Première année du Master
Métiers de l'enseignement, de l'éducation et de la formation
mention second degré - parcours mathématiques
Université de Rennes 1

Quelques exercices d'arithmétique

Jean-Marie Lion

Version du 4 février 2014

Thèmes abordés

Arithmétique : $\mathbf{Z}$, $\mathbf{Z}/n\mathbf{Z}$, division euclidienne, Bezout, Gauss, nombres premiers, décomposition des entiers en produits de nombres premiers, Fermat, Mersenne, équations diophantiennes, indicatrice d'Euler, la méthode RSA, irrationalité de $\sqrt{2}$ et $\exp 1$, représentations des nombres entiers, rationnels et réels, $SL_2(\mathbf{Z})$, sous-groupes de $\mathbf{R}$

Bibliographie

- Théorie des fonctions, Georges Valiron (Masson, 1941)
- Math, nouvelle collection Durrande, TC (classiques TV, 1979)
- Cours de mathématiques spéciales, Ramis, Deschamps, Odoux (Masson, 1983)
- Cours d'algèbre, Daniel Perrin (École normale supérieure de jeunes filles, 1981)
- Pour l'honneur de l'esprit humain, Jean Dieudonné (Hachette 1987)
- Seconde épreuve du Capes externe de mathématiques, 2003
- Wikipedia (`http://fr.wikipedia.org`)
- Images des mathématiques (`http://images.math.cnrs.fr`)
- le site du ministère de l'éducation nationale (`http://eduscol.education.fr/`)
- internet, avec discernement (liste non exhaustive) :
  - `http://www.bibmath.net/`
  - `http://www.math.jussieu.fr/~keller/`
  - `http://www.math.jussieu.fr/~thomas/`
  - `http://mathtous.perso.sfr.fr/`
  - `http://serge.mehl.free.fr/`
  - `http://villemin.gerard.free.fr/`

Rappel du programme d'arithmétique de TS (spécialité maths)

Contenus : divisibilité dans $\mathbf{Z}$, division euclidienne, congruences dans $\mathbf{Z}$, pgcd de deux entiers, entiers premiers entre eux, théorème de Bézout, théorème de Gauss, nombres premiers, existence et unicité de la décomposition en produit de facteurs premiers
Exemple de problèmes : problèmes de codage (codes barres, code ISBN, clé du Rib, code Insee) - problèmes de chiffrement (chiffrement affine, chiffrement de Vigenère, chiffrement de Hill) - questionnement sur les nombres premiers : infinitude, répartition, tests de primalité, nombres premiers particuliers (Fermat, Mersenne, Carmichaël) - sensibilisation au système cryptographique RSA.

Exercice 1.
Soient a et b deux entiers relatifs. Montrer que si $b \neq 0$ il existe un unique couple $(q,r) \in \mathbf{Z} \times \mathbf{N}$ tels que $a = qb + r$ et $0 \leq r < |b|$ (les nombres q et r sont le quotient et le reste de la division euclidienne de a par b).

Exercice 2.
Expliquer l'algorithme suivant :

```
Ecrire "Entrez A puis B"  |  Si A<0 Alors           |  TanQue A>=B Faire
Lire A                    |  Remplacer A par -A     |  Remplacer A par A-B
Lire B                    |  Remplacer S par -S     |  Remplacer Q par Q+S
S=1                       |  Remplacer T par -T     |  FinTantQue
T=1                       |  FinSi                  |  Si T<0 et A>0 Alors
Q=0                       |  Si B<0 Alors           |  Remplacer A par B-A
                          |  Remplacer B par -B     |  Remplacer Q par Q+S
                          |  Remplacer S par -S     |  FinSi
                          |  FinSi                  |  Ecrire Q
                          |                         |  Ecrire A
                          |                         |  Fin
```

Exercice 3.
Un idéal de $\mathbf{Z}$ est un sous-ensemble non vide I de $\mathbf{Z}$ tels que

$$\forall n \in I, -n \in I$$
$$\forall (n,m) \in I, n+m \in I$$
$$\forall n \in I, \forall k \in \mathbf{Z}, kn \in I.$$

1. Soit $I \subset \mathbf{Z}$. Montrer que I est un sous-groupe de $\mathbf{Z}$ si et seulement si I est un idéal de $\mathbf{Z}$.
2. Montrer que si $n \in \mathbf{Z}$ alors $n\mathbf{Z} = I = \{kn : k \in \mathbf{Z}\}$ est un idéal de $\mathbf{Z}$.
Soit I un idéal de $\mathbf{Z}$ différent de $\{0\}$.
3. Montrer que $I^{+*} = \{k : k \in I \text{ et } k > 0\}$ est non vide.
4. Montrer que I^{+*} admet un plus petit élément noté n.
5. Montrer que

$$I^{+*} = \{kn : k \in \mathbf{N}^*\}.$$

6. Montrer que $I = n\mathbf{Z}$.

Exercice 4.
Soit G un groupe de neutre e. Soit $g \in G$. On pose $g^0 = e$ et on note g^{-1} l'inverse de g. On définit par récurrrence sur $n \in \mathbf{N}$ g^n et g^{-n} en posant $g^{n+1} = g^n \cdot g$ et $g^{-(n+1)} = g^{-n} \cdot g^{-1}$.
1. Montrer que $\psi : \mathbf{Z} \to G$ définie par $\psi(n) = g^n$ est un morphisme de groupe.
2. Montrer que $< g >= \{g^n : n \in \mathbf{Z}\}$ est un sous-groupe de G : c'est le groupe engendré par g et si $G =< g >$ on dit que G est monogène ou cyclique.
L'ordre de g est le cardinal de $< g >$ et l'ordre de G est son cardinal.
3. Montrer que $Z = \{n \in \mathbf{Z} : g^n = e\}$ est un sous-groupe de $\mathbf{Z}$.
4. Montrer que si $Z = \{0\}$ alors ψ est injective et $< g >$ est infini.
5. On suppose $Z \neq \{0\}$. Montrer que Z^{+*} est non vide et que le cardinal de $< g >$ est égal au plus petit élément de Z^{+*}.

Exercice 5.
théorème de Lagrange
Soit G un groupe fini et soit H un sous-groupe de G.
1. Montrer que si $a \in G$ alors l'application de G dans G qui à $g \in G$ associe ag est une bijection. Quelle est sa réciproque ?
2. Montrer que la relation $\mathcal{R}$ définie sur G par $a\mathcal{R}b$ si et seulement si $a^{-1}b \in H$ est une relation d'équivalence.
3. Montrer que si $a \in G$ la classe $\overline{a}^{\mathcal{R}}$ de a pour $\mathcal{R}$ est

$$\overline{a}^{\mathcal{R}} = \{ah : h \in H\} = aH.$$

4. Montrer que si $a \in G$ alors $\overline{a}^{\mathcal{R}}$ et H ont même cardinal.
5. Montrer que l'ordre de H (i.e. son cardinal) divise l'ordre de G.

Exercice 6.

pgcd
Soient a et b deux entiers relatifs.
1. Montrer que le sous-ensemble

$$a\mathbf{Z}+b\mathbf{Z}=\{ua+vb : (u,v)\in\mathbf{Z}^2\}$$

est un idéal de $\mathbf{Z}$.
2. En déduire qu'il existe $c\in\mathbf{N}$ tel que $a\mathbf{Z}+b\mathbf{Z}=c\mathbf{Z}$.
Le nombre c ainsi obtenu est noté $pgcd(a,b)$.
3. Montrer que a et b sont des multiples de c.
4. Soit $d\in\mathbf{Z}$. Montrer que si d divise a et b alors d divise c.
5. Montrer que 1 et -1 sont les seuls diviseurs communs à a et b (a et b sont premiers entre eux) si et seulement s'il existe u et v dans $\mathbf{Z}$ tels que $ua+vb=1$ (identité de Bezout).
On suppose a non nul.
6. Montrer que c est non nul et que c divise a et b.
7. Montrer que c est bien le plus grand diviseur commun à a et b au sens de la relation d'ordre usuel.

Exercice 7.
ppcm
Soient a et b deux entiers relatifs.
1. Montrer que le sous-ensemble $a\mathbf{Z}\cap b\mathbf{Z}$ est un idéal de $\mathbf{Z}$.
2. En déduire qu'il existe $d\in\mathbf{N}$ tel que $a\mathbf{Z}\cap b\mathbf{Z}=d\mathbf{Z}$.
Le nombre d ainsi obtenu est noté $ppcm(a,b)$.
3. Montrer que d est un multiple de a et b.
4. Montrer que tout multiple de a et b est un multiple de d.
5. Montrer que si $a=ca'$, $b=cb'$ avec $c=pgcd(a,b)$ alors $d=ppcm(a,b)=ca'b'$.
6. Montrer que d est bien le plus petit multiple commun (naturel) à a et b au sens de l'ordre usuel.

Exercice 8.
algorithme d'Euclide
Soient $(p,q)\in\mathbf{N}\times\mathbf{N}^*$. On considère la suite r définie par récurrence de la façon suivante :
- $r_{-2}=p$ et $r_{-1}=q$
- si $r_{n-1}=0$ alors $r_n=0$ et si $r_{n-1}\neq 0$ alors r_n est le reste de la division euclidienne de r_{n-2} par r_{n-1}.
1. Montrer que si $r_{n-1}\neq 0$ alors $r_n<r_{n-1}$ et $pgcd(p,q)=pgcd(r_{n-1},r_n)$.
2. Montrer que si $n>p$ alors $r_n=0$.
3. Montrer qu'il existe N tel que $r_N\neq 0$ mais $r_{N+1}=0$.
4. Montrer que $pgcd(p,q)=r_N$.

