HX3 2006/2007 - Arithmétique

1. Pour tout $n \in \mathbb{N}^*$, on note $u_n = \sum_{k=1}^{n} k^2 k!$. Montrer que 9 divise u_n si et seulement si $n \neq 1$ et $n \neq 4$.

2. Montrer que l'équation $x^4 + y^4 + z^4 - 2y^2z^2 - 2x^2z^2 - 2x^2y^2 = 120$ n'a pas de solution $(x, y, z) \in \mathbb{Z}^3$.

3. Résoudre dans $\mathbb{Z}^2$: $3x^2 + xy - 11 = 0$

4. Soient $n \in \mathbb{N}^*$, $(a_1, a_2, \dots, a_n) \in (\mathbb{N}^*)^n$. Montrer qu'il existe une partie A non vide de $[\![1, n]\!]$ telle que n divise $\sum_{k \in A} a_k$.

5. Calculer le pgcd et le ppcm de 5576 et 4264.

6. Résoudre dans $\mathbb{Z}^2$ l'équation : $364x + 2565y = 1$.

7. 1) Vérifier que 429 et 700 sont premiers entre eux.
2) Déterminer tous les couples $(u, v) \in \mathbb{Z}^2$ tel que $700u + 429v = 1$.
3) Quel est l'inverse de $\overline{429}$ dans $\mathbb{Z}/700\mathbb{Z}$.

8. Soient $(m, n) \in \mathbb{Z}^2$ et $(a, b, c, d) \in \mathbb{Z}^4$ tel que $ad - bc = 1$. Montrer que $\mathrm{pgcd}(am + bn, cm + dn) = \mathrm{pgcd}(m, n)$.

9. Soit $n \in \mathbb{N}^*$.
1) Montrer que $2n + 1$ et $14n + 3$ sont premiers entre eux.
2) Montrer que $n^4 + 3n^2 + 1$ et $n^3 + 2n$ sont premiers entre eux.
3) Montrer que $\mathrm{ppcm}(1, 2, \dots, 2n) = \mathrm{ppcm}(n + 1, n + 2, \dots, 2n)$.

10. Soit $(a, b, c) \in \mathbb{Z}^3$. Montrer que si a, b et c sont premiers entre eux deux à deux, $ab + bc + ca$ et abc sont premiers entre eux.

11. Soit $(n, p) \in \mathbb{N}^2$, δ un diviseur de np. Vérifier l'existence d'un diviseur ν de n et π de p tel que $\delta = \nu\pi$.

12. Montrer que tout groupe fini de cardinal p premier est cyclique.

13. Soit G un groupe cyclique engendré par a, $n = \mathrm{Card}G$, $k \in \mathbb{Z}$. Démontrer que a^k engendre G si, et seulement si k est premier avec n.

14. 1) Soit G un groupe, a un élément de G, d'ordre fini n, $p \in \mathbb{Z}$. Montrer que l'ordre de a^p est $\dfrac{n}{\mathrm{pgcd}(n, p)}$.
2) Quel est l'ordre de $\bar{p}$ dans $\mathbb{Z}/n\mathbb{Z}$.

15. Soit G un groupe.
1) Soient H et H' deux sous-groupes finis de G dont les cardinaux sont premiers entre eux. Montrer que $H \cap H' = \{1\}$.
2) Soit $(a, b) \in G^2$, d'ordre fini premiers entre eux. Si $ab = ba$, montrer que l'ordre de ab est le produit des ordres de a et de b.

16. Soit $(n_i)_{i \in I}$ une famille finie de $\mathbb{N}^*$. Vérifier l'équivalence des propositions :
(i) $\mathrm{ppcm}_{i \in I}\, n_i = \prod_{i \in I} n_i$
(ii) Les n_i sont premiers entre eux deux à deux.

17. Soient $(n_i)_{i \in I}$ une famille finie non vide d'éléments de $\mathbb{N}^*$ et m un multiple commun aux n_i. Montrer que

$$\left(\underset{i \in I}{\mathrm{ppcm}}\, n_i\right) \left(\underset{i \in I}{\mathrm{pgcd}}\, \frac{m}{n_i}\right) = m = \left(\underset{i \in I}{\mathrm{pgcd}}\, n_i\right) \left(\underset{i \in I}{\mathrm{ppcm}}\, \frac{m}{n_i}\right)$$

Que deviennent ces formules avec $m = \prod_{i \in I} n_i$?

