I SYSTÈMES DE NUMÉRATION, DIVISIBILITÉ.

1. : Les "repunits", ou unités répétées.

   (a) Montrer qu'un nombre formé de 2 goupes identiques 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 $\overbrace{11...11}^{n \text{ fois}}$ en base b n'est pas premier, quelle que soit la base. Que retrouve-t-on lorsque $b = 2$?

   (c) Montrer que que R_n en base 10 ne peut être un carré (utiliser des congruences modulo 4).

2. : Montrer qu'en base b, le nombre $0, a_1a_2...a_n \underbrace{a_1a_2...a_n}...$ est égal à $\dfrac{\overline{a_1a_2...a_n}}{b^n-1}$. Que vaut par exemple 0,9999... en base 10 ?

3. : Trouver a et b entiers naturels tels que $\dfrac{a+b}{2} = \overline{xy}$ 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 :

$$\begin{aligned} N &\equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 - a_9... \quad [7] \\ N &\equiv a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 4a_5 + a_6... \quad [13] \end{aligned}$$

   (a) Trouver un critère de divisibilité par 7 en base 20.

   (b) Trouver un critère de divisibilité par 13 en base 40.

5. Autre critère de divisibilité par 7.

   Montrer que si pour $N = \overline{a_na_{n-1}...a_0}$, on pose $b_0 = a_n$ et $b_k = 3b_{k-1} + a_{n-k}$ pour $k = 1..n$, alors $N \equiv b_n \quad [7]$; appliquer à 2012 et à 12345.

6. Encore un autre.

   (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 2015 et à 12345.

   (b) * Montrer que plus généralement si pour $N = \overline{a_na_{n-1}...a_0}$, on pose $b_0 = a_0$ et $b_k = -2b_{k-1} + a_k$ pour $k = 1..n$, alors $N \equiv 10^n b_n \quad [7]$.

   (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 2015 et à 12345, et trouver deux relations similaires à celle de (b).

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) $n\left(n^2-1\right)\left(4n^2-1\right)\left(9n^2-1\right)$ est multiple de 210.

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) $\forall n \in \mathbb{N}^* \quad 11 \left| \left(2^{6n-5} + 3^{2n}\right) \right.$ et $17 \left| \left(3 \times 5^{2n-1} + 2^{3n-2}\right) \right.$.

    (b) $\forall n \in \mathbb{N} \quad n^2 \left| \left((n+2)^{n+2} - 2^{n+2}\,(n+1)^{n+1}\right) \right.$.

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. * : Les entiers entre 1 et n ont en moyenne environ $\ln n$ diviseurs, à un près près (ou plus précisément, la moyenne du nombre de diviseurs des entiers de 1 à n est comprise entre $\ln n - 1$ et $\ln n + 1$)

    (a) Vérifier cette propriété pour $n = 10$.
    Pour deux entiers naturels i et j on pose $\delta(i,j) = 1$ si i divise j, et 0 sinon.

    (b) Pour un entier naturel n, que représente le nombre $d(n) = \sum_{i=1}^{n} \delta(i,n)$?

    (c) Montrer que $\sum_{j=i}^{n} \delta(i,j) = \left\lfloor \frac{n}{i} \right\rfloor$.

    (d) En déduire que $S(n) = \sum_{j=1}^{n} d(j)$ est compris entre $n(h_n - 1)$ et nh_n où $h_n = \sum_{i=1}^{n} \frac{1}{i}$.

    (e) En utilisant l'encadrement $\ln n \leqslant h_n \leqslant \ln n + 1$, montrer $\frac{S(n)}{n} \simeq \ln n \pm 1$.

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 $p\begin{pmatrix} n \\ p \end{pmatrix} = n\begin{pmatrix} n-1 \\ p-1 \end{pmatrix}$, montrer que pour $1 \leqslant p \leqslant n$, $\begin{pmatrix} n \\ p \end{pmatrix}$ est divisible par $\frac{n}{\operatorname{pgcd}(n,p)}$ et par $\frac{p+1}{\operatorname{pgcd}(n+1,p+1)}$; en déduire que $\begin{pmatrix} 2n \\ n \end{pmatrix}$ est pair et divisible par $n+1$.

15. : Montrer que si z est une racine $n^{ième}$ et $m^{ième}$ de l'unité, alors z est une racine $d^{ième}$ de l'unité avec $d = \operatorname{pgcd}(n,m)$.

16. * : On dit qu'une suite (u_n) est p-périodique si $u_n = u_{n+p}$ pour tout $n \in \mathbb{N}$ (p entier > 0).

    (a) Montrer que si (u_n) est à la fois p-périodique et q-périodique alors (u_n) est d-périodique avec $d = \operatorname{pgcd}(p,q)$.