Exercice 9.
Soit $a,b\in\mathbf{Z}$. Donner un algorithme pour trouver $pgcd(a,b)$ et $u,v\in\mathbf{Z}$ tels que $ua+vb=pgcd(a,b)$.

Exercice 10.
écriture réduite des rationnels
Soit r un rationnel strictement positif : $r=\dfrac{a}{b}$ avec $(a,b)\in\mathbf{N}^*\times\mathbf{N}^*$.
1. Soit $(a',b')\in\mathbf{N}^*\times\mathbf{N}^*$. Montrer que $r=\dfrac{a'}{b'}$ si et seulement si $ab'-a'b=0$.
2. Montrer qu'il existe $(A,B)\in\mathbf{N}^*\times\mathbf{N}^*$ unique tel que $pgcd(A,B)=1$ et $r=\dfrac{A}{B}$ (écriture réduite).
3. Soit r d'écriture réduite $r=\dfrac{A}{B}$ et s d'écriture réduite $s=\dfrac{C}{D}$. On pose $B=B'P$ et $D=D'P$ avec $P=pgcd(B,D)$. Montrer que l'écriture réduite de $r+s$ est de la forme $r+s=\dfrac{E}{F}$ avec $F=B'D'Q$.
4. Soient $p_1,...,p_k$ des nombres premiers. Montrer que $\dfrac{1}{p_1}+...+\dfrac{1}{p_k}$ n'est pas entier.

Exercice 11.
Soit $n \in \mathbf{N}^*$. Soit la relation $\equiv_n$ définie sur $\mathbf{Z}$ par $a \equiv_n b$ si et seulement si n divise $a-b$.
1. Montrer que $\equiv_n$ est une relation d'équivalence.
Lorsque $a \equiv_n b$ on dit que a est congru à b modulo n qu'on peut écrire $a \equiv b(n)$ ou $a \equiv b$ modulo n.
2. Montrer que si $a \in \mathbf{Z}$ alors le reste a' de la division euclidienne de a par n vérifie $a \equiv_n a'$.
3. Montrer que la relation $\equiv_n$ possède exactement n classes d'équivalence, chacune d'elles possèdant un unique représentant parmi les entiers compris entre 0 et $n-1$.
On note $\mathbf{Z}/n\mathbf{Z}$ l'ensemble des classes déquivalence de $\equiv_n$ et si $a \in \mathbf{Z}$ on note $\overline{a}^n$ la classe de a pour $\equiv_n$ (appelée aussi classe de a modulo n).
4. Montrer que si $a \equiv_n b$ et $k \in \mathbf{Z}$ alors $a+k \equiv_n b+k$ et $k \times a \equiv_n k \times b$.
5. Montrer que si $a \equiv_n b$, $c \equiv_n d$ et $k \in \mathbf{Z}$ alors $\overline{a+c}^n = \overline{b+d}^n$ et $\overline{k \times a}^n = \overline{k \times b}^n$.
6. Montrer que $\mathbf{Z}/n\mathbf{Z}$ peut être muni de deux lois $+_n$ et $\times_n$ telles que
- $(\mathbf{Z}/n\mathbf{Z}, +_n, \times_n)$ est un anneau commutatif,
- l'application de $\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ est un morphisme d'anneau.

Exercice 12.
les générateurs de $\mathbf{Z}/n\mathbf{Z}$
Soit $n \in \mathbf{N}^*$ et soit $m \in \mathbf{Z}$. Montrer que $\overline{m}^n$ est un générateur de $\mathbf{Z}/n\mathbf{Z}$ (i.e. $< \overline{m}^n >= \mathbf{Z}/n\mathbf{Z}$ ou encore $\overline{m}^n$ est d'ordre n) si et seulement si $pgcd(n,m) = 1$.

Exercice 13.
les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$
Soit $n \in \mathbf{N}^*$.
1. Soit $d \in \mathbf{N}^*$ tel que d divise n et soit $m \in \mathbf{N}$ le quotient de n par d. Montrer que la classe $\overline{m}^n$ engendre un sous-groupe G_d de $\mathbf{Z}/n\mathbf{Z}$ isomorphe au groupe $\mathbf{Z}/d\mathbf{Z}$.
2. Soit $m \in \mathbf{Z}$. Montrer que $< \overline{m}^n >=< \overline{\tau}^n >$ où $\tau = pgcd(n,m)$.
Soit G un sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ non réduit à $\{0\}$ et soit $m \in \mathbf{N}$ le plus petit entier strictement positif dont la classe modulo n appartient à G.
3. Soit $b \in \mathbf{N}$ tel que $\overline{b}^n \in G$ et soit q et r le quotient et le reste de la division euclidienne de b par m. Montrer que $\overline{r}^n \in G$.
4. Montrer que m divise n.
5. Montrer que $G =< \overline{m}^n >$ est isomorphe à $\mathbf{Z}/d\mathbf{Z}$ où d est le quotient de n par m.
On note D l'ensemble des diviseurs de n. Pour tout d dans D on note O_d l'ensemble des éléments d'ordre d de $\mathbf{Z}/n\mathbf{Z}$ et on note $\phi(d)$ le nombre d'éléments d'ordre d de $\mathbf{Z}/d\mathbf{Z}$ (indicatrice d'Euler).
6. Montrer que si $d, d' \in D$ et $d \neq d'$ alors O_d et $O_{d'}$ sont disjoints.
7. Montrer que

$$\mathbf{Z}/n\mathbf{Z} = \bigcup_{d \in D} O_d.$$

8. Montrer que

$$n = \sum_{d \in D} \phi(d).$$

Exercice 14.
théorème des restes chinois
Soient $n, m \in \mathbf{N}^*$.
1. Soient $a, b \in \mathbf{Z}$. Montrer que si $a \equiv_{mn} b$ alors $a \equiv_m b$ et $a \equiv_n b$.
2. Montrer que l'application $\theta = (\theta_1, \theta_2)$ de $\mathbf{Z}/mn\mathbf{Z}$ dans $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ définie par

$$\theta(\overline{a}^{mn}) = (\overline{a}^m, \overline{a}^n) \text{ si } a \in \mathbf{Z}$$

est un morphisme de groupe.
3. On suppose que $pgcd(m,n) \neq 1$. Montrer qu'il existe $a \in \mathbf{Z}$ tel que $a \equiv_m 0$ et $a \equiv_n 0$ mais $a \not\equiv_{mn} 0$ et en déduire que θ n'est ni injectif ni surjectif.

On suppose que $pgcd(m,n) = 1$ et on considère $u, v \in \mathbf{Z}$ tels que $um + vn = 1$.
4. Soient $a, b \in \mathbf{Z}$. Montrer que si $a \equiv_m b$ et $a \equiv_n b$ alors $a \equiv_{mn} b$ et en déduire que θ est un isomorphisme de groupe.
5. Soient $a, b \in \mathbf{Z}$.
5.a. Montrer que $c = avn + bum$ vérifie $c \equiv_m a$ et $c \equiv_n b$.
5.b. Montrer que $d \in \mathbf{Z}$ vérifie $d \equiv_m a$ et $d \equiv_n b$. si et seulement si $d - c \equiv_0 mn$.
6. Montrer que si g est un générateur de $\mathbf{Z}/mn\mathbf{Z}$ alors $\theta_1(g)$ et $\theta_2(g)$ sont des générateurs de $\mathbf{Z}/m\mathbf{Z}$ et $\mathbf{Z}/n\mathbf{Z}$.
7. Soit $(a,b) \in \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ avec a générateur de $\mathbf{Z}/m\mathbf{Z}$ et b générateur de $\mathbf{Z}/n\mathbf{Z}$. Montrer que l'unique $c \in \mathbf{Z}/mn\mathbf{Z}$ tel que $\theta(c) = (a,b)$ est un générateur de $\mathbf{Z}/mn\mathbf{Z}$.
8. Montrer que le nombre $\phi(mn)$ de générateurs de $\mathbf{Z}/mn\mathbf{Z}$ est égal au produit $\phi(m)\phi(n)$ du nombre de générateurs de $\mathbf{Z}/m\mathbf{Z}$ par le nombre de générateurs de $\mathbf{Z}/n\mathbf{Z}$.
9. Montrer que si $m_1, ..., m_k$ sont deux à deux premiers entre eux alors :
- $\mathbf{Z}/m_1 \cdot ... \cdot m_k\mathbf{Z}$ est isomorphe à $\mathbf{Z}/m_1\mathbf{Z} \times ... \times \mathbf{Z}/m_k\mathbf{Z}$
- $\phi(m_1 \cdot ... \cdot m_k) = \phi(m_1) \cdot ... \cdot \phi(m_k)$.

Exercice 15.
l'indicatrice d'Euler
Soit n un entier supérieur ou égal à 2. On ote $\phi(n)$ le nombre de générateurs de $\mathbf{Z}/n\mathbf{Z}$ c'est à dire le nombre d'entiers naturels premiers avec n et plus petits que n.
1. Montrer que si n est premier (i.e. sans diviseurs autres que 1 et lui même dans $\mathbf{N}$) alors $\phi(n) = n - 1$.
2. On suppose $n = p^r$ avec p premier et $r \in \mathbf{N}$ supérieur ou égal à 2.
2.a. Soit m un entier compris entre 1 et n. Montrer que si m et p ne sont pas premier entre eux alors p divise m.
2.b. Montrer qu'il y a p^{r-1} entiers m non premiers avec n et compris entre 1 et n.
2.c. En déduire

$$\phi(n) = \phi(p^r) = (p^r - p^{r-1}) = n\left(1 - \frac{1}{p}\right).$$

3. On suppose que $n = p_1^{r_1} \cdot ... \cdot p_1^{r_k}$. Montrer que

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot ... \cdot \left(1 - \frac{1}{p_k}\right).$$

Exercice 16.
Soit p un nombre premier, c'est à dire un entier relatif qui admet exactement quatre diviseurs dans $\mathbf{Z}$.
1. Soit $a \in \mathbf{Z}/p\mathbf{Z}^*$. Montrer qu'il existe $b \in \mathbf{Z}^*$ tel que $ab \equiv_p 1$.
2. Montrer que $(\mathbf{Z}/p\mathbf{Z}, +_p, \times_p)$ est un corps.
3. Soit $n \in \mathbf{N}^*$. Montrer que si $(\mathbf{Z}/n\mathbf{Z}, +_n, \times_n)$ est un corps alors n est premier.

