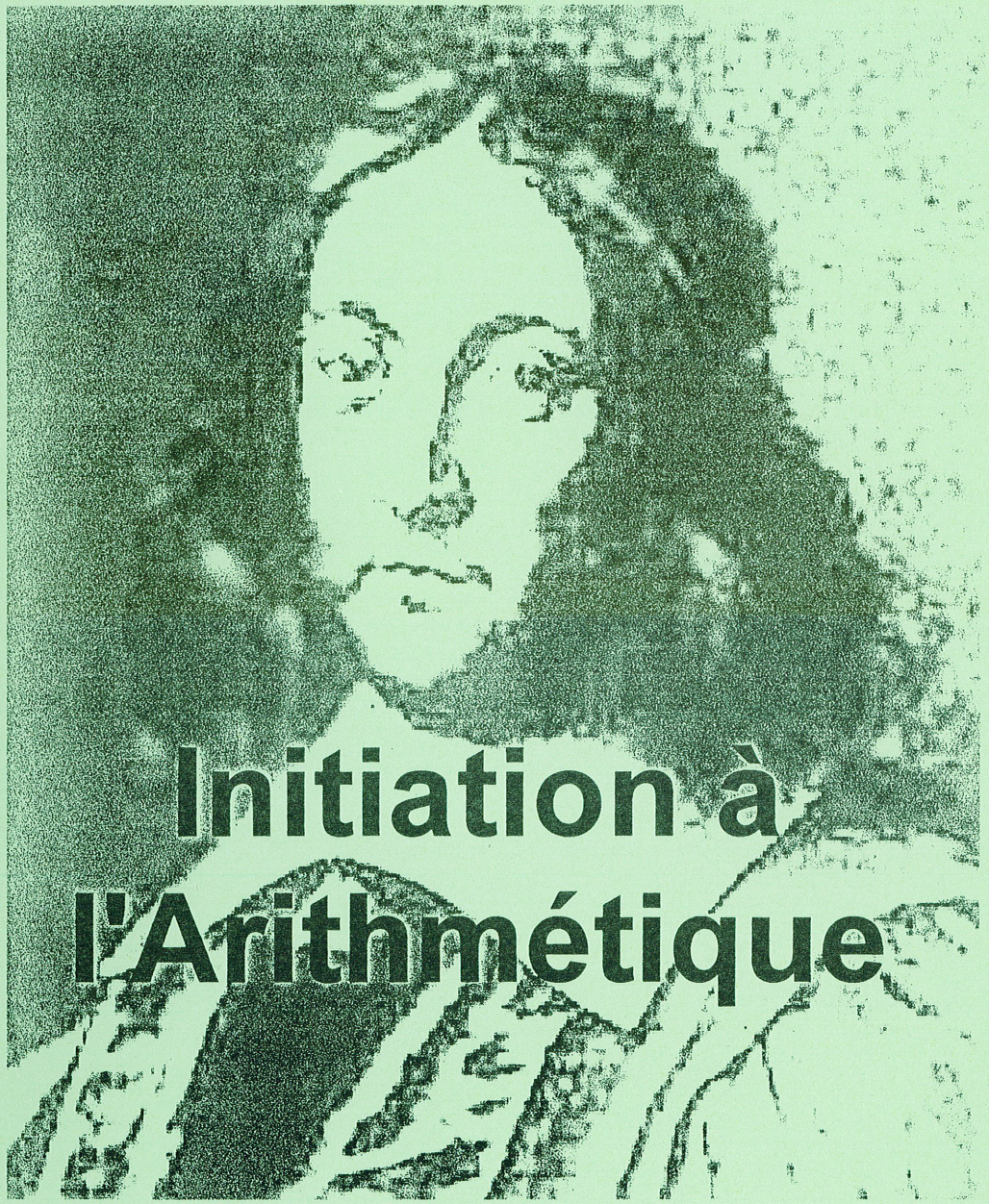
Université Bordeaux I

Institut de Recherche
pour l'Enseignement des Mathématiques

40 rue Lamartine 33400 TALENCE

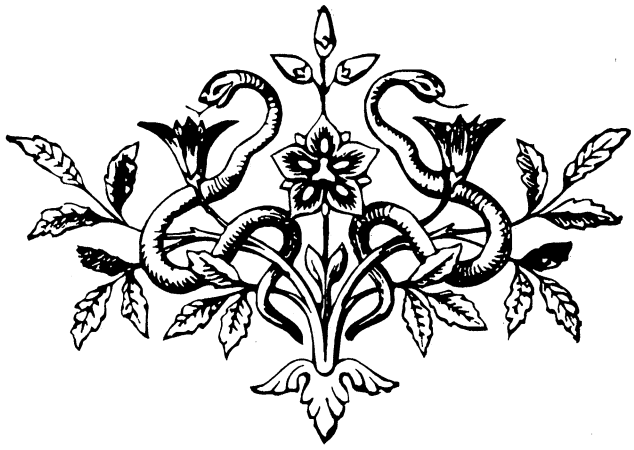


Initiation à l'Arithmétique

Groupe Arithmétique et Géométrie

BORDEAUX 1999

IREM d'Aquitaine



Initiation à l'Arithmétique

Ont participé à l'élaboration de ce fascicule:

BOUSCASSE Jean-Marie Collège Théophile de Viau 47 LE PASSAGE
CHAUMET Marie-Claude Lycée Camille Julian 33 BORDEAUX
DAMEY Pierre Université Bordeaux I 33 TALENCE
GOUTEYRON Antoine Lycée René Cassin 64 BAYONNE
GOUTEYRON Claire Lycée René Cassin 64 BAYONNE
POMES Roland Lycée René Cassin 64 BAYONNE
PINET Bernard Lycée Jean-Baptiste de Baudre 47 AGEN
PUYOU Jacques Lycée Bernard Palissy 47 AGEN
ROBERT Yves Lycée René Cassin 64 BAYONNE

BORDEAUX 1999

INTRODUCTION

Ce document est consacré à l'étude de l'arithmétique élémentaire. C'est le " retour " de cette partie des mathématiques dans l'enseignement dispensé au lycée qui nous a incités à entreprendre sa rédaction.

Il est destiné aux professeurs de mathématiques, auxquels nous proposons des démarches, des progressions, des outils de réflexion, des méthodes de démonstration, des activités et des exercices pouvant nourrir leurs pratiques de classe.

Il est destiné aussi aux préparataires aux CAPES internes et externes de mathématiques, auxquels nous souhaitons apporter un recul indispensable sur les notions et méthodes de l'arithmétique élémentaire.

Il est destiné enfin aux élèves des classes terminales qui voudraient approfondir leurs connaissances et anticiper ainsi la compréhension et l'illustration des notions plus générales d'arithmétique qui seront l'un des objets de leurs études à venir.

