Arithmétique et Algèbre

Université d'Eleuthéria-Polites

Exercices

Bruno Deschamps

Arithmétique des entiers

Exercice 1.— Pour un réel x donné, on appelle *partie entière* (resp. *partie décimale*) de x l'entier noté $[x]$ (resp. le réel élément de $[0,1[$ noté $\{x\}$) et défini comme étant le plus grand entier relatif inférieur à x (resp. l'entier égal à $x-[x]$). Montrer les propositions suivantes :

a) $x=[x]+\{x\}$ et, réciproquement, si $n\in\mathbb{Z}$ et $d\in[0,1[$ sont tels que $x=n+d$ alors $n=[x]$ et $d=\{x\}$.

b) $[x]\leq x<[x]+1$ et, réciproquement, si $n\in\mathbb{Z}$ est tel que $n\leq x<n+1$ alors $n=[x]$.

b') $x-1<[x]\leq x$ et, réciproquement, si $n\in\mathbb{Z}$ est tel que $x-1<n\leq x$ alors $n=[x]$.

c) Si x est entier alors $[x]=x$ et $\{x\}=0$, et, réciproquement, si l'une de ces deux égalités est vérifiée, alors x est entier.

d) $[-x]=-[x]-1$ sauf si x est entier, auquel cas $[-x]=-[x]$.

e) $[x]+[y]\leq[x+y]\leq[x]+[y]+1$.

f) Si $m,x\geq 1$ sont des réels, alors il y a exactement $[x/m]$ multiples de m compris entre 1 et x.

g) Soient $x<y$ deux réels non entiers. Montrer que $[x]=[y]$ si et seulement si, il n'existe pas d'entier dans l'intervalle $]x,y[$.

h) Soient $x\in\mathbb{R}$ et $n\in\mathbb{Z}$, montrer que $[n+x]=n+[x]$.

Exercice 2.— (Théorème de Beatty) Pour un réel $\lambda > 0$, on considère l'ensemble

$$S_\lambda = \{[n\lambda] / \ n \in \mathbb{N}^*\}$$

0/ a) Montrer que $S_\lambda \subset \mathbb{N}^*$ si et seulement si $\lambda \geq 1$.

b) Montrer que si $\lambda < 1$ alors $S_\lambda = \mathbb{N}$.

c) Montrer que si $\lambda \geq 1$ alors, pour tout $n, m \in \mathbb{N}^*$ on a $[n\lambda] = [m\lambda] \Longleftrightarrow n = m$.

d) Soient $\lambda, \mu \geq 1$, montrer que $S_\lambda = S_\mu \Longleftrightarrow \lambda = \mu$.

1/ a) On suppose dans cette question que λ est irrationnel et l'on considère un entier $k > 0$. Montrer que $k \in S_\lambda$ si et seulement si, il existe un entier $n \in \left]\dfrac{k}{\lambda}, \dfrac{k+1}{\lambda}\right[$.

b) En déduire que si α et β sont des réels irrationnels strictement positifs vérifiant $\dfrac{1}{\alpha} + \dfrac{1}{\beta} = 1$ alors les ensembles S_α et S_β forment une partition de $\mathbb{N}^*$.

2/ On suppose dans cette question donnés deux réels α et β tels que les ensembles S_α et S_β forment une partition de $\mathbb{N}^*$.

a) En dénombrant, pour un entier $k \geq 2$ donné, les éléments de l'ensemble $\{1, \cdots, k-1\}$, montrer que $k - 1 \leq \left[\dfrac{k}{\alpha}\right] + \left[\dfrac{k}{\beta}\right] \leq k + 1$. En déduire, en faisant tendre k vers l'infini, que $\dfrac{1}{\alpha} + \dfrac{1}{\beta} = 1$.

b) En raisonnant par l'absurde, montrer que α et β sont irrationnels.

3/ On fixe un entier $\ell \geq 1$. Montrer qu'il existe une et une seule suite strictement croissante d'entiers non nuls $(u_n)_{n \geq 1}$ telle que, si l'on pose $v_n = n\ell + u_n$ pour tout $n \geq 1$, $U = \{u_n / \ n \geq 1\}$ et $V = \{u_n / \ n \geq 1\}$, alors $\complement_{\mathbb{N}^*} U = V$ et décrire cette partie grâce à ce qui précède. Etudier plus particulièrement le cas $\ell = 1$.

Exercice 3.— Pour $n \geq 0$ entier, calculer explicitement

$$\sum_{k \geq 0} \left[\frac{n + 2^k}{2^{k+1}}\right] = \left[\frac{n+1}{2}\right] + \left[\frac{n+2}{4}\right] + \left[\frac{n+4}{8}\right] + \cdots$$

(Ind. On pourra commencer par montrer que, pour tout réel x, on a $[2x] = [x] + [x + 1/2]$.)

Exercice 3 bis.— On se donne un entier $n \geq 2$ et un réel x. Montrer que

$$[nx] = \sum_{k=0}^{n-1} [x + k/n]$$

Exercice 3 ter.— On se donne un entier $n \geq 1$ et un réel x. Montrer que

$$\left[\frac{[nx]}{n}\right] = [x]$$

Exercice 4.— 1/ On se donne un entier $a \geq 0$ et, pour tout entier $n \geq 1$, on pose

$$Q_a(n) = \sum_{h=1}^{n} h^a = 1^a + 2^a + 3^a + \cdots + n^a$$

a) Prouver que, pour tout entier $h \geq 1$, on a $Q_{a+1}(h+1) - Q_{a+1}(h) = h^{a+1} + \sum_{i=0}^{a} C_{a+1}^i h^i$, et en déduire que

$$\sum_{i=0}^{a} C_{a+1}^i Q_i(n) = (n+1)^{a+1} - 1$$

Expliquer alors comment on peut calculer, par récurrence sur a, les valeurs $Q_a(n)$.

b) Donner des expressions polynomiales factorisées en n pour $Q_0(n), Q_1(n), Q_2(n), Q_3(n)$ et $Q_4(n)$.

2/ On se donne un nombre premier p et un entier $n \geq 0$. On souhaite calculer

$$S_n = \sum_{k=1}^{p-1} \left[\frac{k^{2n+1}}{p} \right]$$

Pour tout entier $i \geq 0$, on note $Q_i = Q_i(p-1)$.

a) En remarquant que $S_n = \sum_{k=1}^{p-1} \left[\frac{(p-k)^{2n+1}}{p} \right]$, montrer que $2S_n = 1 - p + \sum_{i=0}^{2n} (-1)^i C_{2n+1}^i p^{2n-i} Q_i$.

b) Calculer explicitement S_0, S_1 et S_2 en fonction de p.

Exercice 5.— a) Montrer que le reste de la division euclidienne par 8 du carré de tout nombre impair est 1.

b) Montrer de même que tout nombre pair vérifie $x^2 \equiv 0, 4 \bmod(8)$.

c) Soient a, b, c trois entiers impairs. Déterminer le reste modulo 8 de $a^2 + b^2 + c^2$ et celui de $2(ab + ac + bc)$. En déduire que ces deux nombres ne sont pas des carrés puis que $ab + bc + ca$ non plus.

Exercice 6.— Soient $a \geq 2$ et $n \geq 1$ tel que $a^n + 1$ soit premier. Montrer que n est en fait une puissance de 2.

Exercice 7.— Soient a et n deux entiers ≥ 1. Montrer que $\sqrt[n]{a}$ est, soit entier, soit irrationnel.

Exercice 8.— Montrer que, pour tout entier $k \geq 0$, il existe des entiers n tel qu'il n'existe aucun nombre premier dans l'intervalle $[n, n+k]$.

Exercice 9.— En s'inspirant de la preuve d'Euclide de l'infinitude de l'ensemble des nombres premiers, montrer qu'il existe une infinité de nombre premier congru à -1 modulo 4.

Exercice 10.— Soient $n \geq 2$ un entier et $a, b \geq 1$ deux entiers

a) Soit $b = aq + r$ la division euclidienne de b par a. Donner le quotient et le reste de la division euclidienne de $n^b - 1$ par $n^a - 1$ en fonction de q et r. En déduire que les propositions suivantes

i) $a|b$,

ii) $(n^a - 1)|(n^b - 1)$,

sont équivalentes.

b) Soit $d > 0$. Montrer que les propositions suivantes

i) $d = (a, b)$,

ii) $n^d - 1 = (n^a - 1, n^b - 1)$,

sont équivalentes.

Exercice 11.— Soient a et b deux entiers non nuls. Montrer que a et b sont premiers entre eux si et seulement si les entiers ab et $(a + b)$ le sont aussi.

Exercice 12.— Pour tout entier $n \geq 1$, on pose $s_n = \sum_{k=1}^{n} k^3$.

o) Montrer, par récurrence sur l'entier $n \geq 1$, que $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

1) Montrer, par récurrence sur l'entier $n \geq 1$, que $s_n = \left(\sum_{k=1}^{n} k\right)^2$. En déduire une expression simple de s_n en fonction de n.

2) Pour $n \geq 1$ on pose $d_n = \text{pgcd}(s_n, s_{n+1})$. Calculer d_n en distinguant le cas n pair du cas n impair.

3) Prouver finalement que, pour tout $n \geq 1$, $\text{pgcd}(s_n, s_{n+1}, s_{n+2}) = 1$.

Exercice 13.— a) Soient $p \geq 1$ un entier et, pour tout $i = 1, \cdots, n$, un entier non nul a_i premier avec p. Montrer que l'entier $A = a_1.\cdots.a_n$ est premier avec p.

b) En déduire que si p est un nombre premier alors p divise le coefficient binomial

$$C_p^i = \frac{p(p-1)\cdots(p-i+1)}{i(i-1)\cdots 1}$$

pour tout $i = 1, \cdots, p-1$.

(Ind. On pourra utiliser le lemme de Gauss.)

c) Prouver alors que, pour tout $a \in \mathbb{N}$ et tout p premier, on a $a^p \equiv a \bmod(p)$ (Petit théorème de Fermat).

Exercice 14.— (Fractions égyptiennes)

1/ Soit $\ell \geq 1$ un entier et $c > 0$ un réel. Montrer que l'ensemble

$$\left\{(x_1, \cdots, x_\ell) \in \mathbb{N}^{*\ell} / \ \frac{1}{x_1} + \cdots + \frac{1}{x_\ell} = c\right\}$$

est fini.

2/ a) Soient $x, y, z \geq 1$ trois entiers. Montrer que $\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$ si et seulement si, il existe trois entiers $u, v, w \geq 1$ avec $(u, v) = 1$ tels que

$$\begin{cases} x &= u(u+v)w \\ y &= v(u+v)w \\ z &= uvw \end{cases}$$

b) On considère $u, v, w, u', v', w' \geq 1$ six entiers tels que $uvw = u'v'w'$ et tels que $(u, v) = (u', v') = 1$. Montrer que

$$\begin{cases} u(u+v)w = u'(u'+v')w' \\ v(u+v)w = v'(u'+v')w' \end{cases} \iff u = u',\ v = v',\ w = w'$$

c) En déduire que, si $n \geq 1$ est un entier dont la décomposition en facteurs premiers est $n = p_1^{e_1} \cdots p_k^{e_k}$, alors l'ensemble

$$\left\{(x, y) \in \mathbb{N}^{*2} / \ \frac{1}{x} + \frac{1}{y} = \frac{1}{n}\right\}$$

contient exactement $1 + \sum_{i=1}^{k} 2^i \sigma_i(e_1, \cdots, e_k)$ où les σ_i désignent les fonctions symétriques élémentaires d'ordre k.

Exercice 15.— A/ (Triplets pythagoriciens) Un triplet d'entiers $(x, y, z) \in \mathbb{N}^{*3}$ est dit *pythagoricien* si $x^2 + y^2 = z^2$. On dira d'un triplet pyhtagoricien (x, y, z) qu'il est primitif si en plus $\text{pgcd}(x, y, z) = 1$.

1.— Expliquer comment la recherche des triplets pythagoriciens se ramène à la recherche des triplets pythagoriciens primitifs.

2.— On suppose dans cette question que (x, y, z) est un triplet pyhtagoricien primitif.

2.a.— Montrer que les entiers x, y, z sont en fait premiers entre eux deux à deux.

2.b.— En raisonnant par l'absurde, montrer que z est nécessairement impair. En déduire que x et y sont de parités différentes.

2.c.— Montrer que si x est impair alors les entiers $z-y$ et $z+y$ sont premiers entre eux. En déduire que chacun de ces entiers est un carré.

3.— Montrer que les triplets pyhtagoriciens primitifs (x,y,z) tels que x soit impair et y soit pair, sont exactement les entiers de la forme

$$x = kl,\ y = \frac{k^2 - l^2}{2},\ z = \frac{k^2 + l^2}{2}$$

où k et l sont deux entiers impairs premiers entre eux tels que $k > l$. Donner alors trois exemples de triplets pythagoriciens primitifs.

4.— Montrer que les triplets pyhtagoriciens primitifs (x,y,z) tels que x soit pair et y soit impair, sont exactement les entiers de la forme

$$x = 2nm,\ y = m^2 - n^2,\ z = m^2 + n^2$$

où n et m sont deux entiers premiers entre eux et de parités différentes tels que $m > n$.

B/ (L'équation $X^{4h} + Y^{4h} = Z^{4h}$)

1.— On souhaite montrer dans cette question que si x, y et z sojt trois entiers tel que $x^4 + y^4 = z^2$ alors au moins un de ces entiers est nul (i.e. $xyz = 0$). On raisonne par l'absurde en supposant l'existence d'un triplet $(x,y,z) \in \mathbb{N}^3$ tel que $x^4 + y^4 = z^2$ et $xyz \neq 0$.

1.a.— Montrer que l'on peut choisir le triplet (x,y,z) de sorte que z soit minimal, c'est-à-dire que si $(x',y',z') \in \mathbb{N}^3$ désigne un triplet tel que $x'^4 + y'^4 = z'^2$ et $x'y'z' \neq 0$ alors $z' \geq z$.

1.b.— Montrer que x et y sont premiers entre eux et en déduire que (x^2, y^2, z) est un triplet pythagoricien primitif.

Quitte à intervertir le rôle de x et de y on va supposer dans la suite que x^2 est pair. Il existe donc deux entiers premiers entre eux n et m de parités différentes tels que $m > n$ et $x^2 = 2nm$, $y^2 = m^2 - n^2$, $z = m^2 + n^2$.

1.c.— Montrer qu'il existe deux entiers $p > q$ premiers entre eux et de parités différentes tels que $n = 2pq$, $y = p^2 - q^2$ et $m = p^2 + q^2$.

