

I SYSTÈMES DE NUMÉRATION, DIVISIBILITÉ.

1. :
- (a) Montrer qu'un nombre formé de 2 groupes de 3 chiffres (comme 127127) est toujours divisible par 7, par 11 et par 13 ; et pour 2 groupes de 4 chiffres, ou 3 groupes de 2 chiffres ?
- (b) Montrer que plus généralement, dans n'importe quel base, un nombre formé d'un motif différent de 1 répété au moins deux fois n'est jamais premier. En déduire que si n n'est pas premier, le nombre R_n qui s'écrit $\overbrace{11\dots 11}^{n \text{ fois}}$ en base b n'est pas premier, quelle que soit la base. Que retrouve-t-on lorsque $b = 2$?
- (c) * Déterminer le reste de la division par 4 de R_n en base 10 ($n \geq 2$). En déduire que R_n ne peut être un carré.
2. : Montrer qu'en base a , le nombre $0, a_1 a_2 \dots a_n \underbrace{a_1 a_2 \dots a_n} \dots$ est égal à $\frac{a_1 a_2 \dots a_n}{a^n - 1}$. Que vaut par exemple 0,9999... en base 10 ?
3. : Trouver a et b entiers naturels tels que $\frac{a+b}{2} = \overline{xy}$ et $\sqrt{ab} = \overline{yx}$ avec $x \neq y$ (en base 10).
4. :
- (a) Déterminer les résidus symétriques (i.e. compris entre -3 et 3) modulo 7 de 1, 10, 10^2 , 10^3 , etc ; en déduire un critère de divisibilité par 7 en base 10.
- (b) Faire de même pour 13.
Réponses :
- $$N \equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 - a_9 \dots \quad [7]$$
- $$N \equiv a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 4a_5 + a_6 \dots \quad [13]$$
5. (a) Trouver un critère de divisibilité par 7 en base 20.
(b) Trouver un critère de divisibilité par 13 en base 40.
6. (a) Montrer qu'un nombre écrit en base 10 est divisible par 7 ssi en retranchant le double de son dernier chiffre au nombre constitué des autres chiffres, on obtient un nombre divisible par 7 ; appliquer ce critère à 2009 et à 123456789.
(b) * Montrer que plus généralement si $N = \overline{a_n a_{n-1} \dots a_0}$, $N \equiv 10^n (a_n - 2(a_{n-1} - \dots - 2(a_1 - 2a_0) \dots)) \quad [7]$.
(c) * En remarquant que $40 = 3 \times 13 + 1$ et $50 = 3 \times 17 - 1$, trouver de même un critère de divisibilité par 13 et un critère de divisibilité par 17 en base 10 ; les appliquer à 2009 et à 123456789, et trouver deux relations similaires à celle de (d).
7. * : Démontrer que dans une base donnée, il n'y a qu'un nombre fini de nombres égaux à la somme des cubes de leurs chiffres ; Déterminer ces nombres en base 5 et 10.
8. : Montrer que, pour tout n entier :
- (a) $n^3 - n$ est multiple de 6, et que si n est impair, $n^3 - n$ est même multiple de 24.
(b) si n n'est ni pair ni multiple de 3, le reste de la division par 24 de n^2 est 1.
(c) $n^5 - 5n^3 + 4n$ est multiple de 120.
(d) $n(n^2 - 1)(4n^2 - 1)(9n^2 - 1)$ est multiple de 7.
9. * : Démontrer que parmi n entiers pris au hasard, on peut toujours en trouver un certain nombre dont la somme est divisible par n .
10. Montrer à l'aide de congruences, que :
- (a) $\forall n \in \mathbb{N}^* \quad 11 \mid (2^{6n-5} + 3^{2n})$ et $17 \mid (3 \times 5^{2n-1} + 2^{3n-2})$.
(b) $\forall n \in \mathbb{N} \quad n^2 \mid ((n+2)^{n+2} - 2^{n+2}(n+1)^{n+1})$.