Son contenu est divisé en quatre parties :

- la partie A est consacrée à l'arithmétique dans $\mathbb{N}$. Après quelques rappels sur une présentation axiomatique(*) de $\mathbb{N}$ et l'introduction des notions de multiple et de diviseur d'un entier naturel, elle propose deux développements possibles :
  - ➢ démarche 1 : on démontre l'unicité de la décomposition d'un nombre en produit de facteurs premiers, puis on en déduit le théorème de Gauss et on introduit la division euclidienne;
  - ➢ démarche 2 : on introduit la division euclidienne, puis on en déduit le théorème de Gauss, puis on en établit l'unicité de la décomposition d'un nombre en produit de facteurs premiers ;
- la partie B est consacrée à l'arithmétique dans $\mathbb{Z}$ et on y développe, en particulier, la notion de congruence modulo n ;

  Les outils utilisés dans les parties A et B sont ceux des classes terminales de lycée.
- la partie C propose des exemples de mise en œuvre et de prolongement des notions exposées précédemment, que ceux-ci fassent partie des programmes de l'enseignement de spécialité en Terminales Scientifiques (étude de l'équation $ax+by=c$, exemples de codages ...) ou bien en dépassent quelque peu le cadre (étude de l'ensemble $\mathbb{Z}/n\mathbb{Z}$) ;
- la partie D, présente quelques algorithmes illustrant les chapitres précédents.

Un recueil d'exercices, pour la plupart " originaux ", destinés à compléter les applications usuelles de l'arithmétique que l'on est assuré de trouver dans les divers manuels scolaires viendra prolonger cet ouvrage.

(*) Le lecteur peut, dans une première lecture, omettre cette introduction axiomatique sans obérer la compréhension de la suite.