Exercice 17.
On munit le groupe $(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, +)$ d'une deuxième loi notée $\times$ et définie de la façon suivante :

$\times$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(1,1)$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$(1,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,1)$	$(0,0)$	$(0,1)$	$(1,1)$	$(1,0)$

1. La loi $\times$ admet-elle un neutre et un élément absorbant ?
2. Vérifier que tout élément autre que $(0,0)$ est inversible.
3. Comment déduire de la table que $\times$ est commutative ?
4. Vérifier que la loi $\times$ est associative.

5. Comment déduire de la table que $\times$ est distributive par rapport à $+$?
6. Que conclure sur $(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, +, \times)$?

Exercice 18.
Soit $n \in \mathbf{N}$.
1. Montrer que si $p \in \mathbf{N}$ premier divise $1+n!$ alors $p > n$.
2. Montrer qu'il existe une infinité de nombres premiers.
On suppose $n \geq 2$.
3. Montrer que si $k \in \mathbf{N}$ et $2 \leq k \leq n$ alors k divise $n!+k$.
4. Montrer que pour tout $\alpha, \beta > 0$ il existe p, q premiers tels que $\alpha < p < q$ et $\beta < q - p$.

Exercice 19.
Soit A l'ensemble des entiers naturels congrus à 3 modulo 4.
1. Montrer que A est non vide.
2. Soient $p_1, ..., p_k \in A$. On pose $P = 4p_1 \cdot ... \cdot p_k - 1$.
2.a. Montrer que si $i = 1, ..., k$ alors $pgcd(P, p_i) = 1$.
2.b. Montrer que l'ensemble E des entiers naturels congrus à 1 modulo 4 est stable par multiplication : si $m, n \in E$ alors $mn \in E$.
2.c. Montrer que si p premier divise P alors $p \in A \setminus \{p_1, ..., p_k\}$.
2.d. Montrer qu'il existe une infinité d'entiers naturels congrus à 3 modulo 4.

Exercice 20.
Soit $n \in \mathbf{N}$. Donner un algorithme de calcul des nombres premiers inférieurs ou égaux à n.

Exercice 21.
lemme de Gauss, par Bezout
Soient $a, b, c \in \mathbf{N}$. On suppose que $pgcd(a, c) = 1$.
1. Montrer qu'il existe $u, v \in \mathbf{Z}$ tels que $ua + vc = 1$.
2. En déduire qu'il existe $U, V \in \mathbf{Z}$ tels que $b = Uab + Vc$.
3. Montrer que si c divise ab et $pgcd(a, c) = 1$ alors c divise b (lemme de Gauss).

Exercice 22.
lemme d'Euclide, preuve de Gauss
Soient $a, b, p \in \mathbf{N}$ avec p premier divisant ab. L'objet de l'exercice est de montrer que p divise a ou b sans avoir recours au lemme de Gauss. On raisonne par l'absurde en montrant que l'hypothèse p ne divise ni a ni b mène à une contradiction.
On suppose $pgcd(p, a) = pgcd(p, b) = 1$.
1. Vérifier que $E = \{n \in \mathbf{N} : pgcd(p, n) = 1 \text{ et } p \text{ divise } nb\}$ est non vide et possède un plus petit élément noté A.
2. Soient Q et R le quotient et le reste de la division euclidienne de A par p : $A = pQ + R$, $Q, R \in \mathbf{N}$ et $0 \leq R < p$. Calculer Rb en fonction de p, Q, A et b et en déduire que $R \in E$.
3. Montrer que $A = R$ et $0 < A < p$.
4. Soient q et r le quotient et le reste de la division euclidienne de p par A : $p = Aq + r$, $q, r \in \mathbf{N}$ et $0 \leq r < A$. Calculer rb en fonction de p, q, A et b et en déduire que $r \in E$.
5. Quelle est la contradiction obtenue ?

Exercice 23.
Montrer que $4^{15} - 4$ est divisible par 15.

Exercice 24.
racines entières
Soit $n, d \in \mathbf{N}$ avec $n, d \geq 2$. On suppose qu'il existe $p, q \in \mathbf{N}$ avec $pgcd(p, q) = 1$ tels que $\left(\frac{p}{q}\right)^d = n$.
1. Montrer que q divise p.

2. En déduire que $q = 1$ et que $n = p^d$.
3. Etudier la rationalité de $\sqrt{2}$ et de $6^{\frac{1}{5}}$.

Exercice 25.
décomposition en facteurs premiers
1. Montrer par récurrence que si $n \in \mathbf{N}$ et $n \geq 2$ il existe un unique $m \in \mathbf{N}^*$ et un unique m-uplet $(p_1, ..., p_m)$ tels que
- les p_k sont des nombres premiers positifs,
- $p_1 \leq ... \leq p_m$,
- $n = p_1 \cdot ... \cdot p_m$.
2. Etendre ce résultat à $\mathbf{Z}$.

Exercice 26.
1. Si $n \in \mathbf{N}^*$ on pose $S_n = \sum_{k=1}^{n} \frac{1}{k}$.
1.a. Montrer que $S_{2n} = \frac{S_n}{2} + \sum_{k=0}^{n-1} \frac{1}{2k+1}$.
1.b. Montrer qu'il existe $a_n, b_n \in \mathbf{N}$ tels que $\sum_{k=0}^{n-1} \frac{1}{2k+1} = \frac{a_n}{2b_n+1}$.
1.c. Montrer que s'il existe $p_n, q_n \in \mathbf{N}$ tels que $S_n = \frac{2p_n+1}{2q_n}$ alors il existe $p_{2n}, q_{2n}, p_{2n+1}, q_{2n+1} \in \mathbf{N}$ tels que $S_{2n} = \frac{2p_{2n}+1}{2q_{2n}}$ et $S_{2n+1} = \frac{2p_{2n+1}+1}{2q_{2n+1}}$.
1.d. Montrer par l'absurde que pour tout $n \neq 1$ il existe $p_n, q_n \in \mathbf{N}$ tels que $S_n = \frac{2p_n+1}{2q_n}$.
2. Soit $n > 1$ fixé.
2.a. Montrer qu'il existe $d \in \mathbf{N}^*$ tel que $2^d \leq n < 2^{d+1}$.
2.b. Soit $k \in \mathbf{N}$, $1 \leq k \leq n$ et $k \neq 2^d$. Montrer que k n'est pas un multiple de 2^d.
2.c. Montrer qu'il existe $a_n, b_n \in \mathbf{N}$ tels que $S_n = \frac{a_n}{2^{d-1}(2b_n+1)} + \frac{1}{2^d}$.
2.d. En déduire qu'il existe $p_n, q_n \in \mathbf{N}$ tels que $S_n = \frac{2p_n+1}{2^d q_n}$.
3. Montrer que $S_n \notin \mathbf{N}$ si $n \neq 1$.

Exercice 27.
valuation
Soit p un nombre premier. Si $n \in \mathbf{Z}^*$ on note $v_p(n)$ et on appelle valuation p-adique l'exposant de p dans la décomposition en facteurs premiers de p. Si $r = \frac{a}{b} \in \mathbf{Q}^*$ on pose $v_p(r) = v_p(a) - v_p(b)$. Enfin on pose $v_p(0) = \infty$.
1. Montrer que $v_p(r)$ pour $r \in \mathbf{Q}^*$ est bien définie : elle ne dépend pas du représentant de r.
2. Prouver $v_p(rs) = v_p(r)v_p(s)$ si $r, s \in \mathbf{Q}^*$.
3. Prouver $v_p(r+s) \geq \min(v_p(r), v_p(s))$ si $r, s \in \mathbf{Q}$.
4. Soit $r, s \in \mathbf{Q}$ tels que $v_p(r) < v_p(s)$. Calculer $v_p(r+s)$.
5. Calculer $v_p(pgcd(a,b))$ et $v_p(ppcm(a,b))$ en fonction de $v_p(a)$ et $v_p(b)$ si $a, b \in \mathbf{Z}^*$.
6. Soit $r \in \mathbf{Q}$. Montrer que $r \in \mathbf{Q} \setminus \mathbf{Z}$ si et seulement s'il existe p premier tel que $v_p(r) < 0$.
7. Soient $p_1, ..., p_n$ des nombres premiers distincts et $a_1, ..., a_n \in \mathbf{Z}$ tels que a_k premier avec p_k si $k = 1, ..., n$. Montrer que $\frac{a_1}{p_1} + ... + \frac{a_n}{p_n}$ n'appartient pas à $\mathbf{Z}$.
8. Soit $n > 1$. Montrer que $v_2(1 + \frac{1}{2} + ... + \frac{1}{n}) < 0$ et en déduire que $1 + \frac{1}{2} + ... + \frac{1}{n}$ n'est pas entier.