11. : Démontrer que les entiers congrus à -1 modulo 4 ne peuvent pas s'écrire comme somme de deux carrés et que les entiers congrus à -1 modulo 8 ne peuvent pas s'écrire comme somme de *trois* carrés (par contre, il a été démontré que tout entier peut s'écrire comme somme de 4 carrés).
12. * : Estimation de la moyenne du nombre de diviseurs d'un entier :
pour deux entiers naturels i et j on pose $\delta(i, j) = 1$ si i divise j , et 0 sinon.
- (a) Pour un entier naturel n , que représente le nombre $d(n) = \sum_{i=1}^n \delta(i, n)$?
- (b) Montrer que $\sum_{j=i}^n \delta(i, j) = \left\lfloor \frac{n}{i} \right\rfloor$.
- (c) En déduire que $\bar{d}(n) = \frac{1}{n} \sum_{j=1}^n d(j)$ est compris entre $h_n - 1$ et h_n où $h_n = \sum_{i=1}^n \frac{1}{i}$.
- (d) Utilisant l'encadrement $\ln n \leq h_n \leq \ln n + 1$, donner un encadrement de $\bar{d}(n)$ puis un équivalent. Vérifier pour $n = 10$.

II THÉORÈMES DE GAUSS ET DE BÉZOUT

13. : Montrer que si un réel x est tel que ax et bx sont entiers, avec a et b entiers premiers entre eux, alors x est entier.
14. * : En utilisant la relation $p \binom{n}{p} = n \binom{n-1}{p-1}$, montrer que pour $1 \leq p \leq n$, $\binom{n}{p}$ est divisible par $\frac{n}{\text{pgcd}(n, p)}$ et par $\frac{p+1}{\text{pgcd}(n+1, p+1)}$; en déduire que $\binom{2n}{n}$ est pair et divisible par $n+1$.
15. : Montrer que si z est une racine $n^{\text{ième}}$ et $m^{\text{ième}}$ de l'unité, alors z est une racine $d^{\text{ième}}$ de l'unité avec $d = \text{pgcd}(n, m)$.
16. * : On dit qu'une suite (u_n) est p -périodique si $u_n = u_{n+p}$ pour tout $n \in \mathbb{N}$.
- (a) Montrer que si (u_n) est p -périodique et q -périodique alors (u_n) est d -périodique avec $d = \text{pgcd}(p, q)$.
- (b) En déduire que p est la plus petite période ≥ 1 de (u_n) et si q est une autre période alors p divise q .
- (c) On suppose que (u_n) est récurrente simple ($u_n = f(u_{n-1})$) ; montrer que si $u_p = u_0$ alors (u_n) est p -périodique.
17. * : Soient a et b deux entiers > 0 .
- (a) Montrer que si a et b sont premiers entre eux, il existe un unique couple d'entiers > 0 (u, v) tel que $au - bv = 1$ vérifiant $u < b$ et $v < a$.
- (b) Montrer que a et b sont *non* premiers entre eux si et seulement s'il existe deux entiers > 0 u et v tels que $au = bv$, avec $u < b$ et $v < a$.
18. :
- (a) Soient a, a' et b trois entiers ; on dit que a' est inverse de a modulo b si et seulement si $aa' \equiv 1 \pmod{b}$; montrer que a possède un inverse modulo b si et seulement si a et b sont premiers entre eux.
- (b) Soit p un nombre premier ; quels sont les entiers ayant un inverse modulo p ? Pour p impair, déterminer un inverse de 1, de -1, de 2 modulo p .

III NOMBRES PREMIERS ET DÉCOMPOSITION EN PRODUITS DE FACTEURS PREMIERS

19. : L'âge du capitaine.
La pertuisane est un sorte de lance utilisée au XV^{ème} et XVI^{ème} siècles. Voici le problème : le dernier jour d'un certain mois de la Première Guerre Mondiale, un obus éclate et met au jour le squelette d'un capitaine. En multipliant l'âge du capitaine au moment de sa mort par le quart du nombre d'années écoulées entre sa mort et la date d'éclatement de l'obus, par numéro du jour remarquable du mois d'éclatement de l'obus, et par la longueur exprimée en pieds de la pertuisane trouvée à côté du squelette, on trouve : 471 569.
Quel est l'âge du capitaine, et quelle est la date de la bataille ?