SOMMAIRE

III- NOMBRES PREMIERS

1- Définition
2- Proposition
3- Proposition
4- Proposition (" Unicité " de la décomposition en produit de facteurs premiers)

IV- DIVISION EUCLIDIENNE

1- Théorème et définition (Division euclidienne)
2-Les sous-groupes additifs de $\mathbb{Z}$

V- CONGRUENCES

1- Définition
2- Propriété
3- Exemples

VI- DIVISEURS ET MULTIPLES COMMUNS A DEUX ENTIERS RELATIFS

1- Plus grand commun diviseur
2- Théorème de Bézout
3- Entiers relatifs premiers entre eux
4- Théorème de Gauss
5- Une conséquence du théorème de Bézout :
6- Plus petit commun multiple
7- Autre présentation du plus petit commun multiple
8- Relation entre *PPCM* et *PGCD*

Partie C - COMPLÉMENTS

I- ETUDE DE L'ENSEMBLE $\mathbb{Z}/n\mathbb{Z}$

1- L'ensemble $\mathbb{Z}/n\mathbb{Z}$
2- Addition et multiplication dans $\mathbb{Z}/n\mathbb{Z}$
3- Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

II- ETUDE DE L'EQUATION $ax+by=c$

III- PLUS GRAND COMMUN DIVISEUR ET PLUS PETIT COMMUN MULTIPLE DE PLUSIEURS ENTIERS

1- Plus grand commun diviseur de plusieurs entiers
2- Plus petit commun multiple de plusieurs entiers
3- Lois de composition interne définies à partir du *PGCD* et du *PPCM*

IV- PETIT THÉORÈME DE FERMAT – THÉORÈME DE WILSON

V- ÉTUDE DE QUELQUES FONCTIONS ARITHMÉTIQUES

1- Nombre de diviseurs d'un entier naturel *n* non nul
2- Somme des diviseurs d'un entier naturel *n* non nul
3- Indicateur d'Euler

VI- PROBLÈMES DE CODAGE

1- Exemple historique : " Le codage de César "
2- Liminaire aux codages actuels
3- Un principe de codage
4- Le codage RSA (Rivest, Shamir, Adleman)

Partie D - ALGORITHMES

Codage RSA à l'aide de la TI 92 PLUS
Algorithmes d'Euclide et de Bézout

Partie E - EXERCICES

Partie A - ARITHMÉTIQUE DANS $\mathbb{N}$

I- AXIOMATIQUE DE $\mathbb{N}$ (Axiomes de Péano)

1- Axiomes de Péano[1]

Il existe un triplet $(\mathbb{N},0,s)$, *où* $\mathbb{N}$ *est un ensemble,* 0 *un élément de* $\mathbb{N}$ *et* s *une application de* $\mathbb{N}$ *dans* $\mathbb{N}$ *vérifiant :*

A1 *s est injective* ;

A2 *l'image de* $\mathbb{N}$ *par* s *est* $\mathbb{N}-\{0\}$;

A3 *toute partie* A *de* $\mathbb{N}$ *telle que* $0 \in A$ et $s(A) \subset A$ *est égale à* $\mathbb{N}$. **(Principe de récurrence)**

Vocabulaire et notations :

- $\mathbb{N}$ est appelé ensemble des entiers naturels ;
- 0 est appelé zéro ;
- s est appelée application successeur ;
- $s(0)$ est noté 1 et appelé un ;
- $\mathbb{N}-\{0\}$ est noté $\mathbb{N}^*$.

Utilisation pratique du principe de récurrence

Pour établir qu'une propriété $\mathcal{P}(n)$ est vraie pour tout entier naturel n :

1) On justifie que $\mathcal{P}(0)$ est vraie ;

2) On montre que pour un entier naturel k, $(\mathcal{P}(k) \Rightarrow \mathcal{P}(s(k)))$ est vraie.

2- Addition dans $\mathbb{N}$

Théorème Définition *Il existe une et une seule application*

$$\begin{aligned}\mathbb{N}\times\mathbb{N} &\to \mathbb{N}\\ (p,q) &\mapsto p+q\end{aligned}$$

vérifiant :

i) pour tout élément p *de* $\mathbb{N}$, $p+0=p$;

ii) pour tout couple (p,q) *d'éléments de* $\mathbb{N}$, $p+s(q)=s(p+q)$.

Cette application s'appelle addition.