Exercice 28.

petit théorème de Fermat par Leibniz, Gauss
On rappelle que si $d \in \mathbf{N}$ alors

$$(x+1)^d = \sum_{k=0}^{d} \frac{d!}{k!(d-k)!} x^k$$

et

$$\frac{d!}{k!(d-k)!} \in \mathbf{N} \text{ si } k \in \mathbf{N} \text{ et } 0 \leq k \leq d.$$

Soit p un nombre premier.

1. Soit $k \in \mathbf{N}$. Montrer que si $0 < k < p$ alors l'entier $\frac{p!}{k!(p-k)!}$ est divisible par p.
2. Soit $n \in \mathbf{Z}$. Montrer que $(n+1)^p \equiv_p n^p + 1$.
3. Soit $n \in \mathbf{Z}$. Montrer que $n^p \equiv_p n$.
4. Soit $n \in \mathbf{Z}$ non multiple de p. Montrer que $n^{p-1} \equiv_p 1$.

Exercice 29.
petit théorème de Fermat, deuxième preuve
Soit p un nombre premier.
1. Soit $a \in \mathbf{Z}/p\mathbf{Z}^*$. Montrer que l'application ψ de $\mathbf{Z}/p\mathbf{Z}$ dans lui même qui à $b \in \mathbf{Z}/p\mathbf{Z}$ associe ab est une bijection.
2. Vérifier que $\psi(\mathbf{Z}/p\mathbf{Z}^*) = \mathbf{Z}/p\mathbf{Z}^*$;
3. Montrer que $(a \cdot 1) \cdot \ldots \cdot (a \cdot (p-1)) \equiv_p 1 \cdot \ldots \cdot (p-1)$.
4. Vérifier que $pgcd(p, 1 \cdot \ldots \cdot (p-1)) = 1$ et que

$$(a \cdot 1) \cdot \ldots \cdot (a \cdot (p-1)) = a^{p-1} \cdot (1 \cdot \ldots \cdot (p-1)).$$

5. En déduire que $a^{p-1} \equiv_p 1$.

Exercice 30.
petit théorème de Fermat par Euler
Soit $n \in \mathbf{N}^*$. Soit E_n l'ensemble des entiers compris entre 1 et $n-1$ et qui sont premiers avec n. On note $\phi(n)$ le cardinal de E_n. On considère un élément a de E_n.
1. Montrer que si $b \in E_n$ alors il existe un unique élément de E_n congru à ab modulo n.
Si $b \in E_n$ on note $p(b)$ l'unique élément de E_n congru à ab modulo n.
2. Montrer que si $b, c \in E_n$ et $b \neq c$ alors $p(b) \neq p(c)$.
3. Montrer que

$$\prod_{b \in E_n} (a \cdot b) \equiv_n \prod_{b \in E_n} b.$$

4. Vérifier que

$$pgcd(n, \prod_{b \in E_n} b) = 1$$

et que

$$\prod_{b \in E_n} (a \cdot b) = a^{\phi(n)} \prod_{b \in E_n} b.$$

5. En déduire que $a^{\phi(n)} \equiv_n 1$.

Exercice 31.
Wilson d'après Gauss
Soit n un entier naturel supérieur ou égal à 2.
1. Montrer que $1! \equiv_2 -1$, $2! \equiv_3 -1$, $3! \equiv_4 2$, $4! \equiv_5 -1$, $5! \equiv_6 0$ et $6! \equiv_7 -1$.
2. On suppose $n > 4$ et qu'il existe $a, b \in \mathbf{N}$ tels que $n = ab$ et $1 < a < b < n$. Montrer que $(n-1)! \equiv_n 0$.
3. On suppose $n > 4$ et qu'il existe $a \in \mathbf{N}$ tel que $n = a^2$. Montrer que $1 < a < 2a < n$ et en déduire que $(n-1)! \equiv_n 0$.

On suppose que n est premier et $n > 4$.
4. Soit $k \in \mathbf{N}$ tel que $2 \leq k \leq n-2$. Factoriser $k^2 - 1$ et en déduire que $k^2 \not\equiv_n 1$.
5. Soit $k \in \mathbf{N}$ tel que $2 \leq k \leq n-2$. Montrer qu'il existe un unique $l \in \mathbf{N}$ tel que $2 \leq l \leq n-2$, $l \neq k$ et $kl \equiv_n 1$.
6. Soit A défini par

$$\{k \in \mathbf{N} : 2 \leq k \leq n-2 \text{ et } \forall l \in \mathbf{N}(2 \leq l \leq k) \Rightarrow kl \not\equiv_n 1\}.$$

Montrer que A a exactement $(n-3)/2$ éléments et qu'il existe une bijection ψ de A dans son complémentaire dans $\{2,...,n-2\}$ telle que si $k \in A$ alors $k\psi(k) \equiv_n 1$.
7. En déduire que $(n-1)! \equiv_n 1 \times (n-1) \equiv_n -1$.

Exercice 32.
Wilson d'après Lagrange
On admet que si $\mathbf{K}$ est un corps, $P \in \mathbf{K}[X]$ un polynôme de degré $n > 0$ et $a \in \mathbf{K}$ une racine de P ($P(a) = 0$) alors il existe un unique polynôme $Q \in \mathbf{K}[X]$ de degré $n-1$ tel que $P = (X-a)Q$.
1. Soient $\mathbf{K}$ un corps, $P \in \mathbf{K}[X]$ un polynôme de degré $n > 0$ et $a_1,..,a_n \in \mathbf{K}$ deux à deux disjoints. On suppose que si $k = 1,...,n$ alors $P(a_k) = 0$. Montrer qu'il existe $\lambda \in \mathbf{K}^*$ tel que

$$P(X) = \lambda(x-a_1) \cdot ... \cdot (x-a_n).$$

Soit p un nombre premier et $P \in (\mathbf{Z}/p\mathbf{Z})[X]$ défini par $P(X) = X^{p-1} - 1$.
2. Vérifier à l'aide du petit théorème de Fermat que $P(a) = 0$ si $a \in \mathbf{Z}/p\mathbf{Z}^*$.
3. Montrer que $P(X) = (X-1) \cdot ... \cdot (X-(p-1))$.
4. En calculant $P(0)$ de deux façons montrer que $(p-1)! \equiv_p -1$.

Exercice 33.
cyclicité du groupe multiplicatif $\mathbf{Z}/p\mathbf{Z}^*$ si p premier
Soit p un nombre premier. Soit D l'ensemble des diviseurs de $p-1$. Si $d \in D$ on note O_d l'ensemble des éléments d'ordre d du groupe multiplicatif $\mathbf{Z}/p\mathbf{Z}^*$ et on note S_d le sous-ensemble de $\mathbf{Z}/p\mathbf{Z}$ des solutions de l'équation polynomiale $X^d - 1 = 0$.
1. Soit $d \in D$.
1.a. Vérifier que S_d est un sous-groupe de $\mathbf{Z}/p\mathbf{Z}^*$.
1.b. Montrer que S_d possède au plus d éléments.
1.c. Montrer que $O_d \subset S_d$.
1.d. Montrer que si O_d est non vide alors S_d est isomorphe au groupe additif $\mathbf{Z}/d\mathbf{Z}$.
1.e. En déduire que si O_d est non vide alors son cardinal est égal à $\phi(d)$, le nombre d'éléments d'ordre d de $\mathbf{Z}/d\mathbf{Z}$.
2. Vérifier que les $O_d, d \in D$ forment une partition de $\mathbf{Z}/p\mathbf{Z}^*$.
3. En déduire que

$$p-1 = \sum_{d \in D, O_d \neq \emptyset} \phi(d).$$

4. En utilisant l'égalité

$$p-1 = \sum_{d \in D} \phi(d)$$

démontrer que les O_d sont tous non vide.
5. En déduire que le groupe multiplicatif $\mathbf{Z}/p\mathbf{Z}^*$ est cyclique.

Exercice 34.
sous-groupes de $\mathbf{R}$.
Soit G un sous-groupe de $\mathbf{R}$ différent de $\{0\}$.
1. Vérifier que si $a \in \mathbf{R}$ alors $a\mathbf{Z} = \{x = ka : k \in \mathbf{Z}\}$ est un sous-groupe de $\mathbf{R}$.
On pose $a = \inf\{x \in G : x > 0\}$.

2. On suppose qu'il existe une suite x_n dans $\{x \in G : x > a\}$ qui tend vers a.
2.a. Soit $\varepsilon > 0$. Montrer qu'il existe $b, c \in G$ tels que $a < b < c < a + \varepsilon$ et en déduire qu'il existe $x \in G$ tel que $0 < x < \varepsilon$.
2.b. Soit $y \in \mathbf{R}$. Montrer qu'il existe $u, v \in G$ tels que $u < y < v$ et $v - u < \varepsilon$.
2.c. Montrer que G est dense.
3. On suppose qu'il n'existe pas de suite x_n dans $\{x \in G : x > a\}$ qui tende vers a.
3.a. Montrer que $a \in G$.
3.b. On suppose qu'il existe $b \in G \setminus a\mathbf{Z}$. Montrer qu'il existe alors $c \in G$ avec $0 < c < a$.
3.c. Montrer que $G = a\mathbf{Z}$.
4. Montrer que $\mathbf{Z} + \sqrt{2}\mathbf{Z}$ est dense.