20. :
- Montrer que si un carré a^2 divise un carré b^2 alors a divise b et $\frac{b^2}{a^2}$ est un carré.
 - En déduire que si n est un entier naturel non carré alors $\sqrt{n} \notin \mathbb{Q}$.
 - Généraliser (a) et (b) en remplaçant 2 par q entier ≥ 2 .
21. On pose $P_n(x) = (x+1)(x^2+1)(x^4+1)\cdots(x^{2^n}+1)$;
- Simplifier $(x-1)P_n(x)$.
 - En déduire la forme développée de $P_n(x)$.
 - En déduire que si $F_n = 2^{2^n} + 1$; $F_n = F_0 F_1 \dots F_{n-1} + 2$; où F_n est le n ième nombre de Fermat.
 - En déduire que si, contrairement à ce qu'espérait Fermat, les nombres de Fermat ne sont pas tous premiers, ils sont au moins premiers deux à deux.
 - En déduire une autre démonstration du fait qu'il y a un nombre infini de nombres premiers.
22. :
- Montrer l'unicité de la forme irréductible d'une fraction ; c'est-à-dire que si $\frac{a}{b} = \frac{c}{d}$ avec $a, b, c, d \in \mathbb{N}^*$, a et b premiers entre eux, c et d premiers entre eux, alors $a = c$ et $b = d$.
 - En déduire que si $a, b \in \mathbb{N}^*$ avec a et b premiers entre eux, a ou b non carré, alors $\sqrt{\frac{a}{b}} \notin \mathbb{Q}$; généraliser à $\sqrt[n]{\frac{a}{b}}$.
23. :
- Montrer que les $(n-1)$ entiers $n! + 2, n! + 3, \dots, n! + n$ pour $n \geq 3$ sont tous composés ; en déduire qu'on peut trouver des listes d'entiers composés consécutifs aussi longues qu'on veut.
 - On pose $n!! \stackrel{def}{=} \prod_{\substack{2 \leq p \leq n \\ p \text{ premier}}} p$; montrer que de nouveau les $(n-1)$ entiers $n!! + 2, n!! + 3, \dots, n!! + n$ sont tous composés.
24. * :
- En s'inspirant de la démonstration d'Euclide de l'infinité des nombres premiers, montrer qu'il existe une infinité de nombres premiers congrus à -1 modulo 4 (indication : $N = 4p_1 p_2 \dots p_n + 1$).
 - Montrer de même qu'il existe une infinité de nombres premiers congrus à -1 modulo 6.
25. *: pour $x \in \mathbb{N}^*$, \mathcal{D}_x désigne l'ensemble des diviseurs de x dans \mathbb{N} . Considérons pour $a, b \in \mathbb{N}^*$ l'application φ :
- $$\left| \begin{array}{l} \mathcal{D}_a \times \mathcal{D}_b \rightarrow \mathbb{N} \\ (d, d') \mapsto dd' \end{array} \right.$$
- A quelle condition nécessaire et suffisante φ est-elle injective ?
 - A quelle condition nécessaire et suffisante a-t-on $\varphi(\mathcal{D}_a \times \mathcal{D}_b) = \mathcal{D}_{ab}$?
26. : Soit $n = \prod_{k=1}^m p_k^{\alpha_k}$ un naturel décomposé en produit de facteurs premiers.
- Montrer que le nombre de diviseurs de n est $N = \prod_{k=1}^m (\alpha_k + 1)$.
 - Que dire donc d'un entier naturel non nul ayant un nombre impair de diviseurs ?
 - Montrer que la somme des diviseurs de n est $S = \prod_{k=1}^m \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$.
 - * Montrer que le produit des diviseurs de n est $P = n^{\frac{N}{2}}$.