1.d.— Montrer que m, p et q sont des carrés et, en écrivant $m = z'^2$, $p = x'^2$ et $q = y'^2$, montrer que $x'^4 + y'^4 = z'^2$. En déduire une absurdité.

2.— Soient $h \geq 1$ un entier et $n = 4h$. Montrer que si $(x,y,z) \in \mathbb{N}^3$ est solution de l'équation

$$X^n + Y^n = Z^n$$

alors $xyz = 0$. En déduire toutes les solutions entières de cette équation.

Exercice 16.— 1) Soient $x, y \in \mathbb{R}$. Montrer, par récurrence sur l'entier $n \geq 1$, que

$$x^n - y^n = (x-y).\sum_{k=0}^{n-1} x^k y^{n-1-k}$$

2) Soient a, b, p des entiers naturels non nuls.

a) Montrer que s'il existe un entier $l \in \mathbb{N}$ tel que $b = a + pl$, alors pour tout $h \in \mathbb{N}$, il existe un entier $m_h \in \mathbb{N}$ tel que $b^h = a^h + pm_h$.

b) En déduire que si $a - b$ est divisible par p, alors l'entier $\sum_{k=0}^{p-1} a^k b^{p-1-k}$ l'est aussi.

c) Prouver finalement que si $a - b$ est divisible par p^n pour un certain entier $n \geq 1$, alors $a^p - b^p$ est divisible par p^{n+1}.

Exercice 17.— (Autour de la série harmonique) On considère, pour tout $n \geq 1$, le réel

$$H(n) = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

1/ Montrer que la suite $(H(n))_n$ tend vers $+\infty$.

2/ Prouver que, pour tout $n \geq 1$, $v_2(H(n)) = -r$ où r est le plus grand entier tel que $2^r \leq n$. En déduire que $H(n)$ n'est entier que pour $n = 1$.

3/ On fixe un entier $m \geq 1$ et pour tout $n \geq 0$, on pose $u_n = H(m+n) - H(m)$ et $a_n = v_2(u_n)$.

a) Montrer que $a_n = -\max_{1 \leq k \leq n} v_2(m+k)$.

b) En déduire toutes les valeurs de n et m pour lesquelles $H(m+n) - H(m)$ est entier.

4/ Soit $p \geq 3$ un nombre premier. On écrit

$$H(p-1) = 1 + \frac{1}{2} + \cdots + \frac{1}{p-1} = \frac{a}{b}$$

où a et b sont premiers entre eux. Montrer que p divise a.

5/ (Théorème de Wolstenholme)

a) Pour $n \geq 1$, expliciter le polynôme $P_n(x) = \sum_{k=0}^{n-1} \frac{(-1)^{k+1}}{k+1} C_n^k x^{k+1}$. En déduire la valeur de $\sum_{k=0}^{n-1} \frac{(-1)^{k+1}}{k+1} C_n^k$.

b) Montrer que, pour tout $n \geq 1$, on a $H(n) = \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k} C_n^k$.

(Ind. On pourra étudier la quantité $H(n+1) - H(n)$ et utiliser la question précédente.)

c) Montrer que si $n \geq 3$ désigne un entier impair alors

$$2H(n-1) = \sum_{k=1}^{n-1} (-1)^{k+1} \frac{(n-1)!}{k!(n-k)!} \frac{n(n-2k)}{k(n-k)}$$

d) On suppose désormais que $n = p \geq 3$ est un nombre premier. Montrer qu'il existe un entier λ tel que

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

e) Montrer que, pour tout $k = 1, \cdots, p-1$, on a $(p-1)\cdots(p-k+1) \equiv (-1)^{k+1}(k-1)! \bmod(p)$. En déduire qu'il existe un entier λ_k tel que

$$\frac{(p-1)!}{k!(p-k)!} = \frac{\lambda_k p}{k!} + \frac{(-1)^{k+1}}{k}$$

f) En déduire qu'il existe un entier μ tel que

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

et montrer alors qu'il existe un entier M tel que

$$6H(p-1) = \frac{M p^2}{(p-1)!}$$

f) Prouver finalement que si $p \geq 5$ désigne un nombre premier et si $H(p-1) = 1 + \frac{1}{2} + \cdots + \frac{1}{p-1} = \frac{a}{b}$ où a et b sont premiers entre eux alors p^2 divise a (ce théorème généralise le 4/).

6/ Pour $n \geq 1$, on pose $H(n) = \dfrac{a(n)}{b(n)}$ où $a(n)$ et $b(n)$ sont deux entiers positifs premiers entre eux. On veut montrer qu'il existe une infinité d'entiers n pour lesquels $a(n)$ n'est pas une puissance d'un nombre premier. On raisonne par l'absurde et l'on suppose l'existence d'un entier $N \geq 1$ tel que, pour tout $n \geq N$, $a(n)$ est la puissance d'un nombre premier.

a) En utilisant le 2/, montrer que, pour tout $n \geq 1$, on a $b(n) > n/2$.

b) En utilisant le 4/et le 1/, montrer qu'il existe un rang $N_0 \geq N$ tel que, pour tout nombre premier $p \geq N_0$, l'entier $a(p-1)$ est une puissance au moins carrée de p.

c) Soit $p \geq N_0$ un nombre premier. Montrer, par récurrence sur l'entier $k \geq 1$, que l'entier $a(p^k - 1)$ est une puissance au moins carrée de p.

(Ind. On pourra remarquer que $H(p^{k+1}-1) = \dfrac{H(p^k-1)}{p} + \displaystyle\sum_{q=1}^{p^k-1}\sum_{r=1}^{p-1} \frac{1}{pq+r}$.)

d) En déduire que $a(p^k - p)$ est aussi divisible par p pour tout $k \geq 2$.

(Ind. On pourra remarquer que $H(p^k - p) = H(p^k - 1) - \displaystyle\sum_{r=1}^{p-1} \frac{1}{p^k - r}$.)

e) On choisit un premier $p \geq N_0$, un entier $n \geq 1$ tel que p^n ne divise pas $a(p-1)$ et un entier $k > n$ tel que $p^k - p > 2p^n$. On écrit

$$H(p^k - 1) - H(p^k - p) = \frac{1}{p^k - 1} + \cdots + \frac{1}{p^k - p + 1} = \frac{a}{b}$$

avec a et b des entiers premiers entre eux.

i) Montrer que $p^n | a$.

ii) Montrer que $a(p-1) \equiv a \bmod(p^k)$.

iii) Conclure.

Exercice 18.— (Nombres de Fermat.)

1) Soit $m \geq 2$ un entier.

a) On suppose que m possède un diviseur impair $q \geq 3$ et l'on pose $m = kq$. Montrer que l'entier $(2^k + 1)$ est un diviseur de l'entier $2^m + 1$.

b) En déduire que si $2^m + 1$ est un nombre premier alors a est pair et m est une puissance de 2.

2) Le n-ième nombre de Fermat est, par définition, l'entier $F_n = 2^{2^n} + 1$.

a) Vérifier que F_n est un nombre premier pour $n = 0, \cdots, 4$.

b) Montrer que, pour tout entier $n \geq 0$, $F_{n+1} = (F_n - 1)^2 + 1$.

c) En déduire que, pour tout entier $n \geq 2$, le chiffre des unités de F_n est 7.

d) En déduire aussi que, pour tout entier $n \geq 1$, $F_n - 2 = \prod_{k=0}^{n-1} F_k$.

e) Prouver alors que si $n \neq m$ sont deux entiers, les entiers F_n et F_m sont premiers entre eux.

3) Soit p un nombre premier et $a \geq 2$ un entier tel qu'il existe un entier $k \geq 1$ vérifiant : $a^k \equiv 1 \bmod(p)$. On considère alors k_0 le plus petit de ces entiers $k \geq 1$. Montrer que si $k \geq 1$ vérifie $a^k \equiv 1 \bmod(p)$ alors $k_0 | k$.
(Indication. On pourra considérer la division euclidienne de k par k_0.)

4) On se donne un entier $n \geq 1$ et un nombre premier $p \neq F_n$ divisant F_n.

a) Montrer que $2^{p-1} \equiv 1 \bmod(p)$.

b) Montrer que $2^{2^{n+1}} \equiv 1 \bmod(p)$ et que $k_0 = 2^{n+1}$ est le plus petit entier k tel que $2^k \equiv 1 \bmod(p)$.

c) En déduire que $p = h2^{n+1} + 1$ où $h \geq 1$ possède un diviseur impair ≥ 3.

5) a) Montrer que les diviseurs premiers éventuels de F_5 sont de la forme $p = 64h + 1$ où $h = 3, 5, 6, 7, 9, 10, \cdots$ est un entier qui possède un diviseur impair ≥ 3.

b) Tenter sa chance avec $h = 10$.

Exercice 19.— a) Montrer que pour tout $n \geq 0$ et tout $k \geq 1$, on a

$$2^{2^{n+k}} - 1 = \left(2^{2^n} - 1\right) \prod_{i=0}^{k-1} \left(2^{2^{n+i}} + 1\right)$$

b) Pour tout entier $n \geq 0$, on pose $F_n = 2^{2^n} + 1$ (n-ième nombre de Fermat). Montrer que pour $n \neq m$, F_n et F_m sont premiers entre eux.

c) En déduire une nouvelle preuve de l'infinitude de l'ensemble des nombres premiers.

Exercice 20.— (Ecriture en base) On considère une suite d'entiers $(n_k)_{k \geq 0}$ telle que $n_0 = 1$ et $n_k \geq 2$ pour tout $k \geq 1$.

a) Montrer que, pour tout entier $m \geq 1$, il existe un unique indice $k_0 \geq 0$ et une unique suite finie d'entiers $a_0, \cdots, a_{k_0}$ telle que $a_i \in \{0, \cdots, n_{i+1} - 1\}$ pour tout $i = 0, \cdots, k_0$ et $a_{k_0} \neq 0$ et telle que

$$m = a_0 n_0 + a_1 n_0 n_1 + \cdots + a_{k_0} n_0 n_1 \cdots n_{k_0}$$

b) Enoncé le résultat précédent lorsque la suite $(n_k)_{k \geq 0}$ est constante égale à un entier $b \geq 2$ pour $k \geq 1$.

Exercice 21.— Calculer le pgcd des entiers $2^{445} + 7$ et 15.

Exercice 22.— Le but de cet exercice est de chercher les triplets d'entiers (a, b, k) avec $k \geq 0$, $a \geq b \geq 1$ vérifiant l'équation

$$(E) \quad 2^k = a^2 + b^2$$

1/ Soient $a, b \in \mathbb{Z}$ et $N = a^2 + b^2$. En étudiant le congruence de N modulo 4 montrer que si N est un multiple de 4, alors a et b sont pairs.

2/ En déduire, par exemple en opérant une récurrence, que pour tout entier $n \geq 0$, l'équation (E) ne possède pas de solution avec $k = 2n$.

3/ Montrer que pour tout entier $n \geq 0$, l'équation (E) possède une unique solution avec $k = 2n + 1$.

Exercice 23.— (Critères de divisibilité)

1/ On considère les écritures en base 10. Montrer qu'un entier est divisible par

a) 10 si et seulement s'il se termine par 0.

b) 5 si et seulement s'il se termine par 0 ou 5.

c) 2 si et seulement s'il se termine par un 0, 2, 4, 6 ou 8.

d) 3 (resp. 9) si et seulement si la somme de ses chiffres l'est aussi.

e) 4 si l'entier formé par ses deux derniers chiffres l'est aussi.

f) 11 si la somme de ses chiffres de rang pair diminuée de la somme de ses chiffres de rang impair est divisible par 11.

2/ On considère les écritures en base $b \geq 2$.

a) Montrer que si d divise b, alors un entier est divisible par d si et seulement si le dernier chiffre de son écriture en base b est lui-même divisible par d.

b) Montrer que si d divise $b - 1$, alors un entier est divisible par d si et seulement si la somme des chiffres de son écriture en base b est elle-même divisible par d.

Exercice 24.— Le but de cet exercice est de démontrer que $\sqrt{2}$ est irrationnel en utilisant l'algorithme d'Euclide. On raisonne par l'absurde et on suppose qu'il existe deux entiers strictement positifs a et b tels que $\sqrt{2} = a/b$. On pose $c = \sqrt{2} + 1$.

a) Vérifier que $a = b + \frac{b}{c}$, puis que $c = 2 + \frac{1}{c}$.

b) Démontrer que b/c est un entier, et qu'il est égal au reste r_1 de la division euclidienne de a par b. Quel est le quotient q_1 de cette division ?

c) Montrer que, dans la division euclidienne de b par r_1, le quotient est $q_2 = 2$ et le reste est $r_2 = r_1/c$.

c) Soit n un entier supérieur ou égal à 2. Démontrer que l'algorithme d'Euclide appliqué au couple (a, b) comporte au moins n étapes, que le n-ième quotient est $q_n = 2$, et que le n-ième reste est $r_n = r_{n-1}/c$. Conclure.

Exercice 25.— (Autour de l'algorithme d'Euclide) Pour a, b deux entiers naturels non nuls, on note $r_0 > r_1 > \cdots > r_{N(a,b)}$ la suite des restes de l'algorithme d'Euclide pour a et b.

I) a) Montrer que, pour tout pour tout $i \in \{0, \cdots, N(a,b) - 2\}$, on a $r_{i+2} < \dfrac{r_i}{2}$.

b) En déduire que $N(a,b) < 2\log_2 b + 1$.

II) a) Que représente l'entier $r_{N(a,b)}$ pour le couple (a, b)?

b) Comparer $N(b,a)$ et $N(a,b)$.

c) Soit $a = bq + r$ la division euclidienne de a par b. Expliciter $N(b,r)$ en fonction de $N(a,b)$ quand $r \neq 0$.

d) Prouver que si a' désigne un entier strictement positif tel que $a \equiv a' \bmod(b)$ alors $N(a,b) = N(a',b)$.

e) Expliquer comment, grâce aux questions précédentes on peut, sans faire le calcul, dresser le tableau à double entrées des valeurs de $N(a,b)$ pour $a, b \in \mathbb{N}^*$. Dresser ce tableau pour $a, b \in \{1, \cdots, 10\}$.