Exercice 35.
fractions continues
Si $a \in \mathbf{R}$ on note $E(a)$ la partie entière de a.
Soit $a \in \mathbf{R}$. On considère les suites d, x et R définies par récurrence de la façon suivante :
- $d_0 = E(a)$, $b_0 = a - d_0$ et $R_0(x) = d_0 + x$. ;
- si $n \in \mathbf{N}$ et $b_n = 0$ alors $b_{n+1} = d_{n+1} = 0$ et $R_{n+1}(x) = R_n(x)$;
- si $n \in \mathbf{N}$ et si $b_n \neq 0$ alors $d_{n+1} = E(\dfrac{1}{b_n})$, $b_{n+1} = \dfrac{1}{b_n} - d_{n+1}$ et $R_{n+1}(x) = R_n(\dfrac{1}{d_{n+1} + x})$.

1. Calculer la suite d associée à $\sqrt{2}$ et celle associée au nombre d'or ($\Psi > 0$ et $\Psi^2 = \Psi + 1$).
2. Vérifier que si $n \geq 1$ alors R_n est la fraction

$$R_n(x) = d_0 + \cfrac{1}{d_1 + \cfrac{1}{\ddots \; d_{n-1} + \cfrac{1}{d_n + x}}}$$

3. Montrer que $R_n(b_n) = a$.
4. En déduire que s'il existe n tel que $b_n = 0$ alors a est rationnel.
5. Montrer que si la suite d est périodique alors le nombre a correspondant est une racine d'un polynôme de degré 2 à coefficients dans $\mathbf{Z}$.
6. On suppose que $a = \dfrac{p}{q}$ avec $p, q \in \mathbf{N}^*$ premiers entre eux.
6.a. Soit r la suite des restes obtenus en appliquant l'algorithme d'Euclide à (p, q). Montrer que $b_n = \dfrac{r_n}{r_{n-1}}$ si $r_{n-1} \neq 0$ et $b_n = 0$ sinon.
6.b. En déduire que $b_n = 0$ et $R_n(0) = \dfrac{p}{q}$ à partir d'un certain rang.
7. On consière les deux suites P et Q définies par récurrence par : $P_{-1} = 1$, $Q_{-1} = 0$, $P_0 = d_0$, $Q_0 = 1$ et si $n \in \mathbf{N}$

$$P_n d_{n+1} + P_{n-1} = P_{n+1} \text{ et } Q_n d_{n+1} + Q_{n-1} = Q_{n+1}.$$

Vérifier que

$$R_n(x) = \frac{P_n + P_{n-1}x}{Q_n + Q_{n-1}x} \text{ et } P_n Q_{n-1} - Q_n P_{n-1} = (-1)^{n+1} \text{ si } n \in \mathbf{N}.$$

8. Montrer que si $r, s, t, u \in \mathbf{R}^{+*}$ vérifient $\dfrac{r}{s} < \dfrac{t}{u}$ alors $\dfrac{r}{s} < \dfrac{r+t}{s+u} < \dfrac{t}{u}$.
9. En déduire que si $n \in \mathbf{N}$ on a

$$\frac{P_{2n}}{Q_{2n}} \leq \frac{P_{2n+2}}{Q_{2n+2}} \leq a \leq \frac{P_{2n+3}}{Q_{2n+3}} \leq \frac{P_{2n+1}}{Q_{2n+1}}.$$

10. Montrer que Q_n est croissante.
11. Soit $n \in \mathbf{N}^*$. On suppose $d_{n+2} \neq 0$. Montrer que $Q_{n+2} \geq 2Q_n$ et en déduire que $Q_{n+2} \geq 2\sqrt{2^n}$.
12. Montrer que $\left|\frac{P_n}{Q_n} - \frac{P_{n+1}}{Q_{n+1}}\right| = \frac{1}{Q_nQ_{n+1}} \leq \frac{1}{Q_n^2}$ si $n \in \mathbf{N}^*$.
13. Montrer que $\frac{P_n}{Q_n}$ tend vers a.
14. Soit $\frac{p}{q}$ tel que $\left|\frac{p}{q} - a\right| < \left|\frac{P_n}{Q_n} - a\right|$.
14.a. Montrer que $\left|\frac{P_n}{Q_n} - \frac{P_{n+1}}{Q_{n+1}}\right| \leq 2\left|\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}}\right|$ si $n \in \mathbf{N}^*$.
14.b. Montrer que $\frac{p}{q}$ est compris entre $\frac{P_n}{Q_n}$ et $\frac{P_{n+1}}{Q_{n+1}}$ ou entre $\frac{P_n}{Q_n}$ et $\frac{P_{n-1}}{Q_{n-1}}$ si $n \in \mathbf{N}^*$.
14.c. Montrer qu'il existe $A \in \mathbf{N}^*$ tel que

$$\left|\frac{P_{n+1}}{Q_{n+1}} - \frac{p}{q}\right| = \frac{A}{qQ_{n+1}} < \frac{1}{Q_nQ_{n+1}} \text{ ou } \left|\frac{P_{n-1}}{Q_{n-1}} - \frac{p}{q}\right| = \frac{A}{qQ_{n-1}} < \frac{1}{Q_{n-1}Q_n}.$$

14.d. Montrer que $q > Q_n$.

Exercice 36.
les points rationnels du cercle unité
On note $C = \{x^2 + y^2 = 1\}$ le cercle unité de $\mathbf{R}^2$. Soit $t \in \mathbf{R}$. On note $m(t) = (x(t), y(t))$ le point d'intersection de la droite D_t d'équation $t(y-1)+x = 0$ avec $C \setminus \{(0,1)\}$.
1. Montrer que

$$\begin{aligned} x(t) &= \frac{2t}{t^2+1} \\ y(t) &= \frac{t^2-1}{t^2+1}. \end{aligned}$$

2. Montrer que $m(t) \in \mathbf{Q}^2$ si et seulement si $t \in \mathbf{Q}$.
3. Résoudre dans $\mathbf{Z}^3$ l'équation $a^2 + b^2 = c^2$.

Exercice 37.
critères de divisibilité
Soit $n \in \mathbf{N}$ un entier et $a_k...a_0$ son écriture décimale :

$$n = \sum_{i=0}^{k} a_i 10^i \text{ avec } a_i \in \{0, ..., 9\}.$$

1. Montrer
1.a. L'entier n est divisible par 3 si et seulement si 3 divise $a_0 + ... + a_k$.
1.b. L'entier n est divisible par 9 si et seulement si 9 divise $a_0 + ... + a_k$.
1.c. L'entier n est divisible par 11 si et seulement si $a_0 + ... + (-1)^k a_k = 0$.
1.d. L'entier n est divisible par 5 si et seulement si 5 divise a_0.
1.e. L'entier n est divisible par 2 si et seulement si 2 divise a_0.
1.f. L'entier n est divisible par 4 si et seulement si 4 divise $a_0 + 2a_1$.
1.g. L'entier n est divisible par 6 si et seulement si 6 divise $a_0 + 4(a_1 + ... + a_k)$.
1.h. L'entier n est divisible par 8 si et seulement si 8 divise $a_0 + 2a_1 + 4a_2$.
2. Soit $d \in \mathbf{N}$ tel que $n = 10d + a_0$.
2.a. Montrer que $n = 10(d - 2a_0) + 21a_0$.
2.b. Montrer que $n \equiv_7 d - 2a_0$.
2.c. Donner un critère de divisibilité par 7.

Exercice 38.

nombres de Mersenne (2^d-1)
Soit $d \in \mathbf{N}$, $d \geq 2$.
1. Montrer que si $n \in \mathbf{N}$ est supérieur ou égal à 3 alors (n^d-1) n'est pas premier.
2. On suppose que $d = pq$ avec $p,q \in \mathbf{N}$ et $p,q \geq 2$. Montrer $(2^{pq}-1)$ est divisible par (2^p-1) et (2^q-1).
3. Montrer que si (2^d-1) est premier alors d est premier.
4. Rechercher le plus petit nombre premier tel que (2^p-1) ne soit pas premier.
5. Vérfier que $2^{23}-1 \equiv_{47} 0$.

Exercice 39.
nombres parfaits
Soit n un entier naturel. On note s_n la somme de ses diviseurs (y compris n) et σ_n la somme de ses diviseurs propres (différents de n).L'entier n est un nombre parfait s'il est égal à la somme de ses diviseurs autres que lui-même (i.e. $n = \sigma_n$ (ou $(s_n = 2n)$).
1. On suppose que $n = pq$ avec $pgcd(p,q) = 1$. Montrer que $s_n = s_p s_q$.
2. On suppose que $n = 2^{d-1}(2^d-1)$ avec (2^d-1) premier (et d entier).
2.a. Montrer que les diviseurs de 2^{d-1} sont les 2^k avec $k = 0,...,d-1$ et ceux de (2^d-1) sont 1 et (2^d-1).
2.b. Calculer $s_{2^{d-1}}$ et s_{2^d-1}.
2.c. Montrer que n est parfait et pair (Euclide).
3. On suppose que n est parfait et pair : $n = 2^d q$ avec $d,q \in \mathbf{N}$ et $d \geq 1$, q impair.
3.a. Montrer que $2^{d+1}q = (2^{d+1}-1)s_q$.
3.b. Montrer qu'il existe $m \in \mathbf{N}^*$ tel que $s_q = 2^{d+1}m$.
3.c. Vérifier que $q = (2^{d+1}-1)m$.
On suppose $m > 1$.
3.d. Montrer que $q = (2^{d+1}-1)m$, $(2^{d+1}-1)$, m, et 1 sont des diviseurs de q.
3.e. Montrer que $s_q \geq 2^{d+1}m$.
3.f. Montrer que $m = 1$ (i.e. l'hypothèse $m > 1$ conduit à une contradiction).
3.g. Vérifier que $q = (2^{d+1}-1)$ et que $s_q = 2^{d+1}$.
3.h. Montrer que q est premier (Euler).