L'entier naturel $p+q$ *se lit « p plus q ». Il est appelé somme de p et de q.*

Conséquence immédiate *Pour tout entier naturel* n, $s(n)=n+1$.

On établit par récurrence les propriétés suivantes, où p, q et r désignent des entiers naturels :

- **Associativité** $(p+q)+r=p+(q+r)$; *cet entier sera noté* $p+q+r$;
- **Commutativité** $p+q=q+p$;
- **Régularité** $p+r=q+r \Rightarrow p=q$;
- **Elément neutre** $p+0=0+p=p$;
- **Autre propriété** $p+q=0 \Leftrightarrow (p=0 \text{ et } q=0)$.

---

[1] Vous noterez l'outrecuidance des auteurs qui se permettent de numéroter les axiomes alors que les entiers naturels ne sont pas encore définis...

3- Multiplication dans $\mathbb{N}$

Théorème Définition *Il existe une et une seule application*

$$\mathbb{N}\times\mathbb{N}\to\mathbb{N}$$
$$(p,q)\mapsto p\times q$$

vérifiant :

i) pour tout élément n de $\mathbb{N}$, $n\times 0=0$;

ii) pour tout couple (p,q) *d'éléments de* $\mathbb{N}$, $p\times s(q)=(p\times q)+p$.

Cette application s'appelle multiplication.

L'entier naturel $p\times q$ *(également noté pq) se lit « p multiplié par q » ou « p fois q ». Il est appelé produit de p et de q.*

Comme pour l'addition, on établit par récurrence les propriétés suivantes, où p, q et r désignent des entiers naturels :

- **Associativité** $(p\times q)\times r=p\times(q\times r)$; *cet entier sera noté* $p\times q\times r$ *ou* pqr ;
- **Commutativité** $p\times q=q\times p$;
- **Elément neutre** $p\times 1=1\times p=p$;
- **Régularité** *r étant non nul :* $p\times r=q\times r\Rightarrow p=q$;
- **Distributivité de la multiplication par rapport à l'addition** $p(q+r)=(pq)+(pr)$ *et* $(q+r)p=(qp)+(rp)$; *ces entiers seront respectivement notés* $pq+pr$ *et* $qp+rp$.
- **Autres propriétés**
  - $pq=1\Leftrightarrow(p=1 \text{ et } q=1)$.
  - $pq=0\Leftrightarrow(p=0 \text{ ou } q=0)$.

Définition (puissance n-ième) *Soit des entiers naturels a et n, n non nul, l'entier naturel* $\underbrace{a\times\ldots\times a}_{n}$ *est appelé puissance n-ième de a. Il est noté* a^n.

L'entier naturel a^n *se lit « a exposant n » ou « a puissance n ».*

Remarque $a^1=a$.

Propriétes *Soit des entiers naturels a, b et des entiers naturels m et n, m et n non nuls,*

- $a^m\times a^n=a^{m+n}$;
- $a^n\times b^n=(a\times b)^n$;
- $(a^m)^n=a^{m\times n}$.

Convention *Si a est un entier naturel non nul, on pose* $a^0=1$.

Remarque Soit des entiers naturels a et b non nuls, les propriétés précédentes sont encore vraies lorsque $n=0$ ou $m=0$.

4- Ordre naturel dans $\mathbb{N}$

a) Définition *Soit des entiers naturels a et b, on écrit* $a \leq b$ *pour signifier qu'il existe un entier naturel d tel que* $b = a + d$.

La relation "$a \leq b$*" se lit « a est inférieur ou égal à b ».*

Remarque Lorsqu'un tel entier naturel *d* existe il est unique.

Vocabulaire et notation :

- la relation $a \leq b$, s'écrit aussi $b \geq a$ et se lit alors « b est supérieur ou égal à a » ;
- l'entier naturel d est noté $b - a$. Il est appelé différence de b et a ;
- lorsque ($a \leq b$ et $a \neq b$) on écrit $a < b$. Cette relation " $a < b$ " se lit « a est strictement inférieur à b » ;
- la relation $a < b$, s'écrit aussi $b > a$, qui se lit « b est strictement supérieur à a ».

b) Théorème *La relation* $\leq$ *ainsi définie sur* $\mathbb{N}$ *est une relation d'ordre total.*

Cela signifie que, étant donné des entiers naturels a, b et c, cette relation vérifie les propriétés suivantes :

Réflexivité $a \leq a$;

Antisymétrie $(a \leq b \text{ et } b \leq a) \Rightarrow a = b$;

Transitivité $(a \leq b \text{ et } b \leq c) \Rightarrow a \leq c$.

