$.
 - (a) Montrer que $k \equiv 1 [p]$.
 - (b) Soit $d \in \mathbb{N}^*$. Montrer que si d divise k alors $d \equiv 1 [p]$.
3. Soit p un nombre premier. Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo p .

Exercice 35 (*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 $n \in \mathbb{N}^*$, $\sum_{d|n} (-1)^{g(d)}$.

Exercice 36 (*SR*)* 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 37 (*Lyon*) Déterminer la somme des racines primitives n -ièmes de l'unité.

Exercice 38 (*PLSR-SR*)* On étend de façon naturelle la valuation 2-adique v_2 à $\mathbb{Q}^*$. Si $n \in \mathbb{N}^*$, soit $H_n = \sum_{k=1}^n \frac{1}{k}$. Calculer $v_2(H_n)$.

Exercice 39 (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 40 (X)

Soit $p \geq 3$ un nombre premier. On définit l'application v de $\mathbb{Q}$ dans $\mathbb{Z} \cup \{+\infty\}$ en posant $v(0) = +\infty$ et, si $(a, b, k) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$ vérifie $a \wedge b = ab \wedge p = 1$, $v\left(p^k \frac{a}{b}\right) = k$.

1. Pour $(x, y) \in \mathbb{Q}^2$, montrer que $v(xy) = v(x) + v(y)$, $v(x + y) \geq \min(v(x), v(y))$.
2. Pour $n \in \mathbb{N}^*$, montrer que $v(n!) < \frac{n}{p-1}$.
3. Soit $P = \sum_{k \in \mathbb{N}} a_k X^k \in \mathbb{Q}[X]$. Pour $i \in \mathbb{N}$, soit $v^{(i)}(P) = \min\{v(a_j) ; j \in \mathbb{N}, j \geq i\}$. On fixe $m \in \mathbb{N}$, $R = (X - m)P$. Montrer que $\forall i \in \mathbb{N}$, $v^{(i+1)}(R) \geq v^{(i)}(P)$.
4. Soient $(d_n)_{n \in \mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$ et, pour $n \in \mathbb{N}$, $b_n = \sum_{k=0}^n \binom{n}{k} d_k p^k$. Montrer que, si la suite $(b_n)_{n \in \mathbb{N}}$ s'annule une infinité de fois, elle est identiquement nulle.

Exercice 41 (*Lyon*) Pour $n \in \mathbb{N}^*$, on note d_n le nombre de diviseurs de n . Montrer que pour tout $\epsilon > 0$, $d_n = O(n^\epsilon)$.

Exercice 42 (PLSR)

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 $F(x) \underset{x \rightarrow +\infty}{=} \frac{3}{\pi^2} x^2 + O(x \ln x)$.

Exercice 43 (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 $\lim_{n \rightarrow \infty} q_n = +\infty$.

Exercice 44 (X)* Pour quelles valeurs de $n \in \mathbb{N}^*$, $\cos\left(\frac{2\pi}{n}\right)$ est-il rationnel?