18. Soient $n \in \mathbb{Z}$ et $(p_i)_{i \in I}$ une famille finie de $\mathbb{Z}$.

1) Vérifier que $\text{ppcm}(n, \text{pgcd}_{i\in I}\, p_i) = \text{pgcd}_{i\in I}(\text{ppcm}(n, p_i))$.
2) Vérifier que si $\text{ppcm}_{i\in I}\, p_i \neq 0$, $\text{pgcd}(n, \text{ppcm}_{i\in I}\, p_i) = \text{ppcm}_{i\in I}(\text{pgcd}(n, p_i))$

---

19. **Nombres de Fermat :** 1) Soit $p \geqslant 1$. On suppose $2^p + 1$ premier. Montrer que p est une puissance de 2.
Pour $n \in \mathbb{N}$, on note $F_n = 2^{2^n} + 1$ (n-ième nombre de Fermat).
2) Montrer que pour $m \neq n$, F_m et F_n sont premiers entre eux.
3) Constater que F_0, F_1, F_2, F_3 et F_4 sont premiers, mais pas F_5.

---

20. **Petit théorème de Fermat :**
1) Soit K un corps fini de cardinal p. Montrer que pour tout $x \in K^*$, $x^{p-1} = 1$.
2) Soit p un nombre premier, $n \in \mathbb{Z}$ non divisible par p. Prouver que $n^{p-1} \equiv 1 \pmod p$.

---

21. On suppose connus les résultats de l'exercice précédent.
1) Quel est le reste de la division euclidienne de $2^{70^{71}}$ par 13?
2) Quel est le reste de la division euclidienne de $1000^{2000^{3000^{4000}}}$ par 19?
3) Montrer que pour tout $n \in \mathbb{Z}$, $n^7 \equiv n \pmod{42}$.
4) Soit $(a, b) \in \mathbb{Z}^2$. Montrer que 56786730 divise $ab(a^{60} - b^{60})$.
5) Trouver les nombres premiers p tel que p divise $2^p + 1$.
6) Montrer que $13 | 2^{70} + 3^{70}$.

---

22. Trouver les $x \in \mathbb{Z}$ tels que :

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 6 \pmod{10} \\ x \equiv 3 \pmod 7 \end{cases}$$

---

23. 1) Montrer qu'il existe une infinité de nombres premiers de la forme $4n + 3$ (avec $n \in \mathbb{N}$).
2) Montrer qu'il existe une infinité de nombres premiers de la forme $6n + 5$ (avec $n \in \mathbb{N}$).

---

24. Soit $(a, b, c) \in \mathbb{Z}^3$ une solution de (E) $x^2 + y^2 = 3z^2$. Montrer que a, b et c sont pairs. Conclure.

---

25. Soient p un nombre premier, $n \in \mathbb{Z}$. Montrer que si n n'est pas congru à 1 modulo p et si $n^3 \equiv 1 \pmod p$ alors $(n + 1)^6 \equiv 1 \pmod p$.

---

26. **Théorème de Wilson :**
1) Soit K un corps fini commutatif. Montrer que $\displaystyle\prod_{x\in K^*} x = -1$.
2) Soit p un nombre premier. Montrer que $(p - 1)! \equiv -1 \pmod p$.

---

27. Soit $p \geqslant 5$ un nombre premier et $N \in \mathbb{N}$ défini par :

$$\sum_{k=1}^{p-1} \frac{1}{k^2} = \frac{N}{(p-1)!^2}$$

Montrer que p divise N.

---

28. Soient p un nombre premier et $1 \leqslant k \leqslant p - 1$. Montrer que p divise C_p^k.

---

29. On suppose connu le résultat de l'exercice précédent. Soit A un anneau intègre de caractéristique finie p, p étant supposé premier. On considère le morphisme de Frobenius :

$$f: \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & x^p \end{array}$$

1) Montrer qu'effectivement, f est un morphisme injectif d'anneau.
2) Qu'est ce que f lorsque $A = \mathbb{Z}/p\mathbb{Z}$?
3) On suppose A fini. Montrer que f est bijective.