Exercice 40.
nombres de Fermat $(2^{2^m}+1)$
1. Montrer que si $a,n \in \mathbf{N}$ alors $(a+1)$ divise $(a^{2n+1}+1)$.
2. Montrer que si $m,n \in \mathbf{N}$ avec n impair alors $(2^{2^m}+1)$ divise $(2^{n2^m}+1)$.
3. Montrer que si (2^d+1) est premier alors il existe $m \in \mathbf{N}$ tel que $d = 2^m$.
4. Vérifier que 641 divise $(2^{32}+1)$ et que $32 = 2^5$.

Exercice 41.
nombres de Carmichaël
Un entier naturel n est un nombre de Carmichaël si pour tout entier a premier avec n, $a^{n-1} \equiv_n 1$.
1. Les nombres premiers sont-ils des nombres de Carmichaël ?
2. Soit n un entier naturel pair différent de 2.
2.a. Vérifier que $n-1$ est premier avec n mais que $(n-1)^{n-1} \not\equiv_n 1$.
2.b. L'entier n est-il un nombre de Carmichaël ?
3. Soit $n = p_1 \cdot ... \cdot p_k$ où les p_i sont des nombres premiers impairs tous distincts. On suppose que chaque terme (p_i-1) divise $n-1$.
3.a. Soit a un entier premier avec n et soit $i = 1,...,k$. Vérifier que p_i divise $a^{p_i-1}-1$ et en déduire que p_i divise $a^{n-1}-1$.
3.b. Démontrer que n divise $a^{n-1}-1$.
3.c. Montrer que a est un nombre de Carmichaël.
3.d. Vérifier que 561 et 1105 sont des nombres de Carmichaël.

4. Soit $n = mp^2$ avec p premier et m entier naturel impair. On suppose que n est un nombre de Carmichaël. On pose $a = 1 + mp$.
4.a. Calculer a^p et montrer que $a^p \equiv_n 1$.
4.b. Montrer que $G = \{a^k : k \in \mathbf{N}\}$ muni de la loi $\times_n$ forme un groupe cyclique d'ordre p.
4.c. Calculer $a(1-mp)$, montrer que a est premier avec n et en déduire que $a^{n-1} \equiv_n 1$.
4.d. En déduire que p divise $n-1$.
4.e. Conclure que n n'est pas un nombre de Carmichaël.
5. Soit $n = p_1 \cdot \ldots \cdot p_k$ où les p_i sont des nombres premiers impairs tous distincts. On suppose que n est un nombre de Carmichaël.
5.a. Dire pourquoi il existe $g_1 \in \mathbf{Z}/p_1\mathbf{Z}, .., g_k \in \mathbf{Z}/p_k\mathbf{Z}$ tels que chaque g_i est d'ordre $p_i - 1$ dans le groupe multiplicatif $\mathbf{Z}/p_i\mathbf{Z}^*$.
5.b. Dire pourquoi il existe $g \in \mathbf{Z}/_{\mathbf{Z}}n$ tel que $g \equiv_{p_i} g_i$ si $i = 1, ..., k$.
5.c. Montrer que g est premier avec n et en déduire que $g^{n-1} \equiv_n 1$.
5.d. Montrer que $g^{n-1} \equiv_{p_i} 1$ et en déduire que $g_i^{n-1} \equiv_{p_i} 1$ si $i = 1, ..., k$.
5.e. Montrer que $p_i - 1$ divise $n-1$.
6. Montrer qu'un entier naturel non premier n est un nombre de Carmichaël si et seulement s'il est de la forme $n = p_1 \cdot \ldots \cdot p_k$ où les p_i sont des nombres premiers impairs tous distincts et chaque terme $(p_i - 1)$ divise $n-1$.

Exercice 42.
irrationalité de $\exp 1$
Soient $u = (u_n)$ et $v = (v_n)$ les deux suites définies par

$$\begin{aligned} u_n &= \sum_{k=0}^{n} \frac{1}{k!}, \\ v_n &= u_n + \frac{1}{n \cdot n!}. \end{aligned}$$

1. Montrer que u et v sont adjacentes.
2. Montrer que u et v ont une limite commune notée $\exp(1)$ et que si $n \in \mathbf{N}$ alors $u_n < \exp(1) < v_n$.
3. Soit $n \in \mathbf{N}$. Montrer qu'il existe $d_n \in \mathbf{N}$ tel que

$$n!u_n = d_n < d_n + \frac{1}{n} = n!v_n.$$

4. Soit $n, p, q \in \mathbf{N}$ tels qu $u_n < \frac{p}{q} < v_n$. Montrer que q ne divise pas $n!$ et en déduire que $q > n$.
5. Montrer que $\exp(1)$ est irrationnel.

Exercice 43.
répartition des nombres premiers
On considère la suite p des nombres premiers successifs : $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ et si $n \in \mathbf{N}$ on note $\pi(n)$ le nombre de nombres premiers compris entre 0 et n. On a $\pi(0) = \pi(1) = 0$ et, si $n \in \mathbf{N}$ est supérieur ou égal à 2, on a $p_{\pi(n)} \leq n < p_{\pi(n)+1}$.
1. On considère la suite u définie par $u_0 = 0$ et par

$$u_n = \sum_{k=1}^{n} \frac{1}{k} \text{ si } n \in \mathbf{N}^*.$$

1.a. Montrer que u est strictement croissante.
1.b. Montrer si $d \in \mathbf{N}$ et si $k \in \mathbf{N}$ est compris entre $2^d + 1$ et 2^{d+1} alors $\frac{1}{k} > \frac{1}{2^d}$ et en déduire que $u_{2^{d+1}} - u_{2^d} > \frac{1}{2}$.
1.c. Montrer que si $d \in \mathbf{N}$ alors $u_{2^d} > \frac{d}{2}$.
1.d. Montrer que $\lim_{+\infty} u = +\infty$.

2. Soit $m \in \mathbf{N}^*$.
2.a. Vérifier que si $k \in \mathbf{N}$ est compris entre 1 et m alors il existe un unique m-uplet $(i_1(k),...,i_m(k)) \in \mathbf{N}^n$ tel que

$$k = \prod_{j=1}^{m} {p_j}^{i_j(k)} \text{ et } 0 \leq i_1(k),...,i_m(k) \leq m$$

et en déduire

$$\sum_{0 \leq i_1,...,i_k \leq m} \prod_{j=1}^{m} \left(\frac{1}{p_j}\right)^{i_j} \geq \sum_{k=1}^{m} \prod_{j=1}^{m} \left(\frac{1}{p_j}\right)^{i_j(k)} = \sum_{k=1}^{m} \frac{1}{k}.$$

2.b. Montrer la double inégalité

$$1 + \frac{2}{p_j} > \frac{1}{1-\frac{1}{p_j}} > \sum_{i=0}^{m} \left(\frac{1}{p_j}\right)^{i} \text{ pour } j \in \mathbf{N} \text{ compris entre 1 et } m$$

et en déduire

$$\prod_{j=1}^{m} \left(1 + \frac{2}{p_j}\right) > \prod_{j=1}^{m} \left(\frac{1}{1-\frac{1}{p_j}}\right) > \prod_{j=1}^{m} \left(\sum_{i=0}^{m} \left(\frac{1}{p_j}\right)^{i}\right) = \sum_{0 \leq i_1,...,i_k \leq m} \prod_{j=1}^{m} \left(\frac{1}{p_j}\right)^{i_j}.$$

2.c. Etablir $\lim_{m \to +\infty} \prod_{j=1}^{m} \left(\frac{1}{1-\frac{1}{p_j}}\right) = +\infty$ et $\lim_{m \to +\infty} \prod_{j=1}^{m} \left(1 + \frac{2}{p_j}\right) = +\infty$.
2.d. Montrer que si $x \geq 0$ alors $x \geq \ln(1+x)$ et en déduire que si $m \in \mathbf{N}^*$ alors

$$\sum_{j=1}^{m} \frac{1}{p_j} \geq \frac{1}{2} \ln \left(\prod_{j=1}^{m} \left(1 + \frac{2}{p_j}\right) \right)$$

puis que $\lim_{m \to +\infty} \sum_{j=1}^{m} \frac{1}{p_j} = +\infty$.
2.e. Montrer que si $\alpha > 1$ alors l'ensemble $I(\alpha) = \{i \in \mathbf{N} : p_i < i^{\alpha}\}$ est infini.
Soit $\varepsilon > 0$.
3. Montrer qu'il existe $M \in \mathbf{N}$ tel que pour tout $m \in \mathbf{N}$ supérieur ou égal à M on a

$$\prod_{j=1}^{m} \left(1 - \frac{1}{p_j}\right) < \varepsilon.$$

4. Soit $l \in \mathbf{N}^*$. On pose $N_l = l \cdot p_1 \cdot ... \cdot p_M$. Soit $n \in \mathbf{N}$ compris entre N_l et N_{l+1}.
4.a. Vérifier que

$$\frac{\pi(n)}{n} \leq \frac{\pi(N_{l+1})}{N_l}.$$

4.b. Vérifier que $\pi(N_{l+1}) \leq \phi(N_{l+1})$ où ϕ désigne l'indicatrice d'Euler.
4.c. Montrer que

$$\pi(N_{l+1}) \leq N_{l+1} \prod_{j=1}^{M} \cdot \left(1 - \frac{1}{p_j}\right) \leq N_{l+1} \varepsilon.$$