(e) * Sans faire intervenir la décomposition en produit de facteurs premiers, mais en utilisant la propriété d'Eratosthène, et en séparant les cas : n carré ou non, montrer que :

- i. $2 \leq N \leq 2\sqrt{n}$.
- ii. $n + 1 \leq S \leq (n + 1)\sqrt{n}$
- iii. $P = \sqrt{n}^N$.
- iv. La somme des inverses des diviseurs de n est $\frac{S}{n}$.

27. :

- (a) Soit $M_p = 2^p - 1$ un nombre de Mersenne premier. Montrer que $N = 2^{p-1}M_p$ est un nombre "parfait", c'est-à-dire que la somme de ses diviseurs **stricts** (i.e. sauf lui-même) est égale à lui-même.
- (b) ** Démontrer que tout nombre parfait pair est du type précédent.

28. * : Par combien de zéros se termine 100! ???

Soient $n \in \mathbb{N}^* \setminus \{1\}$; $p \in \mathbb{P}$; $\alpha = \alpha_p(n!)$ l'exposant de p dans la décomposition de $n!$ en produit de facteurs premiers.

- (a) Que vaut α pour $p > n$?
- (b) Pour $p \leq n$ on note n_1 le quotient de la division de n par p . Montrer que

$$\alpha = n_1 + \alpha_p(n_1!)$$

En déduire un algorithme pour calculer α .

- (c) Calculer $\alpha_2(100!)$ et $\alpha_5(100!)$ et conclure quant au nombre de zéros terminant 100!.

29. : Démontrer qu'un polynôme non constant à coefficients entiers $P = \sum_{k=0}^n a_k X^k$ ne peut pas prendre *uniquement* des valeurs premières pour les valeurs entières naturelles de la variable, mais que par contre, il est possible qu'il en prenne une infinité.

30. : Des nombres premiers en progression arithmétique.

- (a) Montrer que si 3 entiers non multiples de 3 sont en progression arithmétique, la raison est multiple de 3.
- (b) * Soit p un nombre premier ; on rappelle que si p divise un produit, il en divise l'un des termes. Montrer que si p entiers non multiples de p sont en progression arithmétique, la raison est multiple de p .
Indication : soit x_k le reste dans la division par p de $a + kr$; montrer que les nombres x_0, x_1, \dots, x_{p-1} sont p nombres compris entre 1 et $p - 1$...
Montrer que ceci est faux si p n'est plus supposé premier.
- (c) * Application : montrer que si 3 nombres premiers $\neq 3$ sont en progression arithmétique, la raison est multiple de 6 ; donner un exemple.
- (d) * De même, montrer que si 5 nombres premiers $\neq 5$ sont en progression arithmétique, la raison est multiple de 30 ; donner un exemple.

31. * : Désignons par $\pi(n)$ le nombre de nombres premiers $\leq n$. Il a été démontré que pour $n \geq 11$:

$$\frac{\ln n}{n} \leq \pi(n) \leq 1,3 \frac{\ln n}{n}$$

- (a) Vérifier numériquement cette inégalité en calculant $\frac{\pi(n)}{\frac{\ln n}{n}}$ pour $11 \leq n \leq 100$.
- (b) Déduire de cette inégalité le fait qu'il existe toujours au moins un nombre premier entre n et $2n$ (résultat appelé : le "postulat de Bertrand").
Rem : il a été également démontré que $\pi(n) \sim \frac{\ln n}{n}$ (Théorème de Hadamard et de la Vallée Poussin).

32. * : Majoration de $n!!$

Dans cet exercice, n désigne toujours un entier ≥ 2 fixé, q la partie entière supérieure de $n/2$ et p un nombre premier.

(a) Montrer que $\prod_{q \leq p \leq n} p$ divise $\binom{n}{q}$; en déduire que $\prod_{q \leq p \leq n} p \leq 2^n$.

(b) Démontrer par récurrence forte que $n!! \stackrel{def}{=} \prod_{2 \leq p \leq n} p \leq 4^n$.