III) On considère dans cette question la suite $(F_n)_n$ récurrente linéaire d'ordre 2 (dite de Fibonacci[1]) définie par $F_0 = 1$, $F_1 = 2$ et pour tout $n \geq 0$,

$$F_{n+2} = F_{n+1} + F_n$$

1) a) Donner l'expression explicite de la suite $(F_n)_n$ en fonction du nombre d'or $\omega = \dfrac{1+\sqrt{5}}{2}$ et de son conjugué algébrique $\widetilde{\omega} = \dfrac{1-\sqrt{5}}{2}$. En déduire un équivalent simple de la suite $(F_n)_n$ en fonction de ω.

b) Montrer que pour tout $n \geq 0$ on a $1 - \left(\dfrac{\widetilde{\omega}}{\omega}\right)^2 \leq \dfrac{\sqrt{5}F_n}{\omega^{n+2}} \leq 1 - \left(\dfrac{\widetilde{\omega}}{\omega}\right)^3$ et en déduire que pour tout $n \geq 0$ on a $\mathrm{E}(\log_\omega F_n) = n$.

2) Montrer que pour tout $n \geq 0$, les entiers F_n et F_{n+1} sont premiers entre eux.

3) On pose $N = N(a,b)$. Si $(r_n)_{0 \leq n \leq N}$ désigne la suite finie des restes de l'algorithme d'Euclide appliqué au couple (a, b), on note $(\bar{r}_n)_{0 \leq n \leq N}$ la suite finie définie par $\bar{r}_0 = r_N$, $\bar{r}_1 = r_{N-1}, \cdots, \bar{r}_N = r_0$.

a) Montrer que pour tout $n = 0, \cdots, N$ on a $F_n \leq \bar{r}_n$.

b) Montrer que $N(a,b) \leq \log_\omega b$ et comparer ce résultat avec ceux précédemment établis.

c) Pour tout $n \geq 0$, évaluer explicitement en fonction de n l'entier $N(F_{n+1}, F_n)$.

d) En déduire qu'il existe une infinité d'entiers $b > 0$ tels qu'il existe des entiers $a > 0$ vérifiant $N(a,b) > \log_\omega b - 1$.

Exercice 26.— On considère la suite de Fibonacci $(F_n)_n$ (voir exercice 25).

[1] Leonardo Pisano dit *Fibonacci*, mathématicien italien, 1175 (Pise?) - 1240 (Pise?)

a) Montrer que, pour tout $n \geq 1$, on a $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$. En déduire que $\text{pgcd}(F_n, F_{n+1}) = 1$. Retrouver ce résultat en utilisant l'algorithme d'Euclide.

b) Montrer que, pour tout $n \geq 0$ et tout $m \geq 1$, on a $F_{n+m} = F_m F_{n+1} + F_{m-1}F_n$. En déduire que $\text{pgcd}(F_n, F_{m+n}) = \text{pgcd}(F_n, F_m)$ puis que, $\text{pgcd}(F_n, F_m) = \text{pgcd}(F_n, F_r)$ où r est le reste de la division euclidienne de m par n.

c) Prouver finalement que $\text{pgcd}(F_n, F_m) = F_{\text{pgcd}(n,m)}$.

Exercice 27.— (Théorème des quatre carrés) L'objet de cet exercice est de montrer la théorème suivant, conjecturé par Claude-Gaspard Bachet de Méziriac en 1621 et démontré par Joseph Louis Lagrange en 1770 : *tout entier positif est somme de quatre carrés.*

1/ a) Montrer que pour $x_1, \cdots, x_4, y_1, \cdots, y_4 \in \mathbb{Z}$ on a la relation (dite d'Euler) suivante :

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) &= (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 + (x_1y_2-x_2y_1+x_4y_3-x_3y_4)^2 \\ &\quad +(x_1y_3-x_3y_1+x_2y_4-x_4y_2)^2 + (x_1y_4-x_4y_1+x_3y_2-x_2y_3)^2.\end{aligned}$$

b) En déduire que pour montrer le théorème des quatre carrés, il suffit de montrer que tout nombre premier p est somme de quatre carrés. Le montrer pour $p = 2$.

2/ On considère un nombre premier impair p.

a) Soient $a, b \in \{0, \cdots, \frac{(p-1)}{2}\}$ tels que $a \not\equiv b \bmod(p)$, montrer que $a^2 \not\equiv b^2 \bmod(p)$.

b) Soient $a, b \in \{0, \cdots, \frac{(p-1)}{2}\}$ tels que $a \not\equiv b \bmod(p)$, montrer que $-a^2 - 1 \not\equiv -b^2 - 1 \bmod(p)$.

c) En déduire qu'il existe deux entiers u et v et un entier $0 < n < p$ tels que $np = 1 + u^2 + v^2$.

3/ On considère un nombre premier impair p.

a) Montrer qu'il existe un plus petit entier $m \geq 1$ tel que $mp = x_1^2+x_2^2+x_3^2+x_4^2$ (pour $x_1, x_2, x_3, x_4 \in \mathbb{Z}$) et que $m < p$. On suppose dans la suite que $m \neq 1$.

b) Pour $i = 1, \cdots, 4$, l'on considère l'unique entier $y_i \in [\frac{-m+1}{2}, \frac{m}{2}]$ tel que $y_i \equiv x_i \bmod(m)$. Montrer que $y_1^2 + y_2^2 + y_3^2 + y_4^2 = mr$ où r est un entier tel que $0 < r < m$.

c) Montrer que l'on a $mpmr = z_1^2 + z_2^2 + z_3^2 + z_4^2$ où les entiers z_i sont divisibles par m, pour tout $i = 1, \cdots, 4$.

d) En déduire $m = 1$ et donc que p est somme de quatre carrés.

Exercice 28.— (Formule de Legendre) On considère un entier $n \geq 2$ et un nombre premier p. Pour tout entier $k \geq 0$, on considère les sous-ensembles finis U_k, V_k et Ω_k de $\mathbb{N}$ définis par

$$\begin{aligned}U_k &= \{a \in \{1, \cdots, n\} / \ p^k \text{ divise } a\} \\ V_k &= \{a \in \{1, \cdots, n\} / \ p^k \text{ ne divise pas } a\} \\ \Omega_k &= \{a \in \{1, \cdots, n\} / \ v_p(a) = k\}\end{aligned}$$

1) Justifier qu'il existe un plus petit entier $k_0 \geq 0$ tel que $n < p^{k_0}$. Montrer que $k_0 \geq 1$ et expliciter k_0 en fonction de n et p.

2) a) Montrer que, pour tout $k \in \{0, \cdots, k_0 - 1\}$, l'ensemble U_{k+1} est strictement inclus dans U_k et que pour $k \geq k_0$ on a $U_k = \emptyset$.

b) Montrer que, pour tout $k \in \{0, \cdots, k_0 - 1\}$, l'ensemble V_k est strictement inclus dans V_{k+1} et que pour $k \geq k_0$ on a $V_k = \{1, \cdots, n\}$.

c) Prouver que la famille de parties $\{\Omega_0, \cdots, \Omega_{k_0-1}\}$ forme une partition de l'ensemble $\{1, \cdots, n\}$.

3) a) Pour tout $k \geq 0$, établir une relation ensembliste entre Ω_k, U_k et V_{k+1}.

b) Calculer, pour tout $k \geq 0$, $\sharp U_k$ et $\sharp V_k$ puis $\sharp \Omega_k$ en fonction de n, p.

4) Montrer que, $v_p(n!) = \sum_{k\geq 0} k.\sharp\Omega_k$ et en déduire que

$$v_p(n!) = \sum_{k\geq 1}\left[\frac{n}{p^k}\right]$$

5) Montrer que, pour tout entier $n \neq 2$ et tout premier p, on a $\left[\frac{n}{p}\right] \leq v_p(n!) \leq \left[\frac{n-1}{p-1}\right]$ et que

$$\frac{n-p}{p-1} - \frac{\log n}{\log p} < v_p(n!)$$

Exercice 33.bis.— (Autre preuve de la formule de Legendre).

1/ Montrer que, pour tout entier $n \geq 1$ et tout nombre premier p, on a

$$v_p(n!) = [n/p] + v_p([n/p]!)$$

2/ a) Montrer que, pour tout $x \in \mathbb{R}$ et tout entier $m \geq 1$, on a

$$\left[\frac{[mx]}{m}\right] = [x]$$

b) En déduire que si p est un nombre premier et i, j, n sont trois entiers alors

$$p^{i+j} \leq n \Longrightarrow \left[\frac{[n/p^i]}{p^j}\right] = \left[\frac{n}{p^{i+j}}\right]$$

3/ En déduire que, pour tout entier $n \geq 1$ et tout premier p, on a $v_p(n!) = \sum_{k\geq 1}\left[\frac{n}{p^k}\right]$.

Exercice 33.ter.— Montrer que, pour tout $n \geq 1$ et tout $p \in \mathscr{P}$, on a

$$v_p(n!) = \frac{n - N_p(n)}{p-1}$$

où $N_p(n)$ désigne le nombre de chiffres de l'entier n en base p.

Exercice 29.— Grâce à la formule de Legendre, déterminer le nombre de 0 qui terminent l'écriture décimale de 2016!.

Exercice 30.— (Minoration de la fonction π.)

Pour tout entier $n \geq 1$, on pose $\delta(n) = \text{ppcm}(1, 2, \cdots, n)$.

1/ a) Etudier la suite $\delta(n)/\delta(n-1)$.

b) Montrer que, pour tout premier $p \in \mathscr{P}$, $v_p(\delta(n)) = \left[\frac{\log n}{\log p}\right]$.

c) En déduire que $\delta(n) = \prod_{p\leq n} p^{v_p(\delta(n))}$ et, par suite, que $\delta(n) \leq n^{\pi(n)}$ où $\pi(n)$ désigne le nombre de nombres premiers inférieurs à n.

2/ En utilisant la formule de Legendre, montrer que, pour tout $n \geq 1$, l'entier C_{2n}^n divise $\delta(2n)$.

3/ a) Prouver que, pour tout $n \geq 1$, on a $C_{2n}^n \geq \frac{4^n}{2\sqrt{n}}$.

b) Montrer finalement que, pour $n \geq 2$, on a $\pi(n) \geq \log(2)\frac{n}{\log n} - 1$.

Exercice 31.— On souhaite montrer dans cet exercice que si a et n sont deux entiers ≥ 1, alors $n!$ divise le produit $\prod_{k=0}^{n-1}(a^n - a^k)$.

1) Montrer que la propriété est vraie pour $n = 1, 2$.

2) On suppose $n \geq 3$ et l'on considère un nombre premier p.

a) Montrer que $v_p(n!) \leq \left[\frac{n}{p-1}\right]$.

b) Si $v_p(a) \geq 1$, montrer que

$$v_p\left(\prod_{k=0}^{n-1}(a^n - a^k)\right) \geq \frac{n(n-1)}{2} \geq n$$

c) On suppose dans cette question que $v_p(a) = 0$.

c.i) Soit k un entier tel que $n-k$ soit multiple de $p-1$. Montrer que $v_p(a^{n-k} - 1) \geq 1$.

c.ii) Prouver alors que $v_p\left(\prod_{k=0}^{n-1}(a^n - a^k)\right) \geq \left[\frac{n}{p-1}\right]$.

3) Conclure.

Exercice 36.bis.— a) Montrer que, pour tous $x, y \in \mathbb{R}$, on a $[2x] + [2y] \geq [x] + [y] + [x+y]$.

b) En déduire, en utilisant la formule de Legendre, que le coefficient binomial C_{a+b}^{a} divise le produit $C_{2a}^{a} C_{2b}^{b}$.

Exercice 32.— On souhaite montrer le résultat suivant : *pour tout entier $n > 1$, parmi $2n-1$ entiers (non nécessairement distincts), on peut toujours en trouver n dont la somme est divisible par n.*

1/ On suppose donnés deux entiers n et m vérifiant la propriété annoncée et l'on considère une famille $\mathscr{F}$ de $2nm-1$ entiers.

a) Montrer que l'on peut trouver $2m-1$ sous-familles $\mathscr{F}_1, \cdots, \mathscr{F}_{2m-1}$ de $\mathscr{F}$, disjointes deux à deux et comptant chacune n entiers telles que les sommes respectives de ces sous-familles, $s_1, \cdots, s_{2m-1}$ soient toutes divisibles par n.

b) On note $d = \text{pgcd}(n, m)$ et l'on considère la famille $\mathscr{G} = \{\frac{s_1}{d}, \cdots, \frac{s_{2m-1}}{d}\}$. En considérant une certaine sous-famille de m éléments de $\mathscr{G}$ montrer qu'il existe une sous-famille de $\mathscr{F}$ de nm éléments dont la somme est divisible par nm.

c) En déduire que nm vérifie alors la propriété annoncée et, par suite, que pour montrer la propriété en toute généralité il suffit de la montrer pour $n = p$ premier.

2/ On se donne un nombre premier p et $a_1, \cdots, a_{2p-1}$ entiers. En considérant dans le corps $\mathbb{Z}/p\mathbb{Z}$ les deux polynômes $X_1^{p-1} + \cdots + X_{2p-1}^{p-1}$ et $a_1 X_1^{p-1} + \cdots + a_{2p-1} X_{2p-1}^{p-1}$ et en appliquant le théorème de Chevalley-Warning (voir exercice 107), montrer qu'il existe une sous famille de p éléments de $a_1, \cdots, a_{2p-1}$ dont la somme est divisible par p.

3/ Montrer que, pour tout $n \geq 2$, il existe $2n-2$ entiers tels que l'on ne puisse pas trouver n entiers parmi eux dont la somme est divisible par n.

Exercice 33.— (Constante de Mills) On note $(p_n)_n$ la suite croissante des nombres premiers et on admet le résultat (profond) de Ingham qui affirme qu'il existe une constante $K > 0$ telle que, pour tout $n \geq 1$, $p_{n+1} - p_n < K p_n^{5/8}$.

1/ a) Montrer que si $N \geq K^8$ désigne un entier, alors il existe un nombre premier p tel que $N^3 < p < (N+1)^3 - 1$.

b) En déduire qu'il existe une suite de nombres de premiers $(q_n)_n$ telle que, pour tout $n \geq 0$, $q_n^3 < q_{n+1} < (q_n + 1)^3 - 1$.

2/ Pour tout $n \geq 0$, on pose $u_n = q_n^{3^{-n}}$ et $v_n = (q_n + 1)^{3^{-n}}$.

a) Montrer que la suite $(u_n)_n$ converge vers un réel A qui vérifie que, pour tout $n \geq 0$, $u_n < A < v_n$.

b) Montrer que, pour tout $n \geq 0$, l'entier $\left\lfloor A^{3^n} \right\rfloor$ est premier (théorème de Mills).

Exercice 34.— (Majoration de la fonction π.)

