

Licence MI — Semestre 1

Mathématiques discrètes

1. SOMME, RÉCURRENCE, RAISONNEMENT (1 SEMAINE)

1.1. Somme.

Exercice 1.1. On rappelle que $\sum_{k=1}^n k = \frac{n(n+1)}{2}$ et $\sum_{k=0}^n q^k = \frac{1-q^{n+1}}{1-q}$ ($q \neq 1$).

Calculer les sommes $\sum_{k=2}^{n+2} 5k$, $\sum_{k=1}^n (2k+n-1)$, $\sum_{k=1}^n 3^k$, $1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots + \frac{1}{2^n}$ et le produit $\prod_{k=1}^n 7^k (= 7^1 \times 7^2 \times \dots \times 7^n)$.

Exercice 1.2. Soit $S_n = \sum_{k=1}^n k^2 = 1^2 + 2^2 + \dots + n^2$ pour tout entier naturel n .

(1) Calculer de deux manières différentes la somme $\sum_{k=0}^n ((k+1)^3 - k^3)$.

(2) En déduire que $S_n = \frac{n(n+1)(2n+1)}{6}$.

Exercice 1.3. En vous inspirant de la méthode étudiée dans l'exercice précédent, trouvez une formule pour la somme $S_n = \sum_{k=1}^n k^3 = 1^3 + 2^3 + \dots + n^3$.

1.2. Raisonnement par récurrence.

Exercice 1.4. Soit $(u_n)_{n \in \mathbb{N}}$ la suite de nombres réels définie par $u_0 = 2$ et $u_{n+1} = \frac{u_n}{1+u_n}$. Démontrer que pour tout $n \in \mathbb{N}$, $u_n = \frac{2}{2n+1}$.

Exercice 1.5. Soit $(u_n)_{n \in \mathbb{N}}$ la suite de nombres réels par $u_0 = 3$ et $u_{n+1} = 2u_n - 1$ pour tout $n \in \mathbb{N}$. Démontrer que, pour tout $n \in \mathbb{N}$, $u_n = 2^{n+1} + 1$.

Exercice 1.6. Soit $(u_n)_{n \in \mathbb{N}}$ la suite de nombres réels définie par $u_0 = 0$ et pour tout n positif, $u_{n+1} = \sqrt{3u_n + 4}$. Montrer que la suite est majorée par 4.

1.3. Raisonnement par absurde.

Exercice 1.7. Démontrer que si vous rangez $n+1$ paires de chaussettes dans n tiroirs distincts, alors il y a au moins un tiroir contenant au moins 2 paires de chaussettes.

Exercice 1.8. En utilisant un raisonnement par l'absurde, démontrer que :

- (1) La somme et le produit d'un nombre rationnel (non nul pour le produit) et d'un nombre irrationnel sont des nombres irrationnels.
- (2) La racine carrée d'un nombre irrationnel positif est un nombre irrationnel.
- (3) Un rectangle a pour aire 170 m^2 . Montrer que sa longueur est supérieure à 13 m .
- (4) $\sqrt{2}$ est un nombre irrationnel (écrire $\sqrt{2}$ sous forme d'une fraction irréductible p/q puis discuter la parité de p et q).

Exercice 1.9. Soit $n > 0$. Démontrer que si n est le carré d'un entier, alors $2n$ n'est pas le carré d'un entier. Indication : $\sqrt{2}$ est irrationnel.

2. LOGIQUE, ENSEMBLES, APPLICATIONS (2 SEMAINES)

2.1. Quantificateurs $\forall$ et $\exists$.

Exercice 2.1. Ecrire à l'aide de quantificateurs les propositions suivantes :

- (1) Le carré de tout réel est positif.
- (2) Certains réels sont strictement supérieurs à leur carré.
- (3) Aucun entier n'est supérieur à tous les autres.
- (4) Tous les réels ne sont pas des quotients d'entiers.
- (5) Il existe un entier multiple de tous les autres.
- (6) Entre deux réels distincts, il existe un rationnel.
- (7) Etant donnés trois réels, il y en a au moins deux de même signe.

Exercice 2.2. Peut-on intervertir les quantificateurs " $\forall n \in \mathbb{Z}$ " et " $\exists m \in \mathbb{Z}$ " dans les propositions suivantes ? Justifier proprement votre réponse.