Cette relation est alors une relation d'ordre. Cet ordre est de plus total car pour tous entiers naturels a et b, $a \leq b$ ou $b \leq a$.

Propriété (Compatibilité de cette relation avec l'addition dans $\mathbb{N}$) *Soit des entiers naturels p, q et r,*

$$p \leq q \Rightarrow p + r \leq q + r$$

Remarque *On a en réalité* $p \leq q \Leftrightarrow p + r \leq q + r$.

Corollaire *Soit des entiers naturels p, q, p' et q',*

$$(p \leq q \text{ et } p' \leq q') \Rightarrow p + p' \leq q + q'.$$

Propriété (Compatibilité de cette relation avec la multiplication dans $\mathbb{N}$) *Soit des entiers naturels p, q et r.*

$$p \leq q \Rightarrow pr \leq qr.$$

Remarque *De plus si* $r \neq 0$ *on a* $p \leq q \Leftrightarrow pr \leq qr$.

Corollaire *Soit des entiers naturels p, q, p' et q',*

$$(p \leq q \text{ et } p' \leq q') \Rightarrow pp' \leq qq'.$$

c) Définitions

- *On dit qu'une partie non vide A de* $\mathbb{N}$ *est majorée pour signifier qu'il existe un entier naturel n tel que tout élément de A soit inférieur ou égal à n. Un tel entier naturel n est appelé majorant de A.*
- *On dit qu'une partie non vide A de* $\mathbb{N}$ *est minorée pour signifier qu'il existe un entier naturel n tel que tout élément de A soit supérieur ou égal à n. Un tel entier naturel n est appelé minorant de A.*
- *On dit qu'une partie non vide de* $\mathbb{N}$ *est finie pour signifier qu'elle est majorée, sinon elle est dite infinie.*

d) Propriétés de $\mathbb{N}$ liées à l'ordre

- *Toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*
- *L'ensemble* $\mathbb{N}$ *ne possède pas de plus grand élément.*

- *L'entier naturel* 0 *est le plus petit élément de* $\mathbb{N}$.
- *Toute partie majorée non vide de* $\mathbb{N}$ *admet un plus grand élément.*

5- Exemple d'utilisation pratique du principe de récurrence

Soit $\mathcal{P}(n)$ la proposition : $0+1+2+\ldots+n=\dfrac{n(n+1)}{2}$.

- $\mathcal{P}(0)$ est vraie car $0=\dfrac{0\times(0+1)}{2}$.
- $\mathcal{P}(k)\Rightarrow\mathcal{P}(k+1)$

  On cherche à démontrer que : $0+1+\ldots+k=\dfrac{k(k+1)}{2}\Rightarrow 0+1+\ldots+(k+1)=\dfrac{(k+1)(k+2)}{2}$

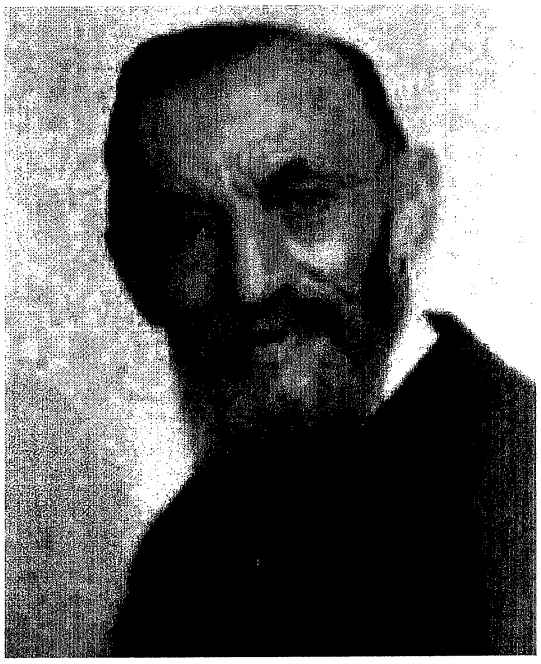
$$0+1+\ldots+k=\frac{k(k+1)}{2}\Rightarrow(0+1+\ldots+k)+(k+1)=\frac{k(k+1)}{2}+(k+1)$$

$$\Rightarrow 0+1+\ldots+(k+1)=\frac{k(k+1)+2(k+1)}{2}$$

$$\Rightarrow 0+1+\ldots+(k+1)=\frac{(k+1)(k+2)}{2}$$

  Donc $(\mathcal{P}(k)\Rightarrow\mathcal{P}(k+1))$ est vraie.