Dans cet exercice, la lettre p désignera toujours un nombre premier, y compris quand elle sera utilisée comme indice de somme ou de produit. Par exemple, $\prod_{p \leq n} p$ désigne le produit des nombres premiers inférieur à n. Pour tout $n \geq 1$ on notera $\pi(n)$ le nombre de nombres premiers compris entre 1 et n (ainsi $\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = 2$, etc.). Si $a \leq b$ désigne deux entiers, on notera $\binom{b}{a} = \frac{b!}{a!(b-a)!}$ le coefficient binomial.

1) a) Prouver que pour tout entier $n \geq 1$, on a $\binom{2n}{n} < 4^n$.

(Ind. On pourra développer l'égalité $4^n = (1+1)^{2n}$.)

b) Montrer que si a et b désignent deux entiers tels que $0 < b/2 \leq a < b$ alors le produit $\prod_{a < p \leq b} p$ divise $\binom{b}{a}$ (le produit considéré est supposé être égal à 1 dans le cas où il n'y aurait pas de nombre premier p dans l'intervalle $]a, b]$).

En particulier, montrer que pour tout $n \geq 1$, le produit $\prod_{n < p \leq 2n} p$ divise $\binom{2n}{n}$.

c) Soit $m \geq 1$ un entier. Comparer les coefficients binomiaux $\binom{2m+1}{m}$ et $\binom{2m+1}{m+1}$. En déduire que $\binom{2m+1}{m} \leq 4^m$ et, par suite, que l'on a l'inégalité $\prod_{m+1 < p \leq 2m+1} p \leq 4^m$.

(Ind. On pourra développer la quantité $(1+1)^{2m+1}$.)

d) Prouver que pour tout entier $n \geq 1$, on a $\prod_{p \leq n} p \leq 4^n$.

(Ind. On pourra démontrer par récurrence, pour $n \geq 1$, la propriété $\mathcal{P}_n$ suivante : pour tout $k = 1, \cdots, 2n$ on a $\prod_{p \leq k} p \leq 4^k$.)

2) a) Montrer que pour tout entier $m \geq 1$ on a $m! > \left(\frac{m}{e}\right)^m$.

(Ind. On pourra se rappeler que pour tout $x \in \mathbb{R}$ on a $e^x = \sum_{n \geq 0} \frac{x^n}{n!}$.)

b) Déduire de ce qui précède que pour tout $n \geq 2$, $\pi(n)! \leq 4^n$ et, par suite que,

$$\pi(n) \log \pi(n) - \pi(n) \leq n \log 4$$

c) Prouver alors, en raisonnant par l'absurde, que pour tout $n \geq 2$ on a $\pi(n) \leq 16 \frac{n}{\log n}$.

Exercice 35.— (Divergence de la série $\sum_{p \in \mathcal{P}} \frac{1}{p}$)

On note $(p_n)_n$ la suite (croissante) des nombres premiers. On veut prouver que la série $\sum \frac{1}{p_n}$ est divergente. On raisonne par l'absurde.

1) Montrer qu'il existe un entier n tel que $\sum_{k \geq n+1} \frac{1}{p_k} \leq \frac{1}{2}$.

2) Fixons un entier N. On considère l'ensemble

$$A = \{h \in \{1, \cdots, N\} / \ \exists k \geq n+1, \ p_k | h\}$$

et l'ensemble $B = \{1, \cdots, N\} - A$.

a) Montrer que $\sharp A \leq N/2$ et, par suite, que $\sharp B \geq N/2$.

b) Montrer que le nombre d'élément $q \in B$ sans facteur carré est majoré par 2^n.

c) Montrer que le nombre de carrés dans B est majoré par $\sqrt{N}$.

d) En déduire que $\sharp B \leq 2^n \sqrt{N}$ et conclure.

3) En utilisant le *théorème des nombres premiers* (du indépendamment à Hadamard et La Vallée Poussin) qui affirme que $\pi(n) \simeq_n \dfrac{n}{\log n}$ (où $\pi(n) = \sharp\{1, \cdots, n\} \cap \mathscr{P}$), donner un équivalent simple de la suite $(p_n)_n$. En déduire un équivalent simple de la suite des sommes partielles $\left(\displaystyle\sum_{k=1}^{n} \frac{1}{p_k} \right)_n$.

Exercice 36.— L'Histoire raconte que les chinois procédaient de la façon suivante pour compter leur armées : *le général demandait aux soldats de se mettre en rang deux par deux, et notait s'il restait un soldat isolé ou non. Il leur demandait ensuite de se mettre en rang trois par trois et notait encore le nombre de soldats isolés qu'il restait. On continuait ainsi, en se mettant en rang ensuite cinq par cinq, puis sept par sept, puis onze par onze, puis treize par treize et dix-sept par dix-sept.*

Montrer que pour des armées de moins de cinq cent mille hommes, cette méthode permet effectivement de compter les soldats.

Exercice 37.— (Anneaux des fonctions arithmétiques) On considère S le $\mathbb{C}$-espace vectoriel des suites complexes $u : \mathbb{N}^* \to \mathbb{C}$. Un élément de S s'appelle une fonction arithmétique.

On note e la suite définie par $e(1) = 1$ et pour tout $n \geq 2$, $e(n) = 0$ et, si u et v sont deux éléments de S, on définit le *produit de convolution* des suites u et v comme étant la suite $u * v$ définie pour $n \geq 1$ par

$$(u * v)(n) = \sum_{ab=n} u(a)v(b) = \sum_{d|n} u(n/d)v(d) = \sum_{d|n} u(d)v(n/d)$$

1/ a) Montrer que muni du produit de convolution, S est un anneau commutatif unitaire intègre.

b) Montrer qu'un élément $u \in S$ est inversible, pour $*$, si et seulement si $u(1) \neq 0$.

c) Donner des exemples d'éléments premiers de S.

2/ On définit la fonction de Möbius, $\mu \in S$, par

$$\begin{cases} \mu(1) & = & 1 & \\ \mu(p_1 \cdots p_k) & = & (-1)^k & \text{si } p_1, \cdots, p_k \text{ désigne des nombres} \\ & & & \text{premiers distincts} \\ \mu(n) & = & 0 & \text{sinon} \end{cases}$$

a) Prouver que μ est l'inverse, pour $*$, de la suite c constante égale à 1 (i.e. pour tout $n \geq 1$, $c(n) = 1$).

b) En déduire la *formule d'inversion de Möbius* : si f et g sont deux éléments de S tels que pour tout $n \geq 1$

$$f(n) = \sum_{d|n} g(d)$$

alors pour tout $n \geq 1$ on a

$$g(n) = \sum_{d|n} \mu(d) f(n/d) = \sum_{d|n} \mu(n/d) f(d)$$

c) Montrer que pour tout entier $n \geq 1$ on a $\sum_{d|n} \varphi(d) = n$ où φ désigne l'indicateur d'Euler.

(Ind. On pourra procéder par récurrence sur le nombre de facteurs premiers de n).

d) Déduire de ce qui précède une formule permettant de calculer simplement $\varphi(n)$.

Exercice 38.— (Calcul de $\det(\text{pgcd}(i,j))_{1\leq i,j\leq n}$)

Pour $n \geq 1$ donné, on considère la matrice $M_n = (\text{pgcd}(i,j))_{1\leq i,j\leq n} \in \mathscr{M}_n(\mathbb{Z})$. On se propose de calculer $\det(M_n)$.

a) Montrer que pour tout $1 \leq i,j \leq n$ on a $\text{pgcd}(i,j) = \sum_{k|i \text{ et } k|j} \varphi(k)$ où φ désigne l'indicateur d'Euler.

b) On considère les deux matrices $A = (a_{i,j})_{i,j} \in \mathscr{M}_n(\mathbb{Z})$ et $B = (b_{i,j})_{i,j} \in \mathscr{M}_n(\mathbb{Z})$ définies, pour $1 \leq i,j \leq n$, par

$$a_{i,j} = \begin{cases} \varphi(j) & \text{si } j|i \\ 0 & \text{sinon} \end{cases} \qquad b_{i,j} = \begin{cases} 1 & \text{si } i|j \\ 0 & \text{sinon} \end{cases}$$

Calculer AB.

c) En déduire que $\det(M_n) = \prod_{k=1}^{n} \varphi(k)$.

Exercice 39.—

1/ a) Montrer que, pour tout entier $n \geq 2$, on a $\varphi(n) \geq \dfrac{n}{p_{\max}(n)}$ où $p_{\max}(n)$ désigne le plus grand nombre premier divisant n.

b) En déduire que, pour tout entier $n \geq 2$, on a $\varphi(n) \geq \sqrt{n}$ et, par suite, que $\lim_n \varphi(n) = +\infty$.

2/ En utilisant l'exercice 35, montrer que $\limsup_n \dfrac{\varphi(n)}{n} = 1$ et $\liminf_n \dfrac{\varphi(n)}{n} = 0$.

Exercice 40.— (Nombres parfaits)

1/ Prouver que si l'entier $2^p - 1$ est premier alors p est lui-même premier. Les nombres premiers de la forme $2^p - 1$ sont appelés nombres premiers de Mersenne.

2/ On considère les fonction arithmétiques "nombre de diviseurs" et "somme des diviseurs", notée respectivement δ et σ, et définies pour $n \geq 1$, par

$$\delta(n) = \sum_{d|n} 1 \quad \text{et} \quad \sigma(n) = \sum_{d|n} d$$

a) Quelles relations la formule d'inversion de Möbius permet-elle d'obtenir pour δ et σ ?

b) Soit $n = p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}$ la décomposition en facteurs premiers de l'entier $n \geq 1$. Montrer que

$$\delta(n) = \prod_{i=1}^{k} (\alpha_i + 1) \quad \text{et} \quad \sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

c) En déduire que δ et σ sont arithmétiquement multiplicatives (i.e. si $(n,m) = 1$ alors $\delta(nm) = \delta(n)\delta(m)$ et $\sigma(nm) = \sigma(n)\sigma(m)$).

d) Prouver que $\delta(n)$ est impair si et seulement si n est un carré parfait.

e) Montrer que, pour tout $n \geq 1$, $\prod_{d|n} d = \sqrt{n}^{\delta(n)}$.

3/ Un entier naturel est dit parfait s'il est la somme de ses diviseurs positifs stricts, autrement dit n est parfait si et seulement si $2n = \sigma(n)$. Par exemple 6 est parfait.

a) Montrer que si $2^p - 1$ est un nombre premier de Mersenne, alors l'entier $n = 2^{p-1}(2^p - 1)$ est parfait.

b) On considère un nombre parfait pair n. On écrit $n = 2^h m$ avec m impair et $h \geq 1$. Montrer que les rapports $\sigma(m)/2^{h+1}$ et $m/(2^{h+1}-1)$ sont égaux à un même entier t. Prouver que $t = 1$ et que par suite $n = 2^h(2^{h+1}-1)$ avec $2^{h+1}-1$ nombre premier de Mersenne.

Exercice 41.— Pour tout entier $n \geq 1$, on note $d(n)$ le nombre de diviseurs positifs de n.

1/ a) On considère $n = p_1^{\alpha_1} \cdots p_h^{\alpha_h}$ la décomposition en facteurs premiers de n. Montrer que $d(n) = \prod_{i=1}^{h}(\alpha_i + 1)$.

b) En déduire que, si n et m sont des entiers premiers entre eux, alors $d(nm) = d(n)d(m)$.

2/ a) Soient $n \geq 1$ et $k \in \{1, \cdots, n\}$. Montrer que $\left[\frac{n+1}{k}\right] = \left[\frac{n}{k}\right]$ si et seulement si k ne divise pas $n+1$. Que vaut $\left[\frac{n+1}{k}\right]$ si $k|(n+1)$?
(Ind. On pourra étudier les divisions euclidiennes de n et $n+1$ par k.)

b) En déduire que, pour tout entier $n \geq 1$, on a $d(1) + \cdots + d(n) = \left[\frac{n}{1}\right] + \cdots + \left[\frac{n}{n}\right]$.

c) Prouver alors que $\sum_{k=1}^{n} d(k) = n \log n + O(n)$.

3/ a) En utilisant le 2.e. de l'exercice 40, montrer que, pour tout $n \geq 1$, on a $\sum_{k=1}^{n} d(k) \log k = 2\sum_{k=1}^{n} \left[\frac{n}{k}\right] \log k$.

b) En déduire que $\sum_{k=1}^{n} d(k) \log k = n \log^2 n + o(n \log^2 n)$.

Exercice 42.— Pour tout entier $n \geq 1$, on pose $d(n) = \sum_{k|n} 1$ et $D(n) = \sum_{k=1}^{n} d(k)$.

a) En écrivant $d(n) = \sum_{k=1}^{n} \delta_{k,n}$ avec $\delta_{k,n} \in \{0, 1\}$ bien choisi, montrer que

$$0 \leq H_n - \frac{D(n)}{n} < 1$$

où $(H_n)_n$ désigne la série harmonique.

b) En déduire un équivalent simple de la suite $(D(n))_n$.

c) En étudiant la série $\sum\left(\frac{D(n+1)}{n+1} - \frac{D(n)}{n}\right)$, montrer que $\sum_{k=1}^{n} \frac{d(k)}{k} \simeq_n \frac{1}{2} \log^2 n$.

Exercice 43.— (Le cryptosystème de la musette.)

Le problème de la musette est le suivant : étant donnés une collection d'objets de volumes différents et une musette de volume fixé, comment choisir des objets parmi la collection pour qu'ils remplissent complétement la musette?

Mathématiquement, ce problème se traduit de la manière suivante : soit V un entier naturel (volume de la musette) et $v_1, \cdots, v_n$ des entiers naturels (v_k est le volume du k-ième objet de la collection), comment trouver une suite finie $\varepsilon_1, \cdots, \varepsilon_n \in \{0, 1\}$ telle que

$$\sum_{k=1}^{n} \varepsilon_k v_k = V$$

($\varepsilon_k = 1$ si l'on ajoute le k-ième objet dans la musette et $\varepsilon_k = 0$ si on le laisse)

Notons que l'existence d'une suite solution n'est pas sure, de même, il peut trés bien exister plusieurs solutions. Tout dépend de V et des v_k.

I) On se donne un entier $n \geq 1$ et $v_1, \cdots, v_n, V$ des entiers naturels.

1) Décrire une méthode pour rechercher d'éventuelles solutions au problème de la musette pour $v_1, \cdots, v_n, V$ et évaluer le nombre d'opérations que cette méthode exige.

D'un point de vue algorithmique, le problème de la musette est réputé (en général) inaccessible en temps machine raisonnable.

