Arithmétique

1. Résoudre dans $\mathbf{Z}$ l'équation $x^y = y^x$ (on pourra commencer par montrer que x divise y si $x < y$).

2. Montrer que 13 divise $3^{70} + 2^{70}$.

3. Montrer que p est premier si et seulement si $(p-1)! + 1$ est congru à 0 modulo p. Soit p un nombre premier. Montrer que si p est congru à 1 modulo 4, -1 a une racine carrée dans $\mathbf{Z}/p\mathbf{Z}$.

4. Trouver les triplets a, b, c tels que $a < b < c$ et $\text{ppcm}(a, b, c) = a + b + c$.

5. Soit $p_1, \ldots, p_k, \ldots$ la suite des nombres premiers consécutifs. Montrer que la suite (p_k) est infinie. La suite $u_k = p_k - p_{k-1}$ est-elle bornée ?

6. Soit p premier impair. Montrer que le nombre de carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$ est $\frac{p-1}{2}$. Montrer que si p est congru à 1 modulo 4, il existe $n \in \mathbb{Z}$ tel que $n^2 \equiv -1$. Montrer qu'il existe $(a, b) \in \mathbb{Z}^2$ tels que $0 < b < \sqrt{p}$ et $|b\frac{n}{p} - a| \leq \frac{1}{\sqrt{p}}$. Montrer que

$$(bn - ap)^2 + b^2 = p.$$

7. Trouver le dernier chiffre de l'écriture décimale de $7^{(7^7)}$.

8. Montrer qu'il existe une infinité de nombres premiers congrus à -1 modulo 4.

9. Soit $A = \{a + bj \ / \ (a, b) \in \mathbb{Z}^2\}$, où $j = e^{2i\pi/3}$.
a) Montrer que A est un sous-anneau de $\mathbb{C}$.
b) Soit $u \in A$. Montrer que u est inversible (dans A) si et seulement si $|u| = 1$. Enumérer les éléments inversibles de A.
c) Soient u et v dans A, avec $v \neq 0$. Etablir l'existence de $(q, r) \in A^2$ vérifiant $u = qv + r$ et $|r| < |v|$.
d) Montrer que A est un anneau principal.

10. Soit $f : \mathbb{N}^* \to \mathbb{R}$ monotone telle que $m \wedge n = 1 \Longrightarrow f(mn) = f(m)f(n)$.
a. Montrer que l'on peut se ramener à f croissante et $f(1) = 1$.
b. Soit p premier et $x_0 \in \mathbb{N}^*$. On note

$$\alpha = \min\{\frac{f(p+x)}{f(x)} \mid x \in \mathbb{N}^*,\ x \geq x_0,\ x \text{ non multiple de } p\}.$$

Prouver que $\alpha = 1$.

11. On note $\Phi_1(X) = X$ et pour $n \geq 2$, $\Phi_n(x) = \prod_{k \wedge n = 1} (X - e^{\frac{2ik\pi}{n}})$
1. Montrer que Φ_n est à coefficients entiers.
2. Que peut on dire d'un nombre premier p divisant $\Phi_n(a)$, où $a \in \mathbb{Z}$, mais aucun des $\Phi_d(a)$ pour d diviseur strict de n.
3. Soit $n \geq 1$ fixé; montrer qu'il existe une infinité de nombres premiers de la forme $\lambda n + 1$ avec $\lambda \in \mathbb{N}$.

12. Montrer qu'il existe un multiple de 1996 dont l'écriture décimale ne comporte que le chiffre 4.

13. Soit p un nombre premier, $n, k \in \mathbb{N}$.
1. Montrer que n est premier si et seulement si, pour tout $i \in [1, n-1]$, n divise C_n^i. 2. Soit $n_0, \ldots, n_j$ et $k_0, \ldots, k_j$ les chiffres de l'écriture de n et k en base p (éventuellement complétés avec des 0). Montrer que

$$C_n^k \equiv C_{n_0}^{k_0} \ldots C_{n_j}^{k_j} \pmod{p}$$

3. Montrer que le nombre de coefficients binomiaux impairs sur la n-ième ligne du triangle de Pascal est une puissance de 2.