- **Conclusion :** pour tout entier naturel n, $\mathcal{P}(n)$ est vraie.



Peano (Giuseppe) (Cuneo, 1858 - Turin, 1932), mathématicien et logicien italien.

II. ARITHMETICA.

§1 +

N_0 vale « numero », et es nomen commune de 0,1,2, etc.
0 » « zero ».
+ » « plus ». Si a es numero, $a+$ indica « numero sequente a ».

Questione, si nos pote definir N_0, significa si nos pote scribe sequalitate de forma

$N_0 =$ expressione composito per signos nota « 0 » « + » « = » ... », quod non es facile.

Ergo nos sume tres idea N_0, 0, + ut idea primitivo, per que nos defini omni symbolo de Arithmetica.

Nos determina valore de symbolo non definito N_0, 0, + per systema de propositio primitivo sequente.

✱ 1. Pp

- 1 $N_0 \in \mathrm{Cls}$
- 2 $0 \in N_0$
- 3 $a \in N_0 . \supset . a+ \in N_0$
- 4 $s \in \mathrm{Cls} . 0 \in s : a \in s . \supset_a . a+ \in s :\supset. N_0 \supset s$ Induct
- 5 $a,b \in N_0 . a+ = b+ . \supset . a = b$
- 6 $a \in N_0 . \supset . a+ \neq 0$

Lege :

- 0 N_0 es classe, vel « numero » es nomen commune.
- 1 Zero es numero.
- 2 Si a es numero, tunc suo successivo es numero.
- 3 N_0 es classe minimo, que satisfac ad conditione 0, 1, 2;

Extrait de " *Rivista di matematica* " (1895) montrant un original des axiomes de Peano.

II- Multiple et diviseur d'un entier naturel

1- Définition (Multiple et diviseur) *Soit des entiers naturels a et b, on dit que b est un diviseur de a pour signifier qu'il existe un entier naturel q tel que* $a = bq$. *Dans ce cas on dit également que b divise a et que a est un multiple de b.*

a) Vocabulaire et notations

- b divise a est noté $b|a$;
- l'ensemble des diviseurs de a est noté $\boldsymbol{Div}(a)$;
- l'ensemble des multiples de b est noté $b\mathbb{N}$;
- lorsque $a = bq$ avec b non nul, q est noté $\frac{a}{b}$.

b) Exemples

- $\boldsymbol{Div}(0) = \mathbb{N}$;
- $\boldsymbol{Div}(1) = \{1\}$;
- $\boldsymbol{Div}(12) = \{1;2;3;4;6;12\}$;
- $0\mathbb{N} = \{0\}$;
- $1\mathbb{N} = \mathbb{N}$;
- $2\mathbb{N} = \{0;2;4;6;\ldots;2n;\ldots\}$, on dit que $2\mathbb{N}$ est l'ensemble des entiers naturels pairs.

c) Propriétés immédiates *Soit un entier naturel n,*

- $1 \in \boldsymbol{Div}(n)$ et $n \in \boldsymbol{Div}(n)$;
- $0 \in n\mathbb{N}$ et $n \in n\mathbb{N}$.

2- Étude de la relation " divise " dans $\mathbb{N}$

a) Théorème (Lien entre la relation " divise " et la relation " est inférieur ou égal à ") *Soit des entiers naturels a et b, a non nul,*

$b|a \Rightarrow b \leq a$.

Démonstration

Lorsque $b|a$ et $a \neq 0$, il existe un entier naturel q non nul, puisque a est non nul, tel que $a = bq$.

Comme $q \geq 1$, $b \leq bq$, donc $b \leq a$.

b) Théorème *La relation " divise " est une relation d'ordre non total dans* $\mathbb{N}$.

Démonstration

Soit des entiers naturels a, b et c,

- Réflexivité $a = a \times 1$, donc $a|a$.
- Antisymétrie

  $a|b \Rightarrow$ il existe un entier naturel q tel que $b = aq$.