2) (Cas particulier des suites supercroissantes) *On suppose dans cette question que la suite $v_1, \cdots, v_n$ est supercroissante, c'est-à-dire que pour tout entier $k = 2, \cdots, n$ on a*

$$v_k > v_{k-1} + \cdots + v_1$$

a) Donner un exemple de suite finie supercroissante.

b) Montrer que si le problème de la musette admet une solution, alors elle est unique.

c) On considère l'algorithme suivant : on prend le plus grand indice $i \in \{1, \cdots, n\}$ tel que $v_i \leq V$. On pose $\epsilon_i = 1$ et on recommence l'opération avec $V - v_i$. Une fois que la boucle est finie, on pose $\epsilon_j = 0$ pour tout indice j qui n'a pas été traité. On pourrait formaliser cet algorithme de la manière suivante :

Pour $i = n$ à 1 faire

- si $v_i \leq V$ faire $\epsilon_i := 1$ et $V := V - v_i$
- sinon faire $\epsilon_i := 0$

Montrer que le problème de la musette admet une solution si et seulement si la dernière valeur de V dans cet algorithme est 0. Dans le cas où cette dernière valeur est bien 0, prouver alors que la suite $\epsilon_1, \cdots, \epsilon_n$ obtenu par l'algorithme est bien la solution au problème de la musette.

d) Que penser de l'efficacité de cet algorithme (en particulier par rapport à celui que vous avez proposé dans le cas général)?

II) (Cryptosystème de Merkle-Hellman) Un groupe d'utilisateurs se fixe un entier n (grand) et convient que les messages lisibles et cryptés que les membres souhaitent s'échanger sont des n-uplets $(\epsilon_1, \cdots, \epsilon_n)$ à valeur dans $\{0, 1\}$.

Chaque utilisateur se donne un entier m, une suite supercroissante $(v_1, \cdots, v_n)$ de somme $\leq m$ et un entier $0 < a < m$ premier à m.

1) Montrer qu'il existe un unique entier b tel que $1 \leq b < m$ tel que $ab \equiv 1\ (m)$. Expliquer comment on fait pour trouver b connaissant a et m.

L'utilisateur garde secret $v_1, \cdots, v_n, m, a, b$ et pour tout $i = 1, \cdots, n$ il calcule w_i le plus petit résidu positif modulo m de l'entier av_i[2]. La clé publique de l'utilisateur est alors le n-uplet $(w_1, \cdots, w_n)$.

Pour envoyer un message $\mathcal{P} = (\epsilon_1, \cdots, \epsilon_k)$ à un utilisateur de clé pulique $(w_1, \cdots, w_n)$, on lui envoie l'entier $C = \sum_{i=1}^{k} \epsilon_i w_i$. La suite $\mathcal{P}$ est donc la solution du problème de la musette pour C et la suite $(w_1, \cdots, w_n)$.

2) On considère V le plus petit résidu positif modulo m de l'entier bC.

a) Montrer que $V = \sum_{i=1}^{n} \epsilon_i v_i$ et en déduire une moyen simple pour retrouver $\mathcal{P}$.

b) Expliquer pourquoi seul le destinataire du message peut le décrypter.

3) (Exemple) On choisit $n = 6$. On choisit $(v_1, v_2, v_3, v_4, v_5, v_6) = (2, 3, 7, 13, 27, 54)$, $m = 110$ et $a = 49$.

[2] On rappelle que cet entier est le plus petit entier positif tel que $w_i \equiv av_i\ (m)$, il est égal au reste de la division euclidienne de av_i par m

a) Justifier que les choix qui viennent d'être fait sont compatibles avec les contraintes du cryptosystème. Calculer la clé publique $(w_1, w_2, w_3, w_4, w_5, w_6)$.

b) Décrypter le message $C = 130$.

Exercice 44.— Pour un entier $n \geq 1$ donné, on considère l'ensemble $\mathscr{E} = \{\pm 1\}^n$ et l'on note génériquement $\varepsilon = (\varepsilon_1, \cdots, \varepsilon_n)$ les éléments de $\mathscr{E}$.

A) Calculer le cardinal de l'ensemble $\left\{ \varepsilon \in \mathscr{E} / \sum_{k=1}^{n} \varepsilon_k = 0 \right\}$.

B) On s'intéresse dans cette question au cardinal γ_n de l'ensemble $\left\{ \varepsilon \in \mathscr{E} / \sum_{k=1}^{n} k\varepsilon_k = 0 \right\}$.

1) Montrer que, si $n \equiv 0, 3 \bmod(4)$, alors $\gamma_n \neq 0$

2) Montrer que $\prod_{k=1}^{n} \cos(kx) = \frac{1}{2^{n-1}} \sum_{\varepsilon \in \mathscr{E}} \cos(\varepsilon_1 x + 2\varepsilon_2 x + \cdots + n\varepsilon_n x)$. En déduire que

$$\gamma_n = \frac{1}{2^n \pi} \int_0^{2\pi} \cos(x)\cos(2x)\cdots\cos(nx)dx$$

3) a) Montrer que, pour tout entier $k \geq 1$, il existe un polynôme $P_k(x) \in \mathbb{R}[x]$ tel que $\cos(kx) = P_k(\cos(x))$.

b) Prouver que P_{2k} est un polynôme pair et que P_{2k+1} est un polynôme impair.

4) Prouver finalement que $\gamma_n = 0$ si $n \equiv 1, 2 \bmod(4)$.

Exercice 45.— (Formule de Taylor discrète) Pour un élément $h \neq 0$ de $\mathbb{C}$ fixé, on considère l'opérateur de différence

$$\begin{array}{rccc} \Delta_h : & \mathbb{C}[x] & \longrightarrow & \mathbb{C}[x] \\ & P(x) & \longmapsto & P(x+h) - P(x) \end{array}$$

et, pour tout entier $k \geq 0$, $\Delta_h^k = \Delta_h \circ \cdots \circ \Delta_h$ l'itérée k fois de Δ_h (avec la convention $\Delta_h^0 = \mathrm{Id}$).

$$\begin{aligned} \Delta_h^0(P)(x) &= P(x) \\ \Delta_h^1(P)(x) &= P(x+h) - P(x) \\ \Delta_h^2(P)(x) &= P(x+2h) - 2P(x+h) + P(x) \\ \Delta_h^3(P)(x) &= P(x+3h) - 3P(x+2h) + 3P(x+h) - P(x) \\ &\vdots \end{aligned}$$

1/ Montrer que, pour tout $P \in \mathbb{C}[x]$, $\Delta_h^k(P)(x)$ est une combinaison $\mathbb{Z}$-linéaire des polynômes $P(x+mh)$ avec $m = 0, \cdots, k$ et expliciter les coefficients de cette combinaison.

2/ a) Prouver que $\Delta_h \in \mathscr{L}(\mathbb{C}[x])$, $\mathrm{Im}(\Delta_h) = \mathbb{C}[x]$ et $\ker(\Delta_h) = \mathbb{C}_0[x]$.

b) Préciser ce que deviennent les résultats de la question a) pour Δ_h^k $(k \geq 1)$.

3/ On pose $\Gamma_0(x) = 1$ et, pour tout $k \geq 1$,

$$\Gamma_k(x) = \frac{x(x-1)\cdots(x-k+1)}{k!} \in \mathbb{C}[x]$$

a) Montrer que la famille $\{\Gamma_k\}_k$ est une base de $\mathbb{C}[x]$.

b) Montrer que, pour tout $k \geq 1$, $\Delta_h(\Gamma_k(x/h)) = \Gamma_{k-1}(x/h)$.

4/ On se donne un polynôme $P \in \mathbb{C}[x]$ de degré $d \geq 0$.

a) Montrer que $P(x) = \sum_{k=0}^{d} \Delta_h^k(P)(0)\Gamma_k\left(\frac{x}{h}\right)$ (Formule de Taylor discrète).

b) En déduire que, si a_d est le terme dominant de P, alors $\Delta_h^d(P)(0) = a_d h^d d!$.

Exercice 46.— On considère deux polynômes premiers entre eux $P, Q \in \mathbb{Z}[X]$, et l'on définit l'application $\delta(P,Q) : \mathbb{Z} \longrightarrow \mathbb{N}$, plus simplement notée δ, par

$$\delta(u) = \text{pgcd}(P(u), Q(u))$$

1/ On souhaite montrer que δ est périodique.

a) Montrer que, pour tout polynôme $H \in \mathbb{Z}[X]$, tout $\lambda \in \mathbb{Z}$ et tout $u \in \mathbb{Z}$, on a $H(u+\lambda) \equiv H(u) \bmod(\lambda)$.

b) En déduire que, pour tout $\lambda \in \mathbb{Z}$ et tout $u \in \mathbb{Z}$, on a $\text{pgcd}(P(u), Q(u), \lambda) = \text{pgcd}(P(u+\lambda), Q(u+\lambda), \lambda)$.

c) On suppose dans cette question qu'il existe deux fonctions $f, g : \mathbb{Z} \longrightarrow \mathbb{Z}$ et un entier λ tels que, pour tout $u \in \mathbb{Z}$,

$$f(u)P(u) + g(u)Q(u) = \lambda$$

Montrer que, pour tout $u \in \mathbb{Z}$, $\delta(u) = \delta(u+\lambda)$.

d) Montrer qu'il existe $U(x), V(x) \in \mathbb{Z}[x]$ et $\lambda \in \mathbb{Z}$ non nul tels que

$$U(x)P(x) + V(x)Q(x) = \lambda$$

et conclure.

2/ On note Π l'ensemble des périodes de la fonction δ auquel on rajoute 0.

a) Montrer que $\Pi = \pi_0\mathbb{Z}$ pour un certain entier $\pi_0 > 0$.

b) Montrer que $\pi = \text{ppcm}\{\delta(u)/\ u \in \mathbb{Z}\}$ existe bien et que $\pi \in \Pi$ (on pourra utiliser la question 1.c). En déduire que $\pi_0 | \pi$.

3/ On reprend les notations et les résultats de l'exercice 45. On note $d = d^\circ P \leq d^\circ Q$ et a_d le terme dominant de P.

a) Montrer que, pour tout $k \geq 1$ et tout $u \in \mathbb{Z}$, on a $\delta(u) | \Delta_{\pi_0}^k(P)(u)$.

b) En déduire que $\pi | a_d \pi_0^d d!$.

Exercice 47.— (Irrationalité de π)

On suppose l'existence de deux entiers a et b positifs tels que $\pi = a/b$. Pour tout entier $n \geq 0$, on considère la fonction polynomiale

$$P_n(x) = \frac{1}{n!} x^n (bx - a)^n$$

1/ On se donne un entier $n \geq 0$.

a) Montrer que, pour tout entier $k \geq 0$, $P_n^{(k)}(0), P_n^{(k)}(\pi) \in \mathbb{Z}$.

b) En déduire que $\int_0^\pi P_n(x) \sin x dx \in \mathbb{Z}$.

2/ a) Prouver que $\lim_n \int_0^\pi P_n(x) \sin x dx = 0$.

b) En déduire que π est irrationnel.

Exercice 48.— (Irrationalité de e)

On considère une suite croissante et non bornée d'entiers strictement positifs $(a_n)_n$. Pour tout $n \geq 0$, on pose $A_n = \prod_{i=0}^{n} a_i$.

1/ Montrer que la série $\sum \frac{1}{A_n}$ converge. On pose $\lambda = \sum_{n=0}^{+\infty} \frac{1}{A_n}$.

2/ a) Montrer que, pour tous $0 \leq n+1 \leq k$, on a $\frac{A_n}{A_k} \leq \left(\frac{1}{a_{n+1}}\right)^{k-n}$. En déduire que, pour n assez grand, $\sum_{k \geq n+1} \frac{A_n}{A_k} \leq \frac{1}{a_{n+1}-1}$.

b) Montrer finalement que $\sum_{k \geq n+1} \frac{A_n}{A_k} \simeq_n \frac{1}{a_{n+1}}$ et, par suite, que $\sin(2\pi\lambda A_n) \simeq_n \frac{2\pi}{a_{n+1}}$.

2/ a) Soit $r \in \mathbb{Q}$. Etudier la suite $(\sin(2\pi r m))_m$ et en déduire une condition nécessaire et suffisante sur une suite extraite $(\sin(2\pi r \varphi(m)))_m$ pour que cette suite extraite converge.

b) Prouver que $\lambda \notin \mathbb{Q}$ et en déduire que $e \notin \mathbb{Q}$.

Exercice 49.— (Putnam 2007)

1/ (Putnam 2007) Déterminer x_{2007} où $(x_n)_n$ est la suite récurrente définie par, $x_0 = 1$ et, pour tout $n \geq 0$,

$$x_{n+1} = 3x_n + [\sqrt{5}x_n]$$

(Ind. Montrer que $x_n = 2^{n-1}F_{2n+3}$.)

2/ (Généralisation) On considère un entier pair $k \geq 2$ et l'on pose $a = F_{k+1} + F_{k-1}$ et $b = F_k$. Déterminer une expression simple de la suite récurrente $(x_n)_n$ définie par, $x_0 = 1$ et, pour tout $n \geq 0$,

$$x_{n+1} = ax_n + [b\sqrt{5}x_n]$$

Exercice 50.— On considère un entier $n \geq 2$ et $a_1, \cdots, a_n$ des entiers naturels. Montrer que, si $\sum_{i=1}^{n} a_i < 2^n - 1$, alors il existe $(\varepsilon_1, \cdots, \varepsilon_n) \in \{-1, 0, 1\}^n$ avec $(\varepsilon_1, \cdots, \varepsilon_n) \neq (0, \cdots, 0)$, vérifiant $\sum_{i=1}^{n} \varepsilon_i a_i = 0$.

(Ind. On pourra montrer que, pour tout $m < 2^n$, il existe $(\varepsilon_1, \cdots, \varepsilon_n)$ tel que m divise l'entier $\sum_{i=1}^{n} \varepsilon_i a_i$. Pour ce faire, on se ramènera au cas où les a_i sont distincts deux à deux. On aura alors intérêt à considérer l'ensemble des parties $\mathcal{P}(E)$ de l'ensemble $E = \{a_1, \cdots, a_n\}$, en regardant en particulier, pour une partie $S \in \mathcal{P}(E)$ donnée, la somme $\sum_{x \in S} x$.)

Exercice 51.— (Formule d'inversion de Pascal et applications)

I.— Formule.