- (1) $\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}$ tel que $n < m$.
- (2) $\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}$ tel que $n^2 < m$.

2.2. Ensembles et opérations d'ensembles.

Exercice 2.3. Dans chacun des cas suivants déterminer si les ensembles A et B sont égaux.

- (1) $A = \{x \in \mathbb{R} \mid x > 0\}$ $B = \{x \in \mathbb{R} \mid x \geq |x|\}$
- (2) $A = \{x \in \mathbb{R} \mid x > 0\}$ $B = \{x \in \mathbb{R} \mid x \leq |x|\}$
- (3) $A = \mathbb{Z}$ $B = \{x \in \mathbb{Z} \mid x^2 - x \text{ pair}\}$
- (4) $A = \{x \in \llbracket 1, 20 \rrbracket = [1, 20] \cap \mathbb{Z} \mid x \text{ impair, non divisible par } 3\}$
 $B = \{x \in \llbracket 1, 20 \rrbracket \mid 24 \text{ divise } x^2 - 1\}$

Exercice 2.4. Définir les ensembles suivants en extension (c'est-à-dire en donnant tous leurs éléments) :

- (1) $A = \{x \in \mathbb{R} \mid x(x+5) = 14\}$
- (2) $B = \{x \in \mathbb{N} \mid x(2x+3) = 14\}$
- (3) $C = \{x \in \llbracket 1, 25 \rrbracket \mid x \text{ est la somme des carrés de deux entiers naturels}\}$
- (4) $D = \{x \in \llbracket 1, 10 \rrbracket \mid x^4 - 1 \text{ est divisible par } 5\}$

Exercice 2.5. Former la liste des parties de $\{a, b, c\}$.

Exercice 2.6. Soit $\mathbb{B} = \{0, 1\}$.

- (1) Quels sont les éléments de $\mathcal{P}(\mathbb{B})$?
- (2) Quels sont les éléments de $\mathcal{P}(\mathcal{P}(\mathbb{B}))$?

Exercice 2.7. Soit $E = \{1, 2, 3, 4, 5, 6, 7\}$ et soit les parties suivantes de E :

$$A = \{1, 2, 3, 4\}; \quad B = \{4, 5, 6, 7\}; \quad C = \{1, 3, 5, 7\}; \quad D = \{2, 3, 4, 5, 6\}.$$

Calculer : $(A \cap B) \cup (C \cap D)$, $(A \cup C) \cap (B \cup D)$, $(A^c \cap D)^c \cap (B \cup C)^c$.

Exercice 2.8. Dans chacun des cas suivants faire la réunion et l'intersection des ensembles A et B .

- (1) $A = \{x \in \mathbb{N} \mid x \text{ impair}\}$ $B = \{x \in \mathbb{N} \mid x \text{ n'est pas divisible par } 3\}$ (Énumérer les premiers termes)
- (2) $A = \{x \in \mathbb{R} \mid 0 \leq x \leq 3\}$ $B = \{x \in \mathbb{R} \mid -2 < x \leq 1\}$
- (3) $A = \{(x, y) \in \mathbb{R}^2 \mid x + y \leq 2\}$ $B = \{(x, y) \in \mathbb{R}^2 \mid 2 < 3x - y\}$ (Résolution graphique)

Exercice 2.9. Dans une classe de 30 élèves, tous font au moins une des deux langues : allemand ou espagnol. 18 font allemand et 19 font espagnol. Combien font les deux langues ?

Exercice 2.10. On se donne trois ensembles A , B , C tels que $A \cap B \cap C = \emptyset$. Sont-ils obligatoirement disjoints 2 à 2 ? Donner des exemples.

Exercice 2.11. Soit $A = \{1, 2, 3\}$, $B = \{1, 5\}$ et $C = \{2, 10\}$.

- (1) Expliciter les produits cartésiens : $A \times B$, $B \times A$, $C \times B$, $(A \cap C) \times B$, ainsi que l'ensemble $(A \times B) \cap (C \times B)$.
- (2) Que remarque-t-on ? Peut-on généraliser le résultat ?
- (3) Énoncer un résultat analogue avec le symbole $\cup$ au lieu de $\cap$.