  $b|a \Rightarrow$ il existe un entier naturel q' tel que $a = bq'$.

  En multipliant membre à membre les deux égalités précédentes on obtient $ab = (ab)(qq')$.

  Deux cas sont alors à envisager :

  1er cas : $ab = 0$

  Alors $a = 0$ ou $b = 0$. Supposons, ce qui ne nuit en rien à la généralité de la démonstration, $a = 0$, comme $b = aq$, on a : $b = 0$ et par conséquent $a = b$.

  2ème cas : $ab \neq 0$

  Alors $qq' = 1$, donc $q = 1$ et $q' = 1$, et par conséquent $a = b$.

- Transitivité

  $a|b \Rightarrow$ il existe un entier naturel q tel que $b = aq$.

  $b|c \Rightarrow$ il existe un entier naturel q' tel que $c = bq'$.

  Avec les deux égalités précédentes on obtient $c = a(qq')$, donc $a|c$.

Cette relation d'ordre n'est pas une relation d'ordre total car, par exemple, 3 ne divise pas 2 et 2 ne divise pas 3.

c) La relation " divise " et les opérations dans $\mathbb{N}$

Proposition *Soit des entiers naturels a, b, c, d et n, n non nul,*

i) $(a|b \text{ et } a|c) \Rightarrow a|(b+c)$;

ii) $(c \leq b, a|b \text{ et } a|c) \Rightarrow a|(b-c)$;

iii) $a|b \Rightarrow a|bc$;

iv) $a|b \Rightarrow ac|bc$;

v) $(a|b \text{ et } c|d) \Rightarrow ac|bd$;

vi) $a|b \Rightarrow a^n|b^n$.

Démonstration

i) $a|b$ et $a|c \Rightarrow$ il existe des entiers naturels q et q' tels que $b = aq$ et $c = aq'$.

On additionne membre à membre ces deux dernières égalités, on obtient $b+c = a(q+q')$, donc $a|(b+c)$.

ii) $a|b$ et $a|c \Rightarrow$ il existe des entiers naturels q et q' tels que $b = aq$ et $c = aq'$;

1er cas : $a = 0$, c'est vrai.

2ème cas : $a \neq 0$, on a $c \leq b$, donc $aq' \leq aq$, donc $q' \leq q$.

Après calcul, on obtient $b-c = a(q-q')$, donc $a|(b-c)$.

iii) $a|b$, or $b|bc$, la relation " divise " étant transitive $a|bc$.

iv) $a|b \Rightarrow$ il existe un entier naturel q tel que $b = aq$.

On multiplie chaque membre de la dernière égalité par c et on obtient : $bc = (ac)q$, donc $ac|bc$.

v) $a|b \Rightarrow ac|bc$, d'après la propriété précédente;

$c|d \Rightarrow bc|bd$, toujours d'après la propriété précédente.

La relation " divise " étant transitive $ac|bd$.

vi) Par récurrence on obtient, pour tout entier naturel n, $a|b \Rightarrow a^n|b^n$.

3- Ensemble des multiples d'un entier naturel non nul

Proposition (N est archimédien) *Soit un entier naturel a et un entier naturel b non nul, il existe un entier naturel q tel que* $bq > a$.

Démonstration

On a : $b \geq 1$ et $a+1 > a$, après calcul, on obtient $b(a+1) > a$.

Corollaire *L'ensemble des multiples d'un entier naturel non nul est infini.*

Proposition *Soit des entiers naturels a et b non nuls,*

$a|b \Leftrightarrow b\mathbb{N} \subset a\mathbb{N}$.

Démonstration

- $a|b \Rightarrow b\mathbb{N} \subset a\mathbb{N}$

Il s'agit de démontrer que tout élément de $b\mathbb{N}$ est un élément de $a\mathbb{N}$.

Soit $c \in b\mathbb{N}$, on a $b \mid c$, or $a \mid b$, donc $a \mid c$, donc $c \in a\mathbb{N}$, donc $b\mathbb{N} \subset a\mathbb{N}$.