Réels et complexes

14. Soit G un sous groupe de $(\mathbf{R}, +)$. Montrer que soit $G = a\mathbf{Z}$ pour un $a \in \mathbf{R}$, soit G est dense dans $\mathbf{R}$.

15. Montrer que $(20 + 14\sqrt{2})^{1/3} + (20 - 14\sqrt{2})^{1/3} \in \mathbf{Q}$.

16. G un groupe abélien totalement ordonné archimédien. Soit $a \in G$, $a > O$. Soit $x \in G$.

a) Montrer que pour tout entier n il existe un unique entier $m_n(x)$ vérifiant $m_n(x)a \leq nx < (m_n(x)+1)a$. On pose $u_n(x) = m_n(x)/n$ et $v_n(x) = (m_n(x)+1)/n$, $U(x) = \{u_n(x) | n \in \mathbf{N}\}$, $V(x) = \{v_n(x) | n \in \mathbf{N}\}$ (parties de $\mathbf{R}$).

b) Montrer que $U(x)$ et $V(x)$ sont deux parties adjacentes de $\mathbf{R}$. Leur borne commune est notée $f(x)$.

c) Montrer que $f: G \to \mathbf{R}$ est strictement croissante et que f est un morphisme de groupes injectif.

d) On suppose de plus que G a la propriété de la borne supérieure. Montrer que G est isomorphe soit à $\mathbf{R}$ soit à $\mathbf{Z}$.

Polynômes

17. Soit $p \in \mathbf{N}$ et $n(0), \ldots, n(p) \in \mathbf{N}$ tels que $\forall i, \quad n(i) \equiv i \pmod{p+1}$. Montrer que $1 + X + \ldots + X^p$ divise $X^{n(0)} + X^{n(1)} + \ldots + X^{n(p)}$.

18. Montrer que pout tout nombre premier p il existe un corps à p^2 éléments.

19. Trouver P de degré 7 tel que $(X-1)^4$ divise $P(X)+1$ et $(X+1)^4$ divise $P(X)-1$.

20. Soit $P(X) = a_n X^n + \ldots + a_o \in \mathbf{Z}[X]$ et p un nombre premier. On suppose que p ne divise pas a_n , divise tous les a_i pour $i < n$, et que p^2 ne divise pas a_o. Montrer que P est irréductible dans $\mathbf{Z}[X]$.

21. Soit $P(X) = a_n X^n + \ldots + a_o \in \mathbf{Z}[X]$ et soit p/q une racine rationnelle de P (avec $p \wedge q = 1$). Montrer que q divise a_n, que p divise a_o et que pour tout entier m, $p - mq$ divise $P(m)$.Trouver les racines rationnelles de $x^3 - 6x^2 + 15x - 14$.

22. Si $P \in \mathbf{Z}[X]$, on note $c(P)$ le PGCD (positif) des coefficients de P. On dit que P est primitif si $c(P) = 1$.

a) Montrer que si un nombre premier divise tous les coefficients d'un produit PQ, il divise tous les coefficients de P ou tous les coefficients de Q. En déduire que le produit de deux polynômes primitifs est encore primitif.

b) Montrer que $c(PQ) = c(P)c(Q)$.

c) Soit $P \in \mathbf{Z}[X]$, $\deg P \geq 1$. Montrer que si P n'est pas irréductible dans $\mathbf{Q}[X]$, il ne l'est pas dans $\mathbf{Z}[X]$. Quels sont les éléménts irréductibles de $\mathbf{Z}[X]$.

23. Trouver les $P \in \mathbf{C}[X]$ tels que $P(X^2) = P(X-1)P(X+1)$.

24. Soit $P \in \mathbf{R}[X]$. Montrer l'équivalence de

(i) $\forall x \in \mathbf{R}, \quad P(x) \geq 0$

(ii) $\exists A, B \in \mathbf{R}[X], \quad P = A^2 + B^2$.

