Epreuve du 18 novembre 2025
Corrigé

exercice 1 Répondre par *vrai* ou *faux* aux assertions suivantes. Justifier toute réponse à l'aide d'un raisonnement, d'un calcul, d'un énoncé de cours (que l'on citera avec soin) ou d'un contre-exemple.

A1 L'application $\mathbf{N}^3 \to \mathbf{N} : (a,b,c) \mapsto 2^a\, 3^b\, 5^c$ est injective.

C'est vrai par unicité (à l'ordre près) de la factorisation primaire d'un entier.

A2 L'entier 349 est un nombre premier.

C'est vrai. Si l'entier N est composé, son plus petit facteur premier p est tel que $p^2 \leq N$. Il suffit donc de vérifier qu'aucun nombre premier $p < \sqrt{349}$ n'est diviseur de 349. Comme $19 \times 19 = 361 > 349$, il suffit de tester $2, 3, 5, 7, 11, 13$ et 17. En notant $N = 249$, on a $N \equiv 1[2]$, $N \equiv 1[3]$, $N \equiv -1[5]$, $N \equiv -1[7]$, $N \equiv 8[11]$, $N \equiv 11[13]$, $N \equiv 9[17]$.

A3 Le dernier chiffre de l'écriture de $5^{5^{5^n}}$ en base 3 est égal à 2 pour tout $n \in \mathbf{N}^\times$.

C'est vrai. On cherche le reste de $5^{5^{5^n}}$ par 3, or $5^2 = 25 \equiv 1[3]$ et $5^{5^n} \equiv 1[2]$, i.e. $5^{5^n} = 2q+1$ et $5^{5^{5^n}} = 5^{2q+1} = (5^2)^q\, 5 \equiv 5[3] \equiv 2[3]$.

A4 Soit p un nombre premier impair. Alors p divise $2^{\frac{p-1}{2}} - 1$ ou p divise $2^{\frac{p-1}{2}} + 1$.

C'est vrai. Comme $p \geq 3$ est impair, p ne divise pas 2 et par le petit théorème de Fermat $2^{p-1} \equiv 1[p]$, i.e. $p \mid 2^{p-1} - 1 = (2^{\frac{p-1}{2}} + 1)(2^{\frac{p-1}{2}} - 1)$. Par Gauss, p divise l'un de ces deux facteurs.

A5 Soit $n \geq 1$ un entier naturel. Si $\sqrt{n} \in \mathbf{Q}$ alors $\sqrt{n} \in \mathbf{N}$.

C'est vrai. Supposons $\sqrt{n} = \frac{a}{b}$ avec a, b des entiers tels que pgcd $(a,b) = 1$.
On sait que pgcd $(a,b) = 1$ équivaut à pgcd $(a^2, b^2) = 1$. L'égalité au carré s'écrit $b^2 n = a^2$, donc b^2 divise a^2, i.e. pgcd $(a^2, b^2) = b^2$, donc $b^2 = 1$ et $\sqrt{n} = a \in \mathbf{N}$.

A6 Le groupe $((\mathbf{Z}/15\mathbf{Z})^\times, \cdot)$ des inversibles multiplicatifs de l'anneau $\mathbf{Z}/15\mathbf{Z}$ est cyclique.

C'est faux. Pour $a \in [1, 15]$, la classe $\overline{a}$ est inversible ssi pgcd $(a, 15) = 1$, i.e.

$$(\mathbf{Z}/15\mathbf{Z})^\times = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$$

et ce groupe est cyclique ssi il contient une classe d'ordre multiplicatif 8.
Pour limiter les calculs on peut se servir du fait qu'un groupe cyclique d'ordre n contient exactement $\varphi(n)$ éléments d'ordre n. Ici $\varphi(8) = 4$ donc si ce groupe est cyclique, l'une des quatre classes $\overline{2}, \overline{4}, \overline{7}, \overline{8}$ est d'ordre 8 (sinon il contiendrait au plus $3 < \varphi(8)$ classes d'ordre 8).

Mais dans $\mathbf{Z}/15\mathbf{Z}$, $\overline{2}^4 = \overline{16} = \overline{1}, \overline{4}^2 = \overline{16} = \overline{1}, \overline{7}^2 = \overline{49} = \overline{4} \Rightarrow \overline{7}^4 = \overline{4}^2 = \overline{1}$ et $\overline{8}^2 = \overline{64} = \overline{4} \Rightarrow \overline{8}^4 = \overline{4}^2 = \overline{1}$ montrent que ces quatre classes sont d'ordre 2 ou 4.

exercice 2

On fixe deux nombres premiers p et q ($p < q$) et deux entiers a et b non nuls.