---

30. Soit $n \in \mathbb{N}$ tel que $2n + 1$ et $3n + 1$ sont des carrés parfaits. Montrer que $40 | n$.

---

31. Soient n et p deux entiers premiers entre eux. Montrer que $\text{pgcd}(np, n+p) = 1$.

---

32. Soient a, b, c et n dans $\mathbb{N}^*$ tel que $\text{pgcd}(a,b) = 1$ et $ab = c^n$. Montrer qu'il existe $(\alpha, \beta) \in \mathbb{N}^2$ tel que $a = \alpha^n$ et $b = \beta^n$.

---

33. Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$ et $n = \displaystyle\prod_{k=1}^{s} p_k^{r_k}$ sa décomposition en facteurs premiers. Quel est le nombre de diviseurs de n?

---

34. Soient $n \in \mathbb{N}^*$, N le nombre de diviseur positif de n, P le produit de ces diviseurs. Donner une relation entre n, N et P.

---

35. 1) Montrer que si x est inversible dans $\mathbb{Z}/24\mathbb{Z}$, $x^2 = \bar{1}$.

2) En déduire que pour tout $(a,b) \in \mathbb{Z}^2$ tel que 24 divise $1 + ab$, 24 divise $a + b$.

3) Montrer que pour tout $n \in \mathbb{N}^*$ divisible par 24, la somme des diviseurs de $n - 1$ est aussi divisible par 24.

---

36. Résoudre dans $\mathbb{N}^* \times \mathbb{N}^*$ l'équation $a^b = b^a$.

---

37. On note A la somme des chiffres de 4444^{4444}, B la somme des chiffres de A et C la somme des chiffres de B. Montrer que $C = 7$.

---

38. Soient N_1, N_2,..., N_q deux à deux distincts dans $\mathbb{N}^*$. Pour tout $k \in \mathbb{Z}$, on pose :

$$P_k = \prod_{i=1}^{q} (N_i + k)$$

1) On suppose que pour tout $1 \leqslant i \leqslant k$, $N_i = i$. Démontrer que pour tout $k \in \mathbb{Z}$, $P_0 | P_k$.

2) Réciproquement, on suppose que pour tout $k \in \mathbb{Z}$, $P_0 | P_k$.

a. En faisant $k = 1$ et $k = -1$, montrer qu'il existe $i \in \{1, 2, \ldots, q\}$, tel que $N_i = 1$.

b. En déduire que N_1, N_2,..., N_q sont les q premiers entiers naturels non nuls.

---

39. Montrer que :

$$(\mathbb{Z}/20\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

---

40. Montrer que $\displaystyle\min_{(n,m) \in \mathbb{N}^{*2}} |36^n - 5^m| = 11$.

---

41. 1) Soient G, H deux groupes finis, $a \in G$, $f : G \longrightarrow H$ un morphisme de groupes. Montrer que l'ordre de $f(a)$ dans H divise celui de a dans G.

2) On considère $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$ muni de leur structure de groupes ($n, m \geqslant 2$) et $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ un morphisme de groupes. On note d l'ordre de $x = f(\bar{1})$.

a. Montrer que d divise n et m.

b. Que peut-on dire de f lorsque n et m sont premiers entre eux ?

c. Exhiber un élément d'ordre d de $\mathbb{Z}/m\mathbb{Z}$.

3) Soit d un diviseur positif commun à n et m, x un élément d'ordre d dans $\mathbb{Z}/m\mathbb{Z}$. Construire un morphisme de groupes $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ tel que $f(\bar{1}) = x$.

---

42. **Théorème chinois :** soit m et n deux entiers naturels non nuls premiers entre eux. Pour $x \in \mathbb{Z}$, on note $\bar{x}$ la classe de x modulo m et $\dot{x}$ la classe de x modulo n.

1) Montrer que

$$f : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & (\bar{x}, \dot{x}) \end{array}$$

est un morphisme d'anneaux.

2) Démontrer que $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ en tant qu'anneaux.

---

43. Pour $p \in \mathbb{Z}$, on note $p.\mathbb{Z}/n\mathbb{Z}$, ou encore $p\mathbb{Z}/n\mathbb{Z}$ le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ image du morphisme de groupes :

$$f : x \in \mathbb{Z}/n\mathbb{Z} \longmapsto p.x \in \mathbb{Z}/n\mathbb{Z}$$

Montrer qu'en tant que groupes :

$$p\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\left(\frac{n}{\mathrm{pgcd}(p,n)}\right)\mathbb{Z}.$$