On considère une suite de complexes $(u_n)_n$ et, pour tout $n \geq 0$, on pose $v_n = \sum_{k=0}^{n} C_n^k u_k$. Montrer que, pour tout $n \geq 0$, on a

$$u_n = (-1)^n \sum_{k=0}^{n} (-1)^k C_n^k v_k$$

II.— Applications.

1) Montrer que, pour tout complexe a et tout entier $n \geq 0$, on a $a^n = \sum_{k=0}^{n} (-1)^{n-k} C_n^k (1+a)^k$.

2) Pour deux entiers $n, p \geq 0$ donnés, on considère le nombre $S_{n,p}$ de surjections d'un ensemble à n éléments vers un ensemble à p éléments.

a) Montrer que $p^n = \sum_{k=0}^{p} C_p^k S_{n,k}$.

b) En déduire $S_{n,p}$.

3) Pour un entier $n \geq 1$ donné, on appelle n-dérangement tout élément de S_n qui ne possède aucun point fixe. On note D_n le nombre de dérangement.

a) Montrer que $n! = \sum_{k=0}^{n} C_n^k D_k$.

b) En déduire D_n.

c) Calculer $\lim_n \frac{D_n}{n!}$ et donner une interprétation probabiliste de ce réel.

Exercice 52.— (Probabilité de tirer au hasard deux entiers premiers entre eux)

1/ (Formule du crible) Montrer que si $E_1, \cdots, E_n$ désignent des ensemble finis, alors on a

$$\sharp \bigcup_{i=1}^{n} E_i = \sum_{\emptyset \neq I \subset \{1,\cdots,n\}} (-1)^{1+\sharp I} . \sharp \bigcap_{i \in I} E_i$$

2/ On considère un entier $n \geq 1$ et l'ensemble $A_n = \left\{(a,b) \in \{1,\cdots,n\}^2 / \ (a,b) = 1\right\}$ des couples d'entiers plus petits que n et premiers entre eux. On note alors $d_n = \frac{\sharp A_n}{n^2}$ la proportion de ces couples dans $\{1,\cdots,n\}^2$. L'objectif de cet exercice est de montrer que $\lim_n r_n = 6/\pi^2$, c'est-à-dire que moralement, la probabilité de tirer au hasard deux entiers premiers entre eux est égale à $6/\pi^2 \approx 0.6079$.

a) On note $p_1 < p_2 < \cdots < p_k$ la liste des nombres premiers $\leq n$ et, pour tout $i = 1, \cdots, k$, on pose $U_i = \left\{(a,b) \in \{1,\cdots,n\}^2 / \ p_i | a \text{ et } p_i | b\right\}$. Montrer que $A_n = \complement \bigcup_{i=1}^{k} U_i$.

b) En utilisant la formule du crible, déduire de la question précédente que

$$\sharp A_n = \sum_{d=1}^{n} \mu(d) \left[\frac{n}{d}\right]^2$$

où μ désigne la fonction de Möbius (voir exercice 37).

c) Montrer que $\left| r_n - \sum_{d=1}^{n} \frac{\mu(d)}{d^2} \right| = O\left(\frac{\log n}{n}\right)$.

d) En déduire que $\rho = \lim_n r_n$ existe et que $\rho = \sum_{d \geq 1} \frac{\mu(d)}{d^2}$.

e) En calculant astucieusement le produit $\left(\sum_{d \geq 1} \frac{\mu(d)}{d^2}\right) . \left(\sum_{n \geq 1} \frac{1}{n^2}\right)$ et en utilisant la propriété fondamentale de la fonction μ, prouver finalement que

$$\rho = \frac{1}{\sum_{n \geq 1} \frac{1}{n^2}} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$$

Arithmétique modulaire

Exercice 53.— Montrer que pour tout $n \geq 0$, $n(n+1)(n+2)(n+3)$ est divisible par 24, et que $n(n+1)(n+2)(n+3)(n+4)$ est divisible par 120.

Exercice 54.— Déterminer les entier $n \geq 1$ tels que $3^{n-1} + 5^{n-1}$ divise $3^n + 5^n$.

Exercice 55.— Trouver le reste de la division euclidienne de 100^{1000} par 13.

Exercice 56.— Déterminer le dernier chiffre de l'écriture en base 10 de l'entier $7^{7^{7^{7^7}}}$

Exercice 57.— On considère l'entier $n = 10q + r$ avec $q \in \mathbb{N}$ et $r \in \{0, \cdots, 9\}$. Montrer que $7|n$ si et seulement si $7|q - 2r$. Est-ce que $7|11228$? Est-ce que $7|15637$?

Exercice 58.— Montrer que 11 divise $2^{123} + 3^{121}$.

Exercice 59.— Montrer que, pour tout $n \in \mathbb{N}$,

$$\begin{array}{llllll} (i) & 6|5n^3 + n & (ii) & 7|3^{2n+1} + 2^{n+2} & (iii) & 11|3^{8n} \times 5^4 + 5^{6n} \times 7^3 \\ (iv) & 5|2^{2n+1} + 3^{2n+1} & (v) & 9|4^n - 1 - 3n & (vi) & 15^2|16n - 1 - 15n \end{array}$$

Exercice 60.— Montrer que, pour tout entier $n \geq 2$, on a $10|2^{2n} - 6$.

Exercice 61.— Soit $n \in \mathbb{N}$. Montrer que la plus grande puissance de 2 qui divise l'entier $5^{2n} - 1$ est 2^{n+2}.

Exercice 62.— Montrer que, pour tous $a, b \in \mathbb{Z}$ et tout $n \geq 1$, on a

$$a \equiv b \bmod(n) \Longrightarrow a^n \equiv b^n \bmod(n^2)$$

Exercice 63.— Montrer, pour $x, y \in \mathbb{N}$, l'équivalence

$$7|x \text{ et } 7|y \Longleftrightarrow 7|x^2 + y^2$$

Exercice 64.— On souhaite résoudre, dans $\mathbb{Z}$, l'équation $x^2 + y^2 + z^2 = x^2y^2$.

1. Montrer que si $(x, y, z) \in \mathbb{Z}^3$ est solution, alors x, y et z sont des entiers pairs.

2. En déduire toutes les solutions.

Exercice 65.— On souhaite résoudre, dans $\mathbb{Z}$, l'équation $5x^3 + 11y^3 = 13z^3$.

1. Montrer que si $(x, y, z) \in \mathbb{Z}^3$ est solution, alors x, y et z sont divisibles par 13.

2. En déduire toutes les solutions.

Exercice 66.— Le but de cet exercice est de montrer que, pour tout $n \geq 0$, l'entier $7^n + n^3$ n'est pas divisible par 9.

1) a) Soit $a \in \mathbb{N}$, montrer que $7^a \equiv 1 \bmod(9)$ si et seulement si a est divisible par 3.

b) Montrer que, pour tout $n \geq 0$, $n^3 \equiv 0, 1$ ou $-1 \bmod(9)$.

2) On considère un entier $n \geq 0$ tel que 9 divise $7^n + n^3$.

a) Montrer que $n^6 \equiv 1 \bmod(9)$ et donc que $7^{2n} \equiv 1 \bmod(9)$.

b) En déduire que n est divisible par 3 et conclure.

Exercice 67.— (Carrés dans $\mathbb{Z}/p\mathbb{Z}$)

On considère un nombre premier $p \geq 3$ et $K = \mathbb{Z}/p\mathbb{Z}$. On rappelle que K est un corps. Dans cet exercice on notera C l'ensemble des carrés de K.

a) On considère l'application $\pi : \{\overline{a}/\ a = 0, \cdots, (p-1)/2\} \longrightarrow C$ définie par $\pi(x) = x^2$. Montrer que π est bijective et en déduire que $\sharp C = \dfrac{p+1}{2}$.

b) Montrer que dans $\mathbb{Z}/p\mathbb{Z}$, tout élément est somme de deux carrés.

c) On considère l'application $\theta : K^* \longrightarrow K^*$ définie par $\theta(x) = x^{\frac{p-1}{2}}$. Montrer que $\mathrm{Im}(\theta) = \{\pm 1\}$. En déduire que si $x \in K^*$, les propositions suivantes

i) x est un carré,

ii) $x^{\frac{p-1}{2}} = 1$.

sont équivalentes.

d) En déduire que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1\ (4)$.

Exercice 68.— Déterminer les entiers naturels n tels que n divise $2^n - 1$.
(Ind. On pourra utiliser le petit théorème de Fermat pour le plus petit premier p divisant n.)

Exercice 69.— (Test de primalité de Miller-Rabin)

On considère $p = 2^s d + 1$ un entier impair (avec $s = v_2(p)$) et, pour un élément $a \in \{1, \cdots, s-1\}$ tel que $a^d \not\equiv 1 \bmod(p)$, la suite d'entier $(b_n)_n$ définie, pour $n \geq 0$, par $b_n = a^{d2^n}$. Montrer que, si pour tout $n = 1, \cdots, s-1$ on a $b_n \not\equiv -1 \bmod(p)$, alors p n'est pas premier.
(Indication. On pourra montrer la contraposée en étudiant les racines du polynôme $x^2 - 1$ dans $\mathbb{Z}/p\mathbb{Z}$.)

Exercice 70.— (Théorème de Wilson) Soit p un entier naturel non nul. Montrer que les propositions suivantes sont équivalentes :

i) p est premier,

ii) $(p-1)! \equiv -1\ (p)$.

(Ind. Pour le sens direct, on pourra essayer de voir les classes modulo p des entiers $(p-1)!$ et -1 comme le coefficient constant d'un même polynôme.)

Exercice 71.— Montrer que, si $p \equiv 1 \bmod(4)$ est un nombre premier, alors $\left[\left(\dfrac{p-1}{2}\right)!\right]^2 \equiv -1 \bmod(p)$

Exercice 72.— (Nombres de Carmichaël)

Un entier $n \geq 2$ est dit *de Carmichaël* si, pour tout entier $a \in \mathbb{Z}$, on a $a^n \equiv a\ (n)$. On se propose dans ce problème de caractériser ces entiers.

1.— Un célèbre théorème implique que tout nombre premier est un nombre de Carmichaël. Enoncer ce théorème et donner son nom.

2.— On se donne un nombre de Carmichaël $n \geq 2$ et un nombre premier p qui divise n.

2.a.i.— En utilisant la formule de binôme de Newton, montrer que $(p+1)^n \equiv 1\ (p^2)$.
2.a.ii.— En déduire que p^2 ne divise pas n et, par suite, que l'entier n est sans facteur carré.

2.b.i.— Montrer que, pour tout $a = 1, \cdots, p-1$, on a $a^{n-1} \equiv 1\ (p)$.
2.b.ii.— En effectuant la division euclidienne de $(n-1)$ par $(p-1)$, montrer que $(p-1)|(n-1)$.
(Ind. On pourra se rappeler que $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif et que, par conséquent, un polynôme de degré r dans $\mathbb{Z}/p\mathbb{Z}$ possède au plus r racines.)

3.— On considère un entier $n \geq 2$.

3.a.— Si p désigne un premier tel que $(p-1)|(n-1)$, montrer que, pour tout $a \in \mathbb{Z}$, $a^n \equiv a\ (p)$.
(Ind. On pourra distinguer le cas $p|a$ du cas $(p, a) = 1$.)

3.b.— En déduire que, si $n = p_1 \cdots p_r$ où $p_1, \cdots, p_r$ désigne une famille de nombres premiers distincts deux à deux tels que $(p_i - 1)|(n-1)$ pour tout $i = 1, \cdots, r$, alors n est un nombre de Carmichaël.

4.a.— Déduire de ce qui précède le *théorème de Korselt* (1899) : un entier $n \geq 2$ est un nombre de Carmichaël si et seulement si n est sans facteur carré et, pour tout diviseur premier p de n, $p-1$

divise $n-1$.

4.b.— Montrer que 561 est un nombre de Carmichaël.

4.c.— Montrer qu'un nombre de Carmichaël qui n'est pas premier possède au moins trois facteurs premiers.

Groupes, anneaux et corps

Exercice 73.— Montrer que les lois suivantes munissent l'ensemble G indiqué d'une structure de groupe, et préciser s'il est abélien :

1/ $x*y=\dfrac{x+y}{1+xy}$ sur $G=]-1,1[$.

2/ $(x,y)*(x',y')=(x+x',ye^{x'}+y'e^{-x})$ sur $G=\mathbb{R}^2$.

Exercice 74.— Sur $\mathbb{R}$, on considère la loi de composition interne $*$ définie par

$$x*y=x+y+xy$$

a) Montrer que $*$ est associative, commutative et possède un élément neutre.

b) Quels sont les éléments inversibles pour cette loi ?

c) Prouver que $*$ est aussi une loi de composition interne sur $\mathbb{R}-\{-1\}$. Est-ce que $\mathbb{R}-\{-1\}$ est un groupe pour cette loi ?

d) Montrer que l'application $f:\mathbb{R}-\{-1\}\longrightarrow\mathbb{R}^*$ définie par $f(x)=1+x$ est un isomorphisme de groupes ($\mathbb{R}^*$ est considéré ici comme groupe multiplicatif).

Exercice 75.— Soit $(G,*)$ un groupe abélien et $a\in G$. On définit sur G une loi $\perp$ en posant :

$$\forall x,y\in G,\ x\perp y=x*y*a$$

Montrer que $(G,\perp)$ est un groupe abélien.

Exercice 76.— Soient a et b deux entiers relatifs non nuls et $n>0$ un entier naturel strictement positif. Dans $\mathbb{Z}$ on considère la loi de composition interne $*$ définie pour $x,y\in\mathbb{Z}$ par

$$x*y=ax+by$$

Par ailleurs, on considère sur $\mathbb{Z}$ la relation d'équivelence $\mathcal{R}_n$ de congruence modulo n : pour tout $x,y\in\mathbb{Z}$,

$$x\mathcal{R}_n y\Longleftrightarrow x\equiv y\ \mathrm{mod}(n)\Longleftrightarrow n|(x-y)$$

1) Montrer que $\mathcal{R}_n$ est compatible avec la loi $*$. *On peut donc considérer le magma quotient* $(\mathbb{Z}/\mathcal{R}_n,\overline{*})$ *où* $\overline{*}$ *est la loi de composition interne induite par* $*$ *sur l'ensemble quotient* $\mathbb{Z}/\mathcal{R}_n$.