Exercice 2.12. Soient les sous-ensembles de $\mathbb{R}$ suivants : $I = [0, 3]$, $J = [0, 4]$. Dessiner, dans le plan rapporté au repère orthonormé $(0, \vec{i}, \vec{j})$, l'ensemble $I \times J$.

Exercice 2.13. Soit $D = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$. Dessiner D et démontrer que D ne peut pas s'écrire comme le produit cartésien de deux parties de $\mathbb{R}$.

2.3. Injections, surjections et bijections.

Exercice 2.14. Dans chaque cas dire si l'application $f : A \rightarrow B$ est injective, surjective, ou bijective. Quand elle est bijective déterminer l'application réciproque.

- (1) $A = \mathbb{R}$ $B = \mathbb{R}$ $f(x) = x + 7$
- (2) $A = \mathbb{R}$ $B = \mathbb{R}$ $f(x) = x^2 + 2x - 3$
- (3) $A = \{x \in \mathbb{R} \mid 9 \geq x \geq 4\}$ $B = \{x \in \mathbb{R} \mid 96 \geq x \geq 21\}$ $f(x) = x^2 + 2x - 3$
- (4) $A = \mathbb{R}$ $B = \mathbb{R}$ $f(x) = 3x - 2|x|$
- (5) $A = \mathbb{R}$ $B = \mathbb{R}$ $f(x) = e^x + 1$
- (6) $A = \mathbb{N}$ $B = \mathbb{N}$ $f(x) = x(x + 1)$

Exercice 2.15. Soit $f : \mathbb{Z} \rightarrow \mathbb{Z}$ définie par $f(n) = n + (-1)^n$.

- (1) Montrer que n et $f(n)$ sont toujours de parité différente.
- (2) Montrer que f est bijective.

- (3) Calculer $f(f(n))$. En déduire une expression de f^{-1} et résoudre l'équation :

$$347 = n + (-1)^n$$

dans laquelle n désigne un entier inconnu.

Exercice 2.16. On considère les deux applications f et g de $\llbracket 1, 9 \rrbracket$ vers lui-même définies par leurs tables des valeurs :

x	1	2	3	4	5	6	7	8	9
$f(x)$	6	4	7	8	9	3	5	1	2

x	1	2	3	4	5	6	7	8	9
$g(x)$	1	2	7	4	5	6	3	8	9

- (1) Représenter de la même façon les applications : $g \circ g$, $g \circ f$, $f \circ f$, $f \circ g$.
- (2) Montrer que f est bijective. Représenter de la même façon son application réciproque.

Exercice 2.17. Si E est un ensemble, on appelle identité de E , et on note Id_E , l'application de E vers E définie par : $\text{Id}_E(x) = x$ quel que soit x dans E .

- (1) L'application Id_E est-elle injective ? surjective ? bijective ?
À présent soit $f : A \rightarrow B$ une application entre deux ensembles non vides A et B .
- (2) Montrer que l'application f est injective si et seulement s'il existe une application $g : B \rightarrow A$ telle que $g \circ f = \text{Id}_A$.
- (3) Montrer que f est surjective si et seulement s'il existe $h : B \rightarrow A$ telle que $f \circ h = \text{Id}_B$.
- (4) Si g existe, est-elle unique ? Même question pour h .
- (5) Si f est bijective montrer qu'on a nécessairement $g = h$.

3. COMBINATOIRE (2 SEMAINES)

3.1. Principe des choix successifs.

Exercice 3.1. Combien de menus différents peut-on composer si on a le choix entre 3 entrées, 2 plats et 4 desserts ?

Exercice 3.2. Un questionnaire à choix multiples, autorisant une seule réponse par question, comprend 15 questions. Pour chaque question, on propose 4 réponses possibles. De combien de façons peut-on répondre à ce questionnaire ?

Exercice 3.3. En informatique, on utilise le système binaire pour coder les caractères. Un bit (binary digit : chiffre binaire) est un élément qui prend la valeur 0 ou la valeur 1. Avec 8 chiffres binaires (un octet), combien de caractères peut-on coder ?