4.d. Montrer que

$$\frac{\pi(n)}{n} \leq 2\varepsilon.$$

5. Montrer que

$$\lim_{n \to +\infty} \frac{\pi(n)}{n} = 0.$$

Exercice 44.
trois clés classiques
1. Le numéro de sécurité sociale est la concaténation d'un numéro I à 13 chiffres caractérisant le porteur du numéro [genre (1 ou 2), année de naissance (2 chiffres), mois de naissance (2 chiffres), démpattement de naissance (2 chiffres), commune de naissance (3 chiffres), rang de naissance dans l'année et la commune (3 chiffres)] et d'une clé C à 2 chiffres et définie par $C-1 \equiv_{97} 97-I$.
1.a. Montrer qu'on détecte un numéro de sécurité sociale erroné si l'erreur porte sur un chiffre.
1.b. Montrer qu'on détecte un numéro de sécurité sociale erroné si l'erreur est la permutation de deux chiffres.
1.c. Montrer qu'on détecte un numéro de sécurité sociale erroné si l'erreur est la permutation de l'année et du mois ou du mois et du département.
2. Le code ISBN est un nombre de 13 chiffres $C = c_1....c_{12}c_{13}$. Les 12 premiers chiffres identifient un ouvrage et le 13e est une clé de contrôle calculée de la façon suivante

$$c_{13} \equiv_{10} 10-(c_1+3c_2+c_3+3c_4+c_5+3c_6+c_7+3c_8+c_9+3c_{10}+c_{11}+3c_{12}).$$

2.a. Montrer qu'on détecte un code ISBN erroné si l'erreur porte sur un chiffre.
2.b. Montrer qu'on détecte un code ISBN erroné si l'erreur est la permutation de deux chiffres successifs sauf si la différence de ces deux chiffres est ± 5.
3. Le numéro de carte bancaire est formé de 16 chiffres : $B = b_1...b_{15}b_{16}$. Le dernier est la clé qui est calculée à partir des autres de la façon suivante : $b_{16} \equiv_{10} 10-(b'_1+...+b'_{15})$ où $b'_{2k-1} = b_{2k-1}$ et $b'_{2k} \equiv_9 2b_{2k}$ si $k = 1,...,7$.
3.a. Montrer qu'on détecte un numéro de carte bancaire erroné si l'erreur porte sur un chiffre.
3.b. Détecte-t-on un numéro de carte bancaire erroné si l'erreur est la permutation de deux chiffres successifs ?

Exercice 45.
trois chiffrements classiques
1. Un chiffrement affine revient à remplacer les lettres par d'autres lettres à l'aide d'une application affine inversible dans $\mathbf{Z}/26\mathbf{Z}$.
1.a. Montrer que $n \in \mathbf{Z}/26\mathbf{Z} \mapsto an+b$ est inversible si et seulement si $pgcd(a,26) = 1$.
1.b. Combien existe-t-il de chiffrements affines ?
2. Un chiffrement de Hill est un chiffrement affine par bloc. Il consiste à remplacer des mots de n lettres (n est une constante du chiffrement par d'autres mots de même longueur à l'aide d'une matrice (n,n) agissant sur $(\mathbf{Z}/26\mathbf{Z})^n$ de façon bijective.
2.a. Montrer que $A \in M_n(\mathbf{Z}/26\mathbf{Z})$ est inversible si et seulement si $pgcd(\mathrm{Det}(A),26) = 1$.
2.b. Combien existe-il de chiffrements de Hill par bloc $(2,2)$ pour l'alphabet de 26 lettres ?
3. Un chiffrement de Vigenère combine une table et une clé. La table correspond à une application θ de $\mathbf{Z}/26\mathbf{Z} \times \mathbf{Z}/26\mathbf{Z}$ dans $\mathbf{Z}/26\mathbf{Z}$ telle que pour tout $a \in \mathbf{Z}/26\mathbf{Z}$ les applications partielles $x \mapsto \theta(a,x)$ et $x \mapsto \theta(x,a)$ sont des bijections. La clé est un mot de longueur n : $b_1...b_n$ avec les b_i dans $\mathbf{Z}/26\mathbf{Z}$. On code un texte de longueur m de la façon suivante. Si $k = 1,...,m$ on remplace la lettre $a_k \in \mathbf{Z}/26\mathbf{Z}$ du texte original par la lettre $\theta(a_k,b_{l_k})$ où $l_k \equiv_n k$ et $1 \leq k \leq n$.
3.a. Comment construire une table de déchiffrement à partir d'une table de chiffrement ?
3.b. Combien existe-t-il de tables de chiffrement ?
3.c. Une table de chiffrement étant donnée, combien de chiffrements différents peut on obtenir avec des clés de 7 caractères ?

Exercice 46.
écriture des entiers et des réels en base a
Soit $a \in \mathbf{N}$ tel que $a \geq 2$.
1. Montrer que si $k \in \mathbf{N}$ alors $a^k \geq 1+k$ et que $a^{k+1} > a^k$.
2. Soit $n \in \mathbf{N}$. Montrer qu'il existe un unique $d \in \mathbf{N}$ tel $a^d \leq n < a^{d+1}$.

3. Montrer par récurrence sur d que si $n \in \mathbf{N}$ vérifie $0 \leq n < 2^{d+1}$ alors il existe un unique $u = (u_0, ..., u_d) \in [0, ..., a-1]^{d+1}$ tel que

$$n = \sum_{k=0}^{d} u_k a^k.$$

Soit $x \in]0,1[$ un réel.
4. Pour tout $k \in \mathbf{N}$ on note y_k la partie entière de $a^k x$ et on note v_k le reste de la division de y_k par a.
4.a. Montrer que si $E(a^n x) = \sum_{k=0}^{n} u_k a^k$ alors pour tout $k = 0, ..., n$ alors $v_k = u_{n-k}$.
4.b. Montrer que les suites $x_n = \sum_{k=0}^{n} v_k \frac{1}{a^k}$ et $y_n = x_n + \frac{1}{a^n}$ sont des suites adjacentes de limite x ($\sum_{k=0}^{+\infty} v_k \frac{1}{a^k}$ est l'écriture de x en base a).
4.c. Montrer que si $a^n x \in \mathbf{N}$ alors pour tout $k > n$ $v_k = 0$ et montrer que si de plus $v_n \neq 0$ alors x est aussi la limite de la suite $x'_n = \sum_{k=0}^{n} v'_k \frac{1}{a^k}$ avec $v'_k = v_k$ si $k < n$, $v'_n = v_n - 1$ et $v'_k = a-1$ si $k > n$.
4.d. Soient $v, v' \in [0, ..., a-1]^{\mathbf{N}}$ non constantes égales à $a-1$ à partir d'un certain rang. Montrer que si $v \neq v'$ alors $x = \sum_{k=0}^{+\infty} v_k \frac{1}{a^k}$ et $x' = \sum_{k=0}^{+\infty} v'_k \frac{1}{a^k}$ sont différents.
4.e. Caractériser l'écriture en base a des rationnels.

Exercice 47.
Soit $a \in \mathbf{N}$ tel que $a \geq 2$. Donner un algorithme pour obtenir l'écriture d'un entier naturel en base a.

Exercice 48.
calcul d'une puissance
Soit $n \in \mathbf{N}^*$. A $x \in \mathbf{Z}/n\mathbf{Z}$ et $d \in \mathbf{N}^*$ on associe les suites $a_k(x)$, $b_k(x,d)$, $d_k(d)$, $r_k(d)$ $D_k(d)$ définies de la façon suivante :
- $a_0(x) = x$, $b_0(x,d) = 1$, $d_0(d) = d$, $D_0(d) = 0$;
- si $k \in \mathbf{N}$ alors
  - $d_{k+1}(d)$ et $r_k(d)$ sont le quotient et le reste de la division euclidienne de $d_k(d)$ par 2 ;
  - $a_{k+1}(x) = a_k(x)^2$;
  - $b_{k+1}(x,d) = b_k(x,d) \times a_k(x,d)^{r_k(d)}$;
  - $D_{k+1}(d) = D_k(d) + r_k(d)2^k$.

1. Montrer que si $d_k(d) > 1$ alors $d_k(d) > d_{k+1}(d) \geq 1$.
2. En déduire qu'il existe k_d tel que $d_k(d) > 1$ si $k < k_d$ et $d_{k_d}(d) = 1$.
3. Montrer que $k_d < \frac{\ln(d)}{\ln(2)} + 1$.
4. Montrer que
  - $d_{k+1}(2d+r) = d_k(d)$ et $r_{k+1}(2d+r) = r_k(d)$ si $r = 0$ ou 1 ;
  - $a_{k+1}(x) = a_k(x^2)$.

En déduire que $x^r b_k(x^2, d) = b_{k+1}(x, 2d+r)$ si $r = 0$ ou 1.
5. Montrer par récurrence sur d que si $x \in \mathbf{Z}/n\mathbf{Z}$ alors $b_{k_d+1} = x^d$.

Exercice 49.
jeux de Nim
1. On dispose d'un tas de 100 cailloux. Deux joueurs s'affrontent en prenant à chaque coup entre 1 à 8 cailloux. Le gagnant est celui qui prend le dernier caillou. Existe-t-il une stratégie gagnante pour le joueur qui débute ?
2. On dispose maintenant de plusieurs tas contenant chacun un nombre arbitraire de cailloux. Deux joueurs s'affrontent en prenant à chaque coup le nombre de cailloux qu'il souhaite (mais au moins un) dans le tas qu'il souhaite.

Soit $n \in \mathbf{N}$. Soit $d_n \in \mathbf{N}$ et $u_0^n, ..., u_{d_n}^n \in \{0,1\}$ tels que $n = \sum_{k=0}^{d_n} u_k^n 2^k$. On note $P_n \in (\mathbf{Z}/2\mathbf{Z})[x]$ le polynôme $P_n(x) = \sum_{k=0}^{d_n} \overline{u_k^n}^2 x^k$.