1. Soit x un entier. Montrer que l'on a

$$x^2 \equiv a^2 \bmod pq \qquad (C)$$

si et seulement si x est solution de l'un des quatre systèmes de congruences

$$\begin{cases} x \equiv \pm a \bmod p \\ x \equiv \pm a \bmod q \end{cases}$$

[*Pour le sens $\Rightarrow$, commencer par écrire ce que signifie la congruence (C), penser à une identité remarquable et se servir du lemme de Gauss.*]

2. Déterminer tous les entiers x tels que

$$x^2 \equiv 1 \bmod 77.$$

3. Faire la liste des éléments d'ordre 2 du groupe multiplicatif $((\mathbf{Z}/77\mathbf{Z})^\times, \cdot)$.

Corrigé: un rappel: soient x et y des entiers et r un nombre premier tel que $r|xy$. Alors $r|x$ ou $r|y$.
En effet, si r ne divise pas x, alors pgcd $(r, x) = 1$ et par Gauss r divise y.

Venons-en à l'exercice:

1. Dans le sens $\Rightarrow$: pq divise $x^2 - a^2 = (x-a)(x+a)$, donc $p|(x-a)(x+a)$ et $q|(x-a)(x+a)$. Par le rappel, p et q divisent l'un des entiers $(x-a)$ et $(x+a)$ ce qui s'écrit $x \equiv \pm a \bmod p$ et $x \equiv \pm a \bmod q$.

Dans le sens $\Leftarrow$: les quatre congruences entrainent $x^2 \equiv a^2 \bmod p$ et $x^2 \equiv a^2 \bmod q$. La factorisation primaire de $x^2 - a^2$ contient donc p et q, i.e. $pq|x^2 - a^2$.

2. Il s'agit de résoudre les quatre systèmes

$$\begin{cases} x \equiv \pm 1 \bmod 7 \\ x \equiv \pm 1 \bmod 11 \end{cases}$$

$++$: $x \equiv 1[77]$ et $--$: $x \equiv -1[77]$.

$+-$: $x \equiv 1[7]$ s'écrit $x = 1 + 7K$ et $x \equiv -1[11]$ s'écrit $x = -1 + 11L$. On cherche donc (K, L) avec $11L - 7K = 2$. Le couple $(K, L) = (6, 4)$ est solution et $x = 1 + 7 \times 6 = 43$ est une solution particulière. La solution générale s'écrit $x \equiv 43[77]$.

$-+$: il suffit de changer le signe du cas $+-$: $x = -43$ est une solution particulière et la solution générale s'écrit $x \equiv -43[77] \equiv 34[77]$.

3. La classe $\overline{1}$ est d'ordre multiplicatif 1. Par la question 2, les classes d'ordre 2 sont $\overline{-1}, \overline{43}$ et $\overline{34}$.

exercice 3 (Trois preuves de l'existence d'une infinité de nombres premiers.)

preuve 1. Soit $F_n = 2^{2^n} + 1, n \in \mathbf{N}$, la suite des nombres de Fermat.

i) Montrer que $\Pi_{k=0}^{n-1} F_k = F_n - 2$ pour tout $n \geq 1$.

ii) En déduire pgcd $(F_k, F_n) = 1$ pour tout $k < n$.

iii) Conclure qu'il y a une infinité de nombres premiers.

preuve 2. On se propose ici de montrer que l'ensemble $P = \{p \text{ premier tel que } p \equiv -1 \text{ mod } 4\}$ est infini.

i) Montrer que tout entier impair est congru à 1 ou à -1 modulo 4.

ii) Faire la liste des dix premiers éléments de P.

Pour $p_1, \ldots, p_N \in P$, on pose $M = 4\,\Pi_{j=1}^{N} p_j - 1$.

iii) Montrer que dans la factorisation primaire $M = \Pi_{k=1}^{r} q_k^{N_k}$ de l'entier M, l'un au moins des facteurs premiers q_k est congru à -1 modulo 4.

iv) Montrer que P est infini.

preuve 3. Pour un nombre premier q, on désigne par $((\mathbf{Z}/q\mathbf{Z})^\times, \cdot)$ le groupe multiplicatif des inversibles du corps $(\mathbf{Z}/q\mathbf{Z}, +, \cdot)$. On note $\overline{a}$ la classe de l'entier a modulo q et si a n'est pas un multiple de q on note ord $(\overline{a})$ l'ordre de $\overline{a} \in (\mathbf{Z}/q\mathbf{Z})^\times$.

i) Montrer que s'il existe un entier $l \geq 1$ tel que $a^l \equiv 1$ mod q, alors $\overline{a} \in (\mathbf{Z}/q\mathbf{Z})^\times$ et ord $(\overline{a})$ divise l. [*Se servir de la division euclidienne.*]

ii) Soit p un nombre premier. Montrer que si q est un facteur premier de $2^p - 1$, alors $q > p$.

iii) Conclure.

corrigé:

preuve 1: i) c'est vrai pour $n = 1$: $F_0 = 2^{2^0} + 1 = 3$, $F_1 = 2^{2^1} + 1 = 5$ et $F_0 = F_1 - 2$.