Exercice 3.4. (1) Combien peut-on former de numéros de téléphone à 8 chiffres ?
(2) Combien peut-on former de numéros de téléphone à 8 chiffres ne comportant pas le chiffre 0 ?

3.2. Permutations, arrangements et combinaisons.

Exercice 3.5. Les 30 étudiants du groupe G25 doivent passer au tableau chacun leur tour. Combien y a-t-il de manières de constituer cette liste de passage ?

Exercice 3.6. Le dimanche matin un bar PMU prend 5000 paris différents pour le tiercé de l'après-midi. Que peut-on dire du nombre de chevaux engagés dans la course ?

Exercice 3.7. Un tournoi sportif compte 8 équipes engagées. Chaque équipe doit rencontrer toutes les autres une seule fois. Combien doit-on organiser de matchs ?

Exercice 3.8. (1) Parmi l'ensemble $\llbracket 1, 100 \rrbracket$, combien sont des carrés de nombres entiers ?

(2) Combien $\llbracket 1, 100 \rrbracket$ a-t-il de parties à 17 éléments contenant exactement trois carrés ?

(3) Combien $\llbracket 1, 100 \rrbracket$ a-t-il de parties contenant trois carrés et trois seulement ?

Exercice 3.9. Pour se rendre en déplacement les onze joueurs d'une équipe de football et leur entraîneur utilisent trois voitures ordonnées ayant chacune quatre places non numérotées. De combien de façons ces douze personnes peuvent-elles se répartir si toutes ont le permis de conduire ? Même question si cinq ne l'ont pas.

Exercice 3.10. Un portemanteau comporte 5 patères alignées. Combien a-t-on de dispositions distinctes (sans mettre deux manteaux l'un sur l'autre bien que ceux-ci soient indiscernables) :

(1) pour 3 manteaux sur ces 5 patères ?

(2) pour 5 manteaux ?

(3) pour 6 manteaux ?

Exercice 3.11. On utilise 5 cartes : l'as de trèfle, les rois de carreau et de coeur, les dames de carreau et de coeur.

(1) Combien y a-t-il de façons de ranger les cartes sur une rangée de 5 places numérotées ?

(2) Que devient ce nombre si l'on place le roi de carreau à côté de sa dame ?

(3) Calculer le nombre de façons de ranger les cartes pour qu'aucun roi ne soit à côté de sa dame.

3.3. Formule du binôme et plus.

Exercice 3.12. Énoncer puis prouver la formule du binôme de Newton.

Exercice 3.13. (1) Si $n = 3$ et $0 \leq k \leq 3$, calculer $\binom{3}{k}$. Vérifier ensuite que

$$\binom{3}{0}^2 + \binom{3}{1}^2 + \binom{3}{2}^2 + \binom{3}{3}^2 = \binom{6}{3}$$

(2) En faisant des calculs similaires, vérifier que

$$\binom{4}{0}^2 + \binom{4}{1}^2 + \binom{4}{2}^2 + \binom{4}{3}^2 + \binom{4}{4}^2 = \binom{8}{4}$$

(3) En déterminant le coefficient de $x^p y^{n+m-p}$ dans $(x+y)^{n+m}$ et dans $(x+y)^n (x+y)^m$, démontrer l'égalité :

$$\binom{n}{0} \binom{m}{p} + \binom{n}{1} \binom{m}{p-1} + \binom{n}{2} \binom{m}{p-2} + \cdots + \binom{n}{p} \binom{m}{0} = \binom{n+m}{p}$$

(4) En déduire que

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}$$

4. ARITHMÉTIQUE (4 SEMAINES)

4.1. Divisibilité, Bézout.

Exercice 4.1. En divisant un nombre par 8, un élève a obtenu 4 pour reste ; en divisant ce même nombre par 12, il a obtenu 3 pour reste. Qu'en pensez-vous ?

Exercice 4.2. Si $n \in \mathbb{Z}$ n'est pas divisible par 3 (resp. 2), montrer que 3 (resp. 8) divise $(n^2 - 1)$.

Exercice 4.3. Quel est le reste de la division euclidienne de $\sum_{k=1}^{2024} k!$ par 15 ?

Exercice 4.4. Calculer $\text{pgcd}(n, n+1)$ et $\text{ppcm}(n, n+1)$ pour $n \in \mathbb{N}$.