    (b) En déduire que si p est la plus petite période $\geqslant 1$ 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 $\geqslant 0$ (u,v) tel que $au - bv = 1$ vérifiant $u < b$ et $v < a$.

    (b) En déduire que si a et b sont premiers entre eux, $a\mathbb{N} - b\mathbb{N} = \mathbb{Z}$.

    (c) 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 $aa' \equiv 1 \ [b]$; 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 une 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 le 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. :

(a) Montrer que si un carré a^2 divise un carré b^2 alors a divise b et $\dfrac{b^2}{a^2}$ est un carré.

(b) En déduire que si n est un entier naturel non carré alors $\sqrt{n} \notin \mathbb{Q}$.

(c) Généraliser (a) et (b) en remplaçant 2 par q entier $\geqslant 2$.

(d) * La généralisation complète.
Montrer que si n et m sont deux entiers > 0 premiers entre eux, r est un rationnel > 0 qui n'est pas la puissance n-ième d'un rationnel, alors $\sqrt[n]{r^m}$ n'est pas rationnel.

21. :

(a) Montrer l'unicité de la forme irréductible d'une fraction ; c'est-à-dire que si $\dfrac{a}{b} = \dfrac{c}{d}$ avec $a, b, c, d \in \mathbb{N}^*$, a et b premiers entre eux, c et d premiers entre eux, alors $a = c$ et $b = d$.

(b) En déduire que si $a, b \in \mathbb{N}^*$ avec a et b premiers entre eux, a ou b non carré, alors $\sqrt{\dfrac{a}{b}} \notin \mathbb{Q}$; généraliser à $\sqrt[n]{\dfrac{a}{b}}$.

22. Petit théorème de Fermat.

(a) Montrer que si p est premier et k est un entier entre 1 et $p-1$ alors $\begin{pmatrix} p \\ k \end{pmatrix}$ est multiple de p.

(b) En déduire que pour tout naturel n, $n^p \equiv n \quad [p]$.

23. Autre application du 22 a).
Soit (f_n) une suite d'entiers du type fibonaccien vérifiant pour tout naturel n : $f_{n+2} = f_{n+1} + f_n$.

(a) Montrer pour tous naturels n et p :
$$f_{n+2p} = \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} f_{n+k}$$

(b) En déduire que si p est premier, $f_{n+2p} - f_{n+p} - f_n$ est multiple de p pour tout naturel n.

24. Encore une autre application.
Soit (L_n) la suite dite de Lucas définie par $L_0 = 2, L_1 = 1$ et pour tout naturel n : $L_{n+2} = L_{n+1} + L_n$.

(a) Montrer que $L_n = \left(\dfrac{1+\sqrt{5}}{2}\right)^n + \left(\dfrac{1-\sqrt{5}}{2}\right)^n$.

(b) Déduire de a) et de 22 a) que si p est premier, alors $2^p L_p = 2 + 2pa$ où a est un entier.

(c) En déduire que $L_p \equiv 1$ [p].

25. On pose $P_n(x) = (x+1)\left(x^2+1\right)\left(x^4+1\right)\cdots\left(x^{2^n}+1\right)$;

(a) Simplifier $(x-1)\,P_n(x)$.

(b) En déduire la forme développée de $P_n(x)$.

(c) En déduire que si $F_n = 2^{2^n}+1$; $F_n = F_0F_1...F_{n-1}+2$; où F_n est le $n$ième nombre de Fermat.

(d) 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.

(e) En déduire une autre démonstration du fait qu'il y a un nombre infini de nombres premiers.

26. :

(a) Montrer que les $(n-1)$ entiers $n!+2,\ n!+3,\ ...,\ n!+n$ pour $n \geqslant 3$ sont tous composés ; en déduire qu'on peut trouver des listes d'entiers composés consécutifs aussi longues qu'on veut.

(b) On pose $n\# \overset{def}{=} \prod_{\substack{2 \leqslant p \leqslant n \\ p \text{ premier}}} p$ (*primorielle* de n) ; montrer que de nouveau les $(n-1)$ entiers $n\#+2,\ n\#+3,\ ...,\ n\#+n$ sont tous composés.

27. * :

(a) 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 : $N = 4p_1p_2...p_n+1$).

(b) Montrer de même qu'il existe une infinité de nombres premiers congrus à -1 modulo 6.
REM : le théorème de Dirichlet, bien plus difficile à démontrer, affirme que dans toute suite arithmétique dont la raison est première avec le premier terme, il existe une infinité de nombres premiers.

28. *: 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 :
$\mathcal{D}_a \times \mathcal{D}_b \to \mathcal{D}_{ab}$
$(d,d') \mapsto dd'$

(a) A quelle condition nécessaire et suffisante φ est-elle injective ?