Si on suppose vrai pour $n \geq 1$, alors $(F_0 F_1 \cdots F_{n-1})F_n = (F_n - 2)F_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2$.

ii) Fixons $k < n$. Si d divise F_k et F_n, alors d divise $F_0 \cdots F_{n-1} = F_n - 2$ et F_n donc d divise $F_n - (F_n - 2) = 2$, i.e. $d = 1$ ou $d = 2$. Mais 2 est exclu car F_n est un nombre impair.

iii) Par le ii), si p_n est un facteur premier de F_n, la suite $(p_n)_{n \in \mathbf{N}^\times}$ est une suite de nombres premiers deux à deux distincts.

preuve 2: i) Soit $N = 2n+1$ un nombre impair. Si $n = 2k$, $N = 4k+1 \equiv 1[4]$ et si $n = 2k+1$, $N = 4k + 3 \equiv -1[4]$.

ii) Ce sont les nombres premiers de la forme $n_k = 4k - 1$. Voici les dix premiers:

$$n_1 = 3, n_2 = 7, n_3 = 11, n_5 = 19, n_6 = 23, n_8 = 31, n_{11} = 43, n_{12} = 47, n_{15} = 59, n_{17} = 67.$$

iii) Les facteurs premiers q_k du nombre impair $M = 4p_1 \cdots p_N - 1$ sont impairs; par le i) $q_k \equiv \pm 1[4]$. Si pour tout k, $q_k \equiv 1[4]$ alors pour tout k, $q_k^{N_k} \equiv 1[4]$ et $M = q_1^{N_1} \cdots q_r^{N_r} \equiv 1[4]$; ceci contredit $M \equiv -1[4]$.

iv) Supposons P fini, i.e. supposons $P = \{p_1, \ldots, p_N\}$ pour un certain $N \geq 10$. Par le iii), l' un des facteurs premiers de M, disons q_k, est congru à -1 modulo 4. Ce facteur q_k est élément de P et par l'hypothèse sur P, $q_k = p_j$ pour un certain $j \leq N$. On a alors $q_k | 4p_1 \cdots p_N - 1$ et $q_k | p_1 \cdots p_N$, donc $q_k | 1$. C'est absurde.

preuve 3: i) *Une réponse:* $a^l \equiv 1[q]$ s'écrit $\overline{a}^l = \overline{1}$ dans $\mathbf{Z}/q\mathbf{Z}$, i.e. $\overline{a}\,\overline{a}^{l-1} = \overline{1}$, donc $\overline{a}$ est inversible d'inverse $\overline{a}^{l-1}$.
Une autre réponse: q étant premier la seule classe $\overline{a} \in \mathbf{Z}/q\mathbf{Z}$ non inversible est la classe nulle $\overline{a} = \overline{0}$ et dans ce cas pour tout $l \geq 1, a^l \equiv 0[q]$.

Par division euclidienne, $l = \tilde{q}\,\mathrm{ord}(\overline{a}) + \tilde{r}$ avec $0 \leq \tilde{r} < \mathrm{ord}(\overline{a})$.
L'égalité $\overline{1} = \overline{a}^l = (\overline{a}^{\mathrm{ord}(\overline{a})})^{\tilde{q}}\overline{a}^{\tilde{r}} = \overline{a}^{\tilde{r}}$ et la majoration $\tilde{r} <$ord $(\overline{a})$ entrainent $\tilde{r} = 0$ par définition de l'ordre, donc ord $(\overline{a})$ divise l.

ii) $q|2^p - 1$ s'écrit $2^p \equiv 1[q]$; par le i) $\overline{2}$ est inversible dans $\mathbf{Z}/q\mathbf{Z}$ et son ordre divise p. p étant premier, ord $(\overline{2})$ est égal à 1 ou p; si c'était 1, on aurait $2 \equiv 1[q]$, i.e. $q|2-1=1$ ce qui est absurde; conclusion: ord $(\overline{2}) = p$.
Par petit Fermat, $2^{q-1} \equiv 1[q]$; à nouveau par le i) ord $(\overline{2}) = p|q-1$, donc $q - 1 \geq p$, i.e. $q > p$.

iii) On peut par exemple observer que toute suite finie $p_1 < \ldots < p_N$ de nombres premiers est une partie stricte de l'ensemble des nombres premiers: en effet, par le ii), tout facteur premier q de $2^{p_N} - 1$ est tel que $q > p_N$.