Exercice 4.5. Déterminer une relation de Bézout pour les paires d'entiers $(17, 27)$, $(168, 245)$ et $(128, 320)$.

Exercice 4.6. (1) Soit $a = 132$, $b = 60$ et $d = \text{pgcd}(132, 60)$.

- (a) Factoriser a et b en produit de nombres premiers et donner la valeur de d .
- (b) Retrouver d à l'aide de l'algorithme d'Euclide et en déduire une paire d'entiers (x_0, y_0) tels que $132x_0 + 60y_0 = d$.
- (c) Pour $c \in \mathbb{Z}$, posons $\mathcal{S}_c = \{(x, y) \in \mathbb{Z}^2 : ax + by = c\}$. Déterminer $\mathcal{S}_c$ dans chacun des cas suivants.

- (i) $c = d$; (ii) $c = d + 1$; (iii) $c = 10d$.

- (2) Refaire ces calculs avec $a = 122$ et $b = 60$.

Exercice 4.7. Trouver les solutions entières de l'équation $102x - 18018y = 18$. Combien y a-t-il de solutions telles que x et y soient compris entre 0 et 4000 ?

Exercice 4.8. Montrer que tout entier n peut s'écrire sous la forme $n = 5a + 19b$ avec $a, b \in \mathbb{Z}$.

Exercice 4.9. Montrer les assertions suivantes :

- (1) Il n'existe pas d'entiers m et n tels que $m + n = 15$ et $\text{pgcd}(m, n) = 7$.
- (2) $\text{pgcd}(m, m+n)$ divise n .
- (3) Si $\text{pgcd}(a, n) = \text{pgcd}(a, m) = 1$, alors $\text{pgcd}(a, mn) = 1$.

Exercice 4.10. Déterminer, en justifiant la réponse, si les énoncés suivants sont vrais ou faux.

- (1) Si a divise mn , alors a divise m ou n .
- (2) Si a divise n ou a divise m , alors a divise mn .
- (3) Si a divise mn et a ne divise pas m , alors a divise n .
- (4) Si m et n divisent a , alors mn divise a .
- (5) Si a divise $42n + 37$ et $7n + 4$, alors a divise 13.
- (6) La somme des diviseurs positifs de 7^3 est égale à 400.

4.2. Congruences.

Exercice 4.11. Montrer qu'un entier n est divisible par :

- (1) 3 (resp. 9) si et seulement si la somme des chiffres de n est divisible par 3 (resp. 9).
- (2) 5 si et seulement si le chiffre des unités de n est 0 ou 5.
- (3) 11 si et seulement si le nombre obtenu en faisant alternativement l'addition et la soustraction des chiffres de n est divisible par 11.

On appliquera ces trois différentes règles à l'entier $N = 29\,461\,905$. Cet entier N est-il divisible par 495 ?

Exercice 4.12. Calculer $174\,277^k$ modulo 11 pour tout $k \in \mathbb{N}$. En déduire que 11 divise le nombre $174\,277^{2\,625} - 1$.

Exercice 4.13. En calculant $4^n + 2^n + 1 \pmod{11}$, trouver les entiers n pour lesquels $4^n + 2^n + 1$ est divisible par 7.

Exercice 4.14. Trouver le chiffre des unités de $109^{2\,007}$ et $23^{24^{25}}$.

Exercice 4.15. Résoudre les équations de congruence suivantes :

- (1) $20x \equiv 3 \pmod{10}$
- (2) $123x \equiv 7 \pmod{5}$
- (3) $107x \equiv 112 \pmod{11}$
- (4) $4x \equiv 8 \pmod{16}$

Exercice 4.16. (1) Trouver l'inverse modulo 13 de 2 et de 11.

- (2) Montrer que si a' est l'inverse de a modulo m et b' est l'inverse de b modulo m , alors $a'b'$ est l'inverse de ab modulo m .