(b) A quelle condition nécessaire et suffisante φ est-elle surjective ?

29. : Soit $n = \prod_{k=1}^{m} p_k^{\alpha_k}$ un naturel décomposé en produit de facteurs premiers.

(a) Montrer que le nombre de diviseurs de n est $N = \prod_{k=1}^{m} (\alpha_k+1)$.

(b) Que dire donc d'un entier naturel non nul ayant un nombre impair de diviseurs ?

(c) Montrer que la somme des diviseurs de n est $S = \prod_{k=1}^{m} \frac{p_k^{\alpha_k+1}-1}{p_k-1}$.

(d) * 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. $2 \leqslant N \leqslant 2\sqrt{n}$.

ii. $n+1 \leqslant S \leqslant (n+1)\sqrt{n}$

iii. $P = \sqrt{n}^N$.

iv. La somme des inverses des diviseurs de n est $\frac{S}{n}$.

30. : Nombres parfaits.

(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.

31. : Nombres amiables, formule de Thābit ibn Qurra (850).

Soit $p = 3.2^{n-1}-1, q = 3.2^n-1, r = 9.2^{2n-1}-1$ pour un entier $n \geqslant 1$; montrer que si p,q,r sont premiers, alors $a = 2^npq$ et $b = 2^nr$ forment une paire de nombres "amiables", ce qui signifie que la somme des diviseurs stricts de l'un est égale à l'autre.

Donner un exemple.

32. * : Par combien de zéros se termine 100! ?
Soient $n \in \mathbb{N}^* \setminus \{1\}$; $p \in \mathbb{P}$; $\alpha_p = v_p(n!)$ l'exposant de p dans la décomposition de $n!$ en produit de facteurs premiers.

(a) Que vaut α_p pour $p > n$?

(b) Pour $p \leqslant n$ on note n_1 le quotient de la division de n par p. Montrer que

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

En déduire un algorithme pour calculer α_p.

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

33. : 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.

34. : 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 $x_0, x_1, ..., x_{p-1}$ 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.

35. * : Désignons par $\pi(n)$ le nombre de nombres premiers $\leqslant n$. Il a été démontré que pour $n \geqslant 11$:

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

(a) Vérifier numériquement cette inégalité en calculant $\dfrac{\pi(n)}{\dfrac{n}{\ln n}}$ pour $11 \leqslant n \leqslant 100$ (calcul formel).

(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 $\pi(n) \sim \dfrac{n}{\ln n}$ (Théorème de Hadamard et de la Vallée Poussin).
REP : pour $n \geqslant 11$, $\pi(2n) > \pi(n)$ dès que $\dfrac{2n}{\ln 2n} > 1,3\dfrac{n}{\ln n}$ soit $2\ln n > 1,3(\ln n + \ln 2)$, soit $n > 2^{13/7}$ soit $n \geqslant 4$, ce qui est bien le cas.

36. *: Obtention d'un minorant de $\pi(n)$, légèrement moins bon que le $\dfrac{n}{\ln n}$ de l'exercice précédent, mais démontré (preuve de Tchebychev).

(a) On note $m_n = \text{ppcm}(1, 2, ..., n)$, et α l'exposant du nombre premier p dans la décomposition en produit de facteurs premiers de m_n.

i. Montrer que $p^\alpha \leqslant n < p^{\alpha+1}$.

ii. En déduire que $m_n = \prod_{p \text{ premier } \leqslant n} p^{\left\lfloor \frac{\ln n}{\ln p} \right\rfloor}$

iii. En déduire que $\pi(n) \geqslant \dfrac{\ln m_n}{\ln n}$; on va maintenant obtenir un minorant de m_n.

(b) Considérons $I_n = \int_0^1 t^n (1-t)^n \, dt$, pour $n \geqslant 0$.

i. Montrer que $I_n = \sum_{k=0}^{n} \frac{(-1)^k \binom{n}{k}}{n+k+1}$;

ii. En déduire que $\frac{1}{m_{2n+1}} \leqslant I_n$.

iii. Montrer que $I_n \leqslant \frac{1}{4^n}$.

iv. Montrer que pour $n \geqslant 2$, $m_n \geqslant 2^{n-2}$.

(c) Montrer l'inégalité annoncée : $\pi(n) \geqslant \ln 2 \frac{n-2}{\ln n}$.

37. * : Majoration de $n\#$ (*primorielle* de n).

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

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

(b) En déduire par récurrence forte que $n\# \overset{def}{=} \prod_{2 \leqslant p \leqslant n} p \leqslant 4^n$ (démonstration dûe à Paul Erdös, 1932). On peut démontrer qu'en fait $n\# = e^{n+o(n)}$.