2) a) Montrer que $\overline{*}$ est associative si et seulement si $n|a(a-1)$ et $n|b(b-1)$.

b) Montrer que $\overline{*}$ est commutative si et seulement si $n|(b-a)$.

c) Prouver que $\overline{*}$ possède un neutre à gauche si et seulement si $n|(b-1)$. Dans cette situation, décrire les neutres à gauche de $\overline{*}$. Donner un exemple, avec $n>3$, où $\overline{*}$ possède exactement 3 neutres à gauche.

d) Proposer une propriété caractéristique analogue à celle de la question c. pour que $\overline{*}$ possède un neutre à droite et décrire les neutres à droite de $\overline{*}$.

e) En déduire que si $\overline{*}$ possède un neutre bilatère alors $\overline{*}$ est associative et commutative. Donner des valeurs explicites de a,b,n pour que $\overline{*}$ soit :

i) associative sans neutre bilatère,

ii) commutative sans neutre bilatère,

iii) associative et non commutative,

iv) commutative et non associative,

v) non commutative et non associative.

3) Montrer que si $\overline{*}$ possède un neutre bilatère alors $(\mathbb{Z}/\mathcal{R}_n, \overline{*})$ est un groupe. Quel est alors ce groupe?

Exercice 77.— Pour tout $(\alpha, \beta) \in \mathbb{C} \times \mathbb{C}$, on pose

$$M(\alpha,\beta) = \begin{pmatrix} \alpha & -\beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix} \in \mathscr{M}_2(\mathbb{C})$$

et l'on considère l'ensemble

$$\mathbb{H}^* = \{M(\alpha,\beta) / \ (\alpha,\beta) \in \mathbb{C} \times \mathbb{C},\ (\alpha,\beta) \neq (0,0)\}$$

a) Montrer que $\mathbb{H}^*$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$.

b) Déterminer explicitement le centre $Z(\mathbb{H}^*)$ de $\mathbb{H}^*$ et montrer que ce groupe est isomorphe au groupe multiplicatif $\mathbb{R}^*$.

Exercice 78.— On considère un nombre premier p et le sous-ensemble de $\mathbb{Q}$ suivant :

$$\mathbb{Q}_{[p]} = \left\{ \frac{a}{p^n} / \ a \in \mathbb{Z},\ n \in \mathbb{N} \right\}$$

a) Montrer que $\mathbb{Q}_{[p]}$ est un sous-groupe de $(\mathbb{Q}, +)$.

b) Pour tout entier $n \in \mathbb{N}$, on considère le sous-groupe $H_n = \left\langle \frac{1}{p^n} \right\rangle$. Montrer que la suite $(H_n)_n$ est strictement croissante pour l'inclusion et que $\mathbb{Q}_{[p]} = \bigcup_{n\in\mathbb{N}} H_n$.

c) Montrer que l'application

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_{[p]} & \longrightarrow & \mathbb{Q}_{[p]} \\ & x & \longmapsto & px \end{array}$$

est un automorphisme du groupe $(\mathbb{Q}_{[p]}, +)$.

Exercice 79.— On considère un groupe $(G, .)$ de neutre e. Montrer que les propriétés suivantes

i) G est abélien,

ii) $\forall x, y \in G,\ xy = yx$,

iii) $\forall x, y \in G,\ (xy)^2 = x^2y^2$,

iv) $\forall x, y \in G,\ (xy)^{-1} = x^{-1}y^{-1}$,

v) l'application $x \longmapsto x^{-1}$ est un automorphisme,

vi) $\forall n \in \mathbb{Z},\ \forall x, y \in G,\ (xy)^n = x^n y^n$,

vii) $\forall x, y \in G,\ \exists k \in \mathbb{Z},\ (xy)^i = x^i y^i$ pour $i = k, k+1, k+2$,

sont équivalentes. En déduire que si pour tout $x \in G$ on a $x^2 = e$ alors G est abélien.

Exercice 80.— 1) On considère un groupe G de neutre e et A une partie finie stable non vide de G (i.e. Pour tout $a, b \in A$ on a $ab \in A$).

a) Soit $a \in A$. Montrer qu'il existe deux entiers distincts n et m tel que $a^n = a^m$. En déduire qu'il existe un entier $h > 0$ tel que $a^h = e$.
(Ind. On pourra considérer l'ensemble des puissances positives de a.)

b) Montrer que A est un sous-groupe de G.

2) (Application) On considère dans cette question le groupe multiplicatif $(\mathbb{C}^*,.)$. Pour tout entier $n \geq 1$ on note μ_n l'ensemble des racines n-ième de l'unité (i.e. l'ensemble des racines dans $\mathbb{C}$ du polynôme $X^n - 1$).

a) Montrer que pour tout $n \geq 1$, μ_n est un sous-groupe de $\mathbb{C}^*$.

b) Soit H un sous-groupe de $\mathbb{C}^*$ d'ordre n. Montrer que $H = \mu_n$.

c) On considère une partie finie non vide $A \subset \mathbb{C}^*$ stable pour la multiplication. En utilisant ce qui précède montrer qu'il existe un entier $n \geq 1$ tel que $A = \mu_n$.

Exercice 81.— *On considère le groupe additif* $\mathbb{Q}$.

1) Montrer que $\mathbb{Q}$ n'est pas monogène.
(Ind. Montrer que $\frac{1}{2n} \notin < \frac{m}{n} >$ pour tout $(m,n) \in \mathbb{Z} \times \mathbb{N}^*$.)

2) Montrer que $\mathbb{Q}$ est engendré par la famille $\left\{ \frac{1}{n!} / \ n \in \mathbb{N} \right\}$.

3) Montrer que tout sous-groupe monogène, non nul, de $\mathbb{Q}$ est infini.

4) Soient $(a,b),(c,d) \in \mathbb{Z} \times \mathbb{N}^*$, $H = < \frac{a}{b}, \frac{c}{d} >$ et $h = \text{pgcd}(ad, bc)$. Montrer que $H = \frac{h}{bd}\mathbb{Z}$.

5) En déduire que tout sous-groupe de type fini de $\mathbb{Q}$ est monogène et, par suite, que $\mathbb{Q}$ n'est pas de type fini.

Exercice 82.— On considère le groupe multiplicatif $(\mathbb{C}^*,.)$, le groupe additif $(\mathbb{R},+)$ et l'application

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{C}^* \\ & x & \longmapsto & e^{2i\pi x} \end{array}$$

1) Montrer que f est un morphisme et déterminer son noyau. On note $\mathbb{U} = \text{Im}(f)$ et on appelle ce groupe le "groupe circulaire". A quel groupe quotient est naturellement isomorphe $\mathbb{U}$? Décrire géométriquement l'ensemble $\mathbb{U}$ quand on regarde $\mathbb{C}$ comme le plan euclidien.

2) On considère l'ensemble

$$\Gamma_\infty = \{ z \in \mathbb{C}^* / \ \exists n \in \mathbb{N}^*, \ z^n = 1 \}$$

Justifier que Γ_∞ est un sous-groupe de $\mathbb{U}$ et montrer que $\Gamma_\infty \simeq \frac{\mathbb{Q}}{\mathbb{Z}}$ ($\mathbb{Q}$ et $\mathbb{Z}$ sont vu ici comme sous-groupes additif de $\mathbb{R}$).

3) Montrer, en utilisant ce qui précède, que $\frac{\mathbb{U}}{\Gamma_\infty} \simeq \frac{\mathbb{R}}{\mathbb{Q}}$.

Exercice 83.— On rappelle que le groupe diédral d'ordre $2n$ est le groupe D_n des isométries du plan laissant globalement invariant un n-polygone régulier.

1) Montrer que D_n est constitué d'exactement n rotations et n réflexions que l'on déterminera.

2) En déduire que D_n est isomorphe au produit semi-direct $\mathbb{Z}/n\mathbb{Z} \ltimes \mathbb{Z}/2\mathbb{Z}$ pour une action que l'on précisera.

3) Soit G un groupe engendré par deux éléments a et b tels que $o(b) = n$ et $o(a) = o(ab) = 2$. Montrer que $G \simeq D_n$.

4) a) En calculant explicitement, pour tout $x, y \in D_n$, le commutateur $[x,y]$, décrire le groupe dérivé $D(Dn)$ de D_n. A quel groupe usuel est alors isomorphe le groupe quotient $D_n/D(D_n)$?

b) Décrire explicitement le centre $Z(D_n)$ de D_n et montrer que si $n = 2k$ est pair alors $D_n/Z(D_n) \simeq D_k$.

Exercice 84.— Dans $GL_3(\mathbb{C})$ (i.e. le groupe multiplicatif des matrices 3×3 à coefficients complexes inversibles) on considère le sous-ensemble

$$\Gamma = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} / \ a,b,c \in \mathbb{C} \right\}$$

a) Montrer que Γ est un sous-groupe de $(GL_3(\mathbb{C}),.)$.

b) Décrire les éléments de $Z(\Gamma)$ (le centre de Γ) et montrer que $Z(\Gamma)$ est isomorphe au groupe additif $(\mathbb{C},+)$.

c) Prouver que l'application

$$\begin{array}{rccc} \theta : & \Gamma & \longrightarrow & \mathbb{C}\times\mathbb{C} \\ & \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} & \longmapsto & (a,c) \end{array}$$

est un épimorphisme de groupes. En déduire que le groupe quotient $\dfrac{\Gamma}{Z(\Gamma)}$ est isomorphe au groupe produit $(\mathbb{C},+)\times(\mathbb{C},+)$.

Exercice 85.— On appelle *application affine* de $\mathbb{R}$ toute application $f:\mathbb{R}\longrightarrow\mathbb{R}$ de la forme $f(x)=ax+b$ avec $(a,b)\in\mathbb{R}^*\times\mathbb{R}$. On note Aff($\mathbb{R}$) l'ensemble des applications affines de $\mathbb{R}$.

1) Montrer que toute application affine de $\mathbb{R}$ est bijective.

2) Prouver que Aff($\mathbb{R}$) est un groupe (on précisera la loi de composition interne).

On considère l'ensemble Trans($\mathbb{R}$) *des translations de* $\mathbb{R}$ *(i.e.* $f\in$ Trans($\mathbb{R}$) *si et seulement s'il existe* $b\in\mathbb{R}^*$ *tel que pour tout* $x\in\mathbb{R}$, $f(x)=x+b$*).*

3) Montrer que Trans($\mathbb{R}$) est un sous-groupe distingué de Aff($\mathbb{R}$) et que le groupe quotient Aff($\mathbb{R}$)/Trans($\mathbb{R}$) est isomorphe au groupe multiplicatif $(\mathbb{R}^*,.)$.
(Ind. Pour montrer l'isomorphisme annoncé on pourra utiliser le premier théorème d'isomorphisme et donc considérer un morphisme bien choisi.)

Exercice 86.— Montrer que pour tout entier $n\geq 3$, le centre $Z(S_n)$ du groupe symétrique S_n est trivial.

(Ind. On montrera qu'une permutation μ qui commute avec toutes les transpositions est nécessairement l'identité. A cet effet, on pourra raisonner par l'absurde en supposant qu'il existe $i\neq j$ tel que $\mu(i)=j$ et en composant μ par de bonnes transpositions.)

Exercice 87.— Soit A un anneau. Sur le groupe additif $A\times\mathbb{Z}$, on définit une multiplication par

$$(a_1,n_1)(a_2,n_2)=(a_1a_2+n_2a_1+n_1a_2,n_1n_2)$$

Montrer que, muni de cette loi, $A\times\mathbb{Z}$ est un anneau unitaire dans lequel A s'injecte.

Exercice 88.— On appelle centre d'un anneau $(A,+,.)$ l'ensemble des éléments $Z(A)=\{a\in A/\ \forall x\in A,\ x.a=a.x\}$.

a) Montrer que $Z(A)$ est un sous-anneau de A (est-ce un idéal?).

b) On suppose que pour tout $x\in A$, $x^2-x\in Z(A)$. Montrer que A est commutatif.

Exercice 89.— Soit A un anneau tel que pour tout $x\in A$ il existe un entier $n=n(x)>1$ tel que $x^n=x$. (On peut démontrer qu'un tel anneau est nécessairement commutatif).

a) Montrer que $x=0$ est le seul élément nilpotent de A (un élément $x\in A$ est dit nilpotent s'il existe $n\in\mathbb{N}$ tel que $x^n=0$).

b) i) Soient $a,b\in A$, montrer qu'il existe $r>1$ tel que $a^r=a$ et $b^r=b$

ii) En déduire que pour tout $a\in A$ et tout entier $k\geq 2$, il existe $r>1$ tel que $(k^r-k)a=0$.

iii) Prouver alors que le sous-groupe additif $<a>$ de A engendré par l'élément a est d'ordre $\nu(a)$ fini et que $\nu(a)$ est sans facteur carré (i.e. $\nu(a)$ n'est pas divisible dans $\mathbb{Z}$ par un carré autre que 1).

c) Prouver que s'il existe un élément dans A qui ne soit pas un diviseur de 0 alors A est unitaire.

Exercice 90.— On appelle élément nilpotent d'un anneau A, tout $a\in A$ tel que $a^n=0$ pour un certain entier $n\in\mathbb{N}$.

a) Donner des exemples d'anneaux possédant des éléments nilpotents.

b) On considère un anneau commutatif A et N le sous-ensemble de A constitué des éléments nilpotents de A. Montrer que N est un idéal de A et que A/N est un anneau qui ne possède pas d'élément nilpotent $\neq 0$.

Exercice 91.— Soit A un anneau commutatif et I un idéal de A. On appelle radical de I l'ensemble $Rad(I) = \{a \in A/\ \exists n \in \mathbb{N}^*,\ a^n \in I\}$. Montrer que $Rad(I)$ est un idéal de A qui contient I.

Exercice 92.— Soit A un anneau et I un idéal à gauche de A. On appelle annulateur de I l'ensemble $Ann(I) = \{a \in A/\ \forall x \in I,\ ax = 0\}$. Montrer que $Ann(I)$ est un idéal à gauche de A.

Exercice 93.— Soit A un anneau unitaire et $\mathcal{M}_n(A)$ l'ensemble des matrices carrés $n \times n$ à coefficients dans A.

a) Montrer que $\mathcal{M}_n(A)$ a naturellement une structure d'anneau unitaire pour des lois de composition internes que l'on précisera.

b) Pour tout $i, j \in \{1, \cdots, n\}$, on considère la matrice $E_{i,j}$ dont tous les coefficients sont nuls sauf celui de la ligne i et de la colonne j qui vaut 1. Pour $M \in \mathcal{M}_n(A)$ calculer le produit $E_{p,r}ME_{s,q}$.

c) En déduire que si J désigne un idéal de $\mathcal{M}_n(A)$ alors il existe un idéal I de A tel que $J = \mathcal{M}_n(I)$.

d) Montrer que si $A = K$ est un corps, alors $\mathcal{M}_n(K)$ est simple (i.e. ne possède pas d'idéaux non triviaux.

e) Donner des exemples d'idéaux à gauche (resp. à droite) de $\mathcal{M}_n(A)$ qui ne sont pas triviaux.