Exercice 4.17. Résoudre les systèmes de congruences

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases} \quad \text{et} \quad \begin{cases} x \equiv 5 \pmod{6} \\ 7x \equiv 5 \pmod{12} \end{cases}$$

Exercice 4.18. (1) Résoudre le système de congruences $\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 3 \pmod{7} \end{cases}$

- (2) Soient m et n deux entiers premiers entre eux. Montrer que, pour tous $y, z \in \mathbb{Z}$, il existe $x \in \mathbb{Z}$ tel que $x \equiv y \pmod{m}$ et $x \equiv z \pmod{n}$ et que toutes les solutions $x \in \mathbb{Z}$ sont congrues modulo mn .

Exercice 4.19. Trouver les entiers n tels que :

- (1) n est divisible par 4 et le reste de la division euclidienne de n par 3 ou par 5 est 2.
- (2) le reste de la division euclidienne de n par 11 est 4 et le reste de la division euclidienne de n par 17 est 3.

Exercice 4.20. Soient a, b et c des entiers positifs tels que $a^2 + b^2 = c^2$ (on rappelle que le triplet $(3, 4, 5)$ vérifie la relation). Montrer que :

- (1) a ou b est un multiple de 3.
- (2) a ou b ou c est un multiple de 5.
- (3) a ou b est un multiple de 2.
- (4) a ou b est un multiple de 4.

4.3. Nombres premiers.

Exercice 4.21. Prouver qu'il y a une infinité de nombres premiers.

Exercice 4.22. Soit p un nombre premier. Montrer que, pour tout entier k avec $1 < k < p$, on a $\binom{p}{k} \equiv 0 \pmod{p}$. En déduire que si a et b sont deux entiers, on a $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Exercice 4.23. Énoncer et prouver le petit théorème de Fermat.

Exercice 4.24. Soient p un nombre premier et a un nombre entier. Montrer que si p ne divise pas $a-1$, alors p divise $a + a^2 + \dots + a^{p-1}$.

Exercice 4.25. Montrer que 5 divise $n^5 - n$ pour tout entier n .

Exercice 4.26. Soient p et q deux nombres premiers distincts. Montrer que

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Exercice 4.27. Montrer que :

- (1) si $a^3 + 1$ (avec $a \in \mathbb{N}$) est un nombre premier, alors $a = 1$.
- (2) si $2^n - 1$ (avec $n \in \mathbb{N}$) est un nombre premier, alors n est premier.

On pourra notamment utiliser les factorisations suivantes :

$$u^N - 1 = (u - 1) \cdot \sum_{k=0}^{N-1} u^k \quad ; \quad u^3 - v^3 = (u - v) \cdot (u^2 + uv + v^2)$$

Exercice 4.28. Montrer qu'il existe une infinité de nombres premiers p tels que $p \equiv 3 \pmod{4}$. *Indication : on pourra supposer qu'il y en a un nombre fini $p_1, \dots, p_k$ et considérer l'entier $N = 4p_1 \dots p_k - 1$.*

Exercice 4.29. Montrer que, pour tout entier m , il existe un entier naturel n tel que l'intervalle d'entiers $\llbracket n, n+m \rrbracket$ ne contienne aucun nombre premier.

Indication : on pourra considérer des nombres du type $\ell! + k$ avec $\ell \in \mathbb{N}$ et $0 \leq k \leq \ell$.

Exercice 4.30. Un nombre de Fermat est un entier de la forme $F_n = 2^{2^n} + 1$ avec $n \in \mathbb{N}$.

- (1) Soient F_n et F_m deux nombres de Fermat avec $n > m$. Montrer que si p est un nombre premier qui divise F_m , alors $2^{2^n} \equiv 1 \pmod{p}$.
- (2) En déduire que deux nombres de Fermat distincts sont premiers entre eux.
- (3) En déduire une autre preuve de l'infinitude des nombres premiers.

Exercice 4.31. (1) Soit p un nombre premier. Montrer que, pour tout $x \in \llbracket 1, p-1 \rrbracket$, il existe un unique entier $x' \in \llbracket 1, p-1 \rrbracket$ tel que $xx' \equiv 1 \pmod{p}$.

(2) Soit p un nombre premier. Résoudre modulo p l'équation $x^2 \equiv 1 \pmod{p}$.

(3) En déduire le *théorème de Wilson* (John Wilson, 1741-1793) :
un nombre $p \geq 2$ est premier si et seulement si $(p-1)! \equiv -1 \pmod{p}$.