25. Soit $P \in \mathbf{R}[X]$ scindé n'ayant que des racines simples, $P(X) = a_n X^n + \ldots + a_o$. Montrer que $\forall q \in [1, n-1], \quad a_{q-1} a_{q+1} \leq {a_q}^2$.

26. Soit $n \in \mathbb{N}$, $n \geq 3$. Montrer qu'il n'existe pas de polynômes P, Q, R à coefficients complexes et non tous trois proportionnels tels que: $P^n + Q^n = R^n$.

27. a) Etant donné un corps K, $n+1$ éléments distincts de K notés $a_o, \ldots, a_n$ et $n+1$ éléments de K notés $b_o, \ldots, b_n$, montrer qu'il existe un unique polynôme $P(X)$ de degré inférieur ou égal à n vérifiant $P(a_i) = b_i$, pour $i = 0, \ldots, n$.

b) Montrer que $P(X)$ s'écrit donc d'une manière et d'une seule sous la forme

$$P(X) = c_o + c_1(X - a_o) + c_2(X - a_o)(X - a_1) + \ldots + c_n(X - a_o)(X - a_1)\ldots(X - a_{n-1})$$

$$= d_o + d_1(X - a_1) + d_2(X - a_1)(X - a_2) + \ldots + d_n(X - a_1)(X - a_2)\ldots(X - a_n)$$

et que $c_n = d_n$

c) pour $i \leq j$, soit $D_{i,j}$ le coefficient de degré $j - i$ du polynome de degré inférieur ou égal à $j - i$ ayant pour valeur b_k aux points a_k pour $i \leq k \leq j$. Montrer que $\forall k, \quad c_k = D_{o,k}$ et que l'on a $D_{o,n} = \dfrac{D_{o,n-1} - D_{1,n}}{a_n - a_o}$. En déduire que plus généralement $\forall i \leq j, \quad D_{i,j} = \dfrac{D_{i,j-1} - D_{i+1,j}}{a_j - a_i}$.

d) En déduire un algorithme de calcul des c_k.

e) Construire un algorithme d'évaluation de $P(x)$ connaissant les c_k.

28. Trouver les polynômes P, Q de $\mathbb{R}[X]$ tels que $P(X)^2 + (1 - X^2)Q(X)^2 = 1$.

29. Soit f et g deux polynômes à coefficients complexes, de degré $p \geq 1$ et $q \geq 1$ respectivement.

a) Montrer que f et g admettent une racine commune si, et seulement si, il existe deux polynômes A et B non nuls, avec $\deg A \leq q - 1$ et $\deg B \leq p - 1$, tels que $Af + Bg = 0$.

b) Soit φ l'application de $\mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X]$ vers $\mathbb{C}_{p+q-1}[X]$ définie par :

$$\varphi(A, B) = Af + Bg.$$

Montrer que φ est bijective si, et seulement si, f et g n'ont aucune racine commune.

c) Soit $f(X) = aX^2 + X - 1$ et $g(X) = aX^3 + aX^2 + 1$. Donner la matrice de φ, puis une condition nécessaire et suffisante sur a pour que f et g aient une racine commune.

30. Soit K un corps commutatif. Déterminer les automorphismes du corps $K(X)$ des fractions rationnelles à une indéterminée sur K.

31. Soient P et Q deux polynômes de $\mathbb{R}[X]$, scindés sur $\mathbb{R}$. On suppose que les racines de Q ne sont pas dans $[0, \deg P]$. Soit $P = \sum_{k=0}^{n} a_k X^k$. On pose $R = \sum_{k=0}^{n} a_k Q(k) X^k$. Montrer que R est scindé sur $\mathbb{R}$.

32. Soit (P, Q) un couple de polynômes réels simplement scindés tels qu'entre deux racines de l'un il y ait toujours au moins une racine de l'autre. Montrer que le polynôme $\lambda P + \mu Q$ reste scindé lorsque le couple (λ, μ) décrit $\mathbb{R}^2$. Etudier une réciproque.