Exercice 94.— Soit A un anneau commutatif unitaire et M un idéal de A. Montrer que les propositions suivantes sont équivalentes :

i) M est maximal,

ii) $\forall x \in A - M,\ \exists y \in A,\ 1 - xy \in M$.

Exercice 95.— Soit A un anneau de caractéristique N. A tout entier $m \in \mathbb{N}$, on associe l'ensemble $I_m = \{x \in A/\ mx = 0\}$.

a) Vérifier que I_m est un idéal bilatère de A et que $I_m = I_d$ où $d = pgcd(N, m)$.

b) On suppose que $N = ab$ avec a et b des entiers premiers entre eux. Montrer que A est isomorphe à l'anneau produit $I_a \times I_b$.

Exercice 96.— Soit I un idéal d'un anneau commutatif A. On appelle racine de I l'ensemble

$$\sqrt{I} = \{a \in A/\ \exists n \in \mathbb{N},\ a^n \in I\}$$

a) Montrer que $\sqrt{I}$ est un idéal de A.

b) Soient I, J deux idéaux de A. Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$ et $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

c) L'idéal $\sqrt{\{0\}}$ est appelé le nilradical de A et les éléments de $\sqrt{\{0\}}$ sont appelés éléments nilpotents. Montrer que si I est un idéal de A et si $s : A \longrightarrow A/I$ désigne la surjection canonique, on a $\sqrt{I} = s^{-1}(\sqrt{\{0\}})$.

Exercice 97.— Soit A un anneau commutatif et unitaire.

1) Montrer que les deux propositions suivantes sont équivalentes :

i) l'ensemble des éléments non-inversibles de A forment un idéal,

ii) l'ensemble des idéaux stricts de A admet un plus grand élément (pour l'inclusion).

Dans cette situation, on dit que A est *quasi local*.

2) Soit A un anneau quasi local, montrer que A ne possède pas d'autres éléments idempotents que 0 et 1 (un élément $f \in A$ est dit idempotent si $f^2 = f$).

3) Montrer que si l'ensemble des idéaux principaux de A est totalement ordonné (pour l'inclusion), alors A est quasi local.

Exercice 98.— Soit A un anneau factoriel et $\mathcal{I}$ un système de représentants des éléments irréductibles de A. Soit $\mathcal{D} \subset \mathcal{I}$ et

$$S = \left\{ u \prod_{p \in I} p^{\alpha_p} / u \in U(A),\ I \text{ fini} \subset D,\ \forall p,\ \alpha_p \in \mathbb{N} \right\}$$

Dans le corps $K = \mathrm{Frac}(A)$, on considère la partie :

$$A[S^{-1}] = \left\{ \frac{a}{s},\ (a,s) \in A \times S \right\}$$

a) Montrer que $A[S^{-1}]$ est un sous-anneau de A.

b) Prouver que $A[S^{-1}]$ est factoriel et décrire les éléments irréductibles de $A[S^{-1}]$.

c) Appliquer ce résultat à $S = A - \mathcal{P}$ quand $\mathcal{P}$ est un idéal premier de A, à des situations classiques.

Exercice 99.— Soit A un sous-anneau unitaire de $\mathbb{Q}$.

a) Montrer que $\mathbb{Z} \subset A$.

b) On pose $S = \{x \in \mathbb{Z},\ x^{-1} \in A\}$. Montrer que si $\frac{a}{b} \in A$ avec $a, b \in \mathbb{Z}$ premiers entre eux, alors $b \in S$. En déduire que $A = \mathbb{Z}[S^{-1}]$. Quels sont les inversibles de A?

c) Déterminer les automorphismes d'anneaux de A.

d) Soit I un idéal de A. Montrer qu'il existe I_0 un idéal de $\mathbb{Z}$ tel que $I = I_0[S^{-1}]$. En déduire que A est principal.

Exercice 100.— Soit I, J deux idéaux d'un anneau principal A. Expliciter les idéaux $I \cap J$, $I + J$ et $I.J$ et dire quand ces derniers sont égaux.

Exercice 101.— Montrer qu'un anneau intègre fini à plus de deux éléments est un corps.

Exercice 102.— (Corps des quaternions d'Hamilton) On considère un $\mathbb{R}$-espace vectoriel V de dimension 4 rapporté à une base $e = (e_0, e_1, e_2, e_3)$. Dans V, on définit une loi de composition interne $(.)$ comme suit.
Pour x et y deux éléments de V, on écrit x et y dans la base e sous la forme:

$$\begin{array}{rcll} x & = & x_0e_0 + x_1e_1 + x_2e_2 + x_3e_3 & (x_0, x_1, x_2, x_3) \in \mathbb{R}^4 \\ y & = & y_0e_0 + y_1e_1 + y_2e_2 + y_3e_3 & (y_0, y_1, y_2, y_3) \in \mathbb{R}^4 \end{array}$$

On définit

$$\begin{array}{rcl} (x.y) & = & (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3)e_0 \\ & + & (x_0y_1 + x_1y_0 + x_2y_3 - x_3y_2)e_1 \\ & + & (x_0y_2 + x_2y_0 + x_3y_1 - x_1y_3)e_2 \\ & + & (x_0y_3 + x_3y_0 + x_1y_2 - x_2y_1)e_3 \end{array}$$

On note $\mathbb{H}$ l'espace vectoriel V muni (outre les lois spécifiques à la structure de $\mathbb{R}$-espace vectoriel de V) de la loi $(.)$. Les éléments de $\mathbb{H}$ s'appellent des quaternions.

a) Exprimer sous forme d'une table les produits $(e_i.e_j)$ pour $0 \leq i, j \leq 3$.

b) Montrer que $\mathbb{H}$ est une $\mathbb{R}$-algèbre unitaire non commutative. Montrer que l'ensemble des quaternions de la forme x_0e_0 est isomorphe au corps des réels. Par abus de langage et de notation les quaternions de la forme x_0e_0 seront notés x_0 et appelés réels. Montrer que les réels commutent avec tous les éléments de $\mathbb{H}$.

c) On considère le quaternion $q = x_0 + x_1e_1 + x_2e_2 + x_3e_3$. On appelle conjugué de q le quaternion $\bar{q} = x_0 - x_1e_1 - x_2e_2 - x_3e_3$. Quels sont les quaternions égaux à leurs conjugués? Pour r et q dans $\mathbb{H}$, exprimer $(\overline{r+q})$ et $\overline{rq}$ en fonction $\bar{r}$ et $\bar{q}$.

On appelle norme de q le quaternion $N(q) = q.\bar{q}$. Montrer que $N(q)$ est réel et exprimer $N(q)$ en fonction de x_0, x_1, x_2, x_3. A quelle condition a-t-on $N(q) = 0$? Calculer $N(rq)$ en fonction de $N(r)$ et $N(q)$.

d) Montrer que $\mathbb{H}$ est un corps et si $q \neq 0$, exprimer q^{-1} en fonction de $\bar{q}$ et $N(q)$.

e) On appelle quaternions purs les quaternions de la forme $x_1e_1 + x_2e_2 + x_3e_3$. Montrer que q est un quaternion pur si et seulement si q^2 est un réel négatif.

f) Pour $\alpha \in \mathbb{R}$, on note q_α le quaternion $\cos(\alpha)e_1 + \sin(\alpha)e_2$. Calculer q_α^2, en déduire que bien que $\mathbb{H}$ soit un corps le polynôme $X^2 + 1$ admet une infinité de racines. N'est-ce pas absurde?

Exercice 103.— On considère un corps K commutatif et dans K^2 on définit deux lois de composition interne "+" et ".": pour tous couples $(x, y) \in K^2$ et $(x', y') \in K^2$, on pose

$$\begin{array}{lcl}(x,y)+(x'+y') & = & (x+x', y+y') \\ (x,y).(x',y') & = & (xx'-yy', xy'+yx')\end{array}$$

On note alors L_K l'ensemble K^2 muni de ces deux lois.

1) On suppose K quelconque.

a) Montrer que L_K est un anneau commutatif et unitaire.

b) On suppose qu'il existe $\epsilon \in K$ tel que $\epsilon^2 = -1$. Trouver les diviseurs de 0 dans L_K. L_K est-il un corps?

c) Montrer que si $X^2 + 1$ n'a pas de racine dans K, L_K est un corps.

d) Appliquer ce résultat à $K = \mathbb{R}$.

2) On s'occupe maintenant du cas $K = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier.

a) On suppose que p est impair. Montrer que si un élément $\alpha \in K^*$ est le carré d'un élément de K^*, alors $\alpha^{\frac{p-1}{2}} = 1$.

En déduire que si $p + 1$ est divisible par 4, alors $L_{\mathbb{F}_p}$ est un corps.

b) Si $p = 2$, montrer que $L_{\mathbb{F}_2}$ n'est pas un corps.

c) Si $p = 4m + 1$, montrer que $\overline{(2m)!}$ est racine de $X^2 + 1$, en déduire que $L_{\mathbb{F}_p}$ n'est pas un corps.

d) Ecrire alors les tables des lois de $L_{\mathbb{F}_9}$.

Exercice 104.— Montrer que dans un corps fini, tout élément est somme de deux carrés.

Exercice 105.— Soit $K = \{x_1, \cdots, x_n\}$ un corps fini. Montrer que la K-algèbre des fonctions polynomiales sur K (i.e. les applications $f : K \to K$ tel qu'il existe un polynôme $P \in K[X]$ vérifiant $f(x) = P(x)$ pour tout $x \in K$) est isomorphe à $K[X]/(\Omega)$ où $\Omega(X) = (X - x_1)\cdots(X - x_n)$.

Que dire si K est infini?

Exercice 106.— Soit p un nombre premier et $a \in \mathbb{N}^*$, posons $q = p^a$. Montrer que toute application de $\mathbb{F}_q$ dans lui-même est polynomiale. Plus précisément, montrer que pour toute fonction $f : \mathbb{F}_q \to \mathbb{F}_q$, il existe un unique polynôme $P \in \mathbb{F}_q[X]$ de degré $\leq q - 1$ tel que $f(x) = P(x)$ pour tout $x \in \mathbb{F}_q$.

Exercice 4.— 1) On considère S le $\mathbb{C}$-espace vectoriel des suites complexes $u : \mathbb{N}^* \to \mathbb{C}$. On note e la suite définie par $e(1) = 1$ et pour tout $n \geq 2$, $e(n) = 0$ et, si u et v sont deux éléments de S, on définit le *produit de convolution* des suites u et v comme étant la suite $u * v$ définie pour $n \geq 1$ par

$$(u * v)(n) = \sum_{ab=n} u(a)v(b) = \sum_{d|n} u(n/d)v(d) = \sum_{d|n} u(d)v(n/d)$$

a) Montrer que muni du produit de convolution, S est une $\mathbb{C}$-algèbre commutative et unitaire.

b) Montrer qu'un élément $u \in S$ est inversible, pour $*$, si et seulement si $u(1) \neq 0$.

c) On définit la fonction de Möbius, $\mu \in S$, par

$$\begin{cases} \mu(1) & = & 1 & \\ \mu(p_1 \cdots p_k) & = & (-1)^k & \text{si } p_1, \cdots, p_k \text{ désigne des nombres premiers distincts} \\ \mu(n) & = & 0 & \text{sinon} \end{cases}$$

Prouver que μ est l'inverse, pour $*$, de la suite c constante égale à 1 (i.e. pour tout $n \geq 1$, $c(n) = 1$).

d) En déduire la *formule d'inversion de Möbius* : si f et g sont deux éléments de S tels que pour tout $n \geq 1$

$$g(n) = \sum_{d|n} g(d)$$

alors pour tout $n \geq 1$ on a

$$f(n) = \sum_{d|n} \mu(d) f(n/d) = \sum_{d|n} \mu(n/d) f(d)$$

2) (Application au dénombrement des polynômes irréductibles de $\mathbb{F}_q[X]$) Soient p un nombre premier et $a \in \mathbb{N}^*$, posons $q = p^a$.

a) Montrer qu'il existe, pour tout entier $n \in \mathbb{N}^*$, des polynômes irréductibles de degrés n dans $\mathbb{F}_q[X]$.

b) Montrer que si $P \in \mathbb{F}_q[X]$ est un polynôme irréductible de degré n, alors P divise $X^{q^n} - X$.

c) Pour $j \in \mathbb{N}^*$, notons $Irr(q, j)$ l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_q[X]$ de degré j. Montrer que

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in Irr(q,d)} P(X)$$

Exercice 107.— (Théorème de Chevalley-Warning) Soit p un nombre premier et q une puissance non nulle de p. On considère un ensemble fini d'indices I et, pour tout $i \in I$, $f_i \in \mathbb{F}_q[X_1, \cdots, X_n]$ un polynôme à n indéterminées. On note $V \subset \mathbb{F}_q^n$ l'ensemble des zéros communs aux f_i.

a) Montrer que le polynôme

$$P[X_1, \cdots, X_n] = \prod_{i \in I} \left(1 - f_i^{q-1}(X_1, \cdots, X_n)\right)$$

est la fonction caractéristique de V.

Pour tout polynôme $f \in \mathbb{F}_q[X_1, \cdots, X_n]$, on pose $S(f) = \sum_{(x_1, \cdots, x_n) \in \mathbb{F}_q^n} f(x_1, \cdots, x_n)$.

b) Montrer que $\sharp V \equiv S(P) \bmod(p)$.

c) Déterminer la valeur de la somme $\sum_{x \in \mathbb{F}_q} x^k$ en fonction de l'entier $k > 0$, en distinguant le cas où k est divisible par $q - 1$.

d) Montrer que si $\sum_{i \in I} \mathrm{d}^\circ f_i < n$ alors $S(P) = 0$.

e) En déduire que, si $\sum_{i \in I} \mathrm{d}^\circ f_i < n$ et que les f_i sont sans terme constant, alors les f_i possèdent un zéro non trivial en commun.

Exercice 108.— Soit p un nombre premier et n et r deux entier > 0.

a) Montrer que si r est premier avec $p^n - 1$, tout élément de $\mathbb{F}_{p^n}$ est une puissance r-ième.

b) Montrer que si r divise $p^n - 1$ et si $\alpha \in \mathbb{F}_{p^n}{}^*$, alors les propositions suivantes sont équivalentes :

i) α est une puissance r-ième,

ii) $\alpha^{(p^n-1)/r} = 1$.