2.a. Montrer que si les entiers naturels $n_1, ..., n_d$ sont tels que $0 < n_1 \leq ... \leq n_d$ et $P_{n_1} + ...P_{n_d} \neq 0$ alors il existe $m_1, ..., m_d \in \mathbf{N}$ tels que $m_k = n_k$ si $k \neq d$ et $m_d < n_d$ tels que $P_{m_1} + ...P_{m_d} = 0$.

2.b. Montrer que si les entiers naturels non nuls $n_1, ..., n_d$ sont tels que $P_{n_1} + ...P_{n_d} = 0$ alors si $m_1, ..., m_d \in \mathbf{N}$ sont tels que $m_k = n_k$ sauf pour d et $m_d < n_d$ alors $P_{m_1} + ... + P_{m_d} \neq 0$.

2.c. Soient $n_1, ..., n_d$ les nombres de cailloux dans les tas au début du jeu. Donner une condition nécessaire et suffisante pour que le joueur qui débute dispose d'une stratégie gagnante et expliquer cette stratégie.

Exercice 50.

applications linéaires préservant $\mathbf{Z}^d$

Soit $d \in \mathbf{N}$ et $A \in M_d(\mathbf{R})$.

1. On suppose que A préserve $\mathbf{Z}^d$. Montrer que $A \in M_d(\mathbf{Z})$.

2. On suppose que la restriction de A à $\mathbf{Z}^d$ est une bijection. Montrer que $\mathrm{Det}(A) = 1$.

3. Soit $n \in \mathbf{N}$.

3.a. Vérifiez que si $x \in \mathbf{Z}^d$ alors $\overline{A}^n(\overline{x}^n) = \overline{A(x)}^n$.

3.b. Vérifier que $\overline{A}^n \in M_d(\mathbf{Z}/n\mathbf{Z})$ est inversible si et seulement si $\mathrm{Det}(A)$ est premier avec n.

Exercice 51.

le chiffrement RSA de Rivest, Shamir et Adleman

Soient p et q deux nombres premiers différents. On pose $n = pq$. Soient aussi c et d deux entiers naturels strictement inférieurs à $\phi(n)$ (où ϕ désigne l'indicatrice d'Euler) et inverses l'un de l'autre dans $\mathbf{Z}/\phi(n)\mathbf{Z}$.

1. Montrer qu'il existe $k \in \mathbf{Z}$ tel que $cd = 1 + k(p-1)(q-1)$.

2. Soit $a \in \mathbf{N}$ et $a < n$. Vérifier les égalités

$$(a^c)^d \equiv_p a^{cd} \equiv_p a^{1+k(p-1)(q-1)} \equiv_p a \cdot \left(a^{(p-1)}\right)^{k(q-1)}$$
$$(a^c)^d \equiv_q a^{cd} \equiv_q a^{1+k(p-1)(q-1)} \equiv_q a \cdot \left(a^{(q-1)}\right)^{k(p-1)}$$

3. En distinguant les cas a premier avec p et q, a premier seulement avec p et a premier seulement avec q montrer à l'aide du théorème de Fermat les égalités $(a^c)^d \equiv_p a$ et $(a^c)^d \equiv_q a$.

4. En déduire que $(a^c)^d \equiv_n a$.

Une société de crédit identifie à distance le possesseur d'une carte de crédit par la transmission du code confidentiel. Pour que cette transmission soit sécurisée il est nécessaire de crypter le code a. Le chiffrement RSA consiste à transmettre non pas a mais $A \equiv a^c$ modulo n. La société qui reçoit A calcule A^d modulo n. Elle retrouve ainsi le code a. Dans cette méthode les nombres n et c sont publics. Ils sont accessibles à tous les clients. Les nombres p, q et d ne sont connus que de la société. Pour les calculer il est nécessaire de factoriser n. Ceci est à réaliser si n est très grand. Ceci garantit la fiabilité du chiffrement RSA.

Exercice 52.

le chiffrement de El Gamal

Une personne A doit envoyer un message m (m entier naturel) de façon chiffrée à B, une seconde personne. Cette dernière choisit p premier plus grand que tout message susceptible de lui être envoyé et un élément $g \in \mathbf{Z}/p\mathbf{Z}^*$. Elle choisit aussi $s \in \mathbf{N}$ qu'il garde secret. Elle calcule $b = g^s$ et communique à A le triplet (p, g, b). En retour A choisit $t \in \mathbf{N}$, calcule $a = g^t$ et $c = mb^t$ et renvoie (a, c) à B.

1. Montrer qu'il existe $h \in \mathbf{Z}/p\mathbf{Z}$ tel que $gh = 1$.

2. Que fait B pour retrouver m ?

La sécurité du chiffrement de El Gamal qui vient d'être décrit réside dans la difficulté de calcul du *logarithme discret* (i.e. trouver s connaissant le triplet (p,g,b)).

Exercice 53.
Échange de clés de Diffie-Hellman
Une personne A envoie un message X chiffré en Y à B. Les algorithmes ψ de chiffrement et déchiffrement ψ^{-1} sont publics et dépendent d'une clé $K \in \mathbf{Z}/p\mathbf{Z}^*$ (avec p premier) : $Y = \psi(K,X)$ et $X = \psi^{-1}(K,Y)$. La construction de la clé et la transmission du message chiffré se font de la façon suivante. B choisit $g \in \mathbf{Z}/p\mathbf{Z}^*$ et $b \in \mathbf{N}$. Il calcule $\beta = g^b$ et communique à A le couple (g,β). A choisit alors $a \in \mathbf{N}$, calcule $K = \beta^a$ et $\alpha = g^a$ et il communique à A ce nombre α en même temps que le message chiffré $Y = \psi(K,X)$.
1. Vérifier que K n'est pas nul.
2. Comment B fait-il pour trouver la clé K et déchiffrer le message ?
3. Supposons qu'une tierce personne C intercepte les échanges entre A et B et modifie les informations. Après avoir avoir reçu (g,β) de B il transmet (g,γ) à A avec $\gamma = g^c$, c étant choisi par ses soins.
3.a. Peut-il déchiffer le message chiffré envoyé par A ?
3.b. Que doit-il envoyer à B pour que B puisse retrouver X en déchifrant le message chiffré reçu ?

Exercice 54.
Cryptosystème de Merkle-Hellman
Soit $n \in \mathbf{N}^*$ et soit $a = (a_1,...,a_n) \in \mathbf{N}^{*n}$. On pose $||a|| = \sum_{i=1}^{n} a_i$. Si $\sum_{i=1}^{k-1} a_i < a_k$ pour tout $k = 2,...,n$ on dit que a est super-croissant.
1. Montrer que $(1,2,...,2^{n-1})$ est super-croissant et que $2^{k-1} \leq a_k$ pour tout $k = 1,...,n$ si $(a_1,...,a_n)$ est super-croissant.
Soit $f : \{0,1\}^n \to \mathbf{N}$ définie par $f(x) = \sum_{i=1}^{n} x_i a_{n+1-i}$ si $x = (x_1,...,x_n) \in \{0,1\}^n$.
2. Montrer que si $x \in \{0,1\}^n$ alors $f(0,...,0) = 0 \leq f(x) \leq ||a|| = f(1,...,1)$.
On suppose a super-croissant.
3. Montrer que f est strictement croissante de $\{0,1\}^n$ muni de l'ordre lexicographique dans $\mathbf{N}$.
4. Soit $y \in \mathbf{N}$. On considère $z = (z_1,...,z_n) \in \{0,1\}^n$ défini par $z_1 = 1$ si $y \geq ||a||$ ou $z_1 = 0$ sinon, et, pour $k \in \{1,...,n-1\}$ $z_{k+1} = 1$ si $y \geq ||a|| - \sum_{i=1}^{k} z_i a_{n+1-i}$ ou $z_{k+1} = 0$ sinon. Montrer que s'il existe $x \in \{0,1\}^n$ tel que $y = f(x)$ alors $x = z$.
On fixe $N \in \mathbf{N}$ tel que $||a|| < N$ et $K \in \mathbf{N}$ tel que $K < N$ et $pgcd(K,N) = 1$.
5. Montrer qu'il existe $L \in \mathbf{N}$ tel que $KL \equiv_N 1$ et $L < N$.
6. Si $k = 1,...,n$ on note b_k l'unique entier naturel strictement inférieur à N tel que $b_k \equiv_N K a_k$. Montrer que les b_k sont tous différents et qu'il existe une unique permutation σ de $\{1,...,n\}$ telle que $c = (c_1,...,c_n)$ définie par $c_k = b_{\sigma(k)}$ si $k = 1,...,n$ vérifie $c_1 < ... < c_n$.
7. Soit $g : \{0,1\}^n \to \mathbf{N}$ définie par $g(x) = \sum_{i=1}^{n} x_i c_{n+1-i}$ si $x = (x_1,...,x_n) \in \{0,1\}^n$. Montrer que si $x \in \{0,1\}^n$ alors $f(x) \equiv_N L g((x_{\sigma(1)},...,x_{\sigma(n)}))$.
L'envoi par un individu B à un individu A d'un mot binaire chiffré à l'aide du cryptosystème de Merkle-Hellman se fait de la façon suivante. A choisit une clé secrète formée d'un $n-$uplet super-croissant a et des entiers N et K comme dans l'exercice. Il calcule $c = (c_1,...,c_n)$ et transmet à B ce n-uplet. B chiffre le mot x en calculant $g(x)$ qu'il transmet à A. Ce dernier déchiffre (i.e. retrouve x à partir de $g(x)$) en utilisant les questions 4, 5, 6 et 7.