- $b\mathbb{N} \subset a\mathbb{N} \Rightarrow a \mid b$

  On a $b \in b\mathbb{N}$, donc $b \in a\mathbb{N}$, donc $a \mid b$

4- Ensemble des diviseurs d'un entier naturel non nul

Proposition *Soit des entiers naturels a et b non nuls,*

$a \mid b \Leftrightarrow \boldsymbol{Div}(a) \subset \boldsymbol{Div}(b)$.

Démonstration

- $a \mid b \Rightarrow \boldsymbol{Div}(a) \subset \boldsymbol{Div}(b)$

  Soit $c \in \boldsymbol{Div}(a)$, on a $c \mid a$ et $a \mid b$, donc $c \mid b$, donc $c \in \boldsymbol{Div}(b)$, par conséquent $\boldsymbol{Div}(a) \subset \boldsymbol{Div}(b)$.

- $\boldsymbol{Div}(a) \subset \boldsymbol{Div}(b) \Rightarrow a \mid b$

  $a \in \boldsymbol{Div}(a)$, donc $a \in \boldsymbol{Div}(b)$, donc $a \mid b$.

Proposition *L'ensemble des diviseurs d'un entier naturel a non nul est fini.*

Démonstration

C'est une partie non vide de $\mathbb{N}$ majorée par a.

Leonardo Pisano Fibonacci (Pise 1170 - Pise 1250) mathématicien italien.

Publie en 1202 " *Liber abaci* ". A fait ses études en Afrique du Nord où son père était diplomate.

III- Nombres premiers

1- Définition *Un nombre est premier lorsqu'il admet exactement deux diviseurs,* 1 *et lui-même.*

Exemples

$\boldsymbol{Div}(0) = \mathbb{N}$, donc 0 n'est pas premier.

$\boldsymbol{Div}(1) = \{1\}$, donc 1 n'est pas premier.

$\boldsymbol{Div}(2) = \{1;2\}$, donc 2 est premier.

$\boldsymbol{Div}(3) = \{1;3\}$, donc 3 est premier.

$\boldsymbol{Div}(4) = \{1;2;4\}$, donc 4 n'est pas premier.

2- Proposition *Tout entier naturel n non premier et strictement supérieur à* 1 *possède au moins un diviseur premier dont le carré est inférieur ou égal à n.*

Démonstration

On a $n \in \boldsymbol{Div}(n)$ et $n \neq 1$, donc $\boldsymbol{Div}(n) \neq \{1\}$. Il en résulte que $\boldsymbol{Div}(n) - \{1\}$ est non vide, il possède donc un plus petit élément p tel que $p < n$ puisque n n'est pas premier.

Supposons que p ne soit pas premier, il existe alors un élément q de $\mathbb{N}$ qui divise strictement p, donc tel que $q | n$ et $1 < q < p < n$; il en résulte que q appartient à $\boldsymbol{Div}(n) - \{1\}$ et $q < p$, ce qui est en contradiction avec p plus petit élément de $\boldsymbol{Div}(n) - \{1\}$.

Par conséquent p est premier.

De plus, on peut écrire $n = p \times m$. On a m qui appartient à $\boldsymbol{Div}(n) - \{1\}$ puisque n n'est pas premier et donc $p \leq m$. Il en résulte que $p^2 \leq n$.

3- Proposition *L'ensemble des nombres premiers est infini.*

Démonstration

Soit un entier naturel n supérieur ou égal à 1. Considérons l'entier naturel[2] $a = n! + 1$.

D'après la proposition précédente, a possède un diviseur premier p.

Supposons $p \leq n$, on a alors $p | a$ et $p | n!$, donc $p | 1$, ce qui est en contradiction avec p premier. Il en résulte que $p > n$.

Pour tout entier naturel n non nul, il existe donc un nombre premier p supérieur à n. L'ensemble des nombres premiers n'est donc pas majoré, il est infini.

4- Existence d'une décomposition en produit de facteurs premiers

Proposition *Tout entier naturel strictement supérieur à* 1 *admet une décomposition en produit de facteurs premiers.*

Notation Soit des entiers naturels p et q tels que $p \leq q$, on note $[\![p, q]\!]$ l'ensemble des entiers naturels n tels que $p \leq n \leq q$.

Démonstration

Soit l'ensemble $\mathcal{D}$ des entiers naturels strictement supérieurs à 1 admettant une décomposition en produit de facteurs premiers.

- $\mathcal{D}$ contient tous les nombres premiers.
- $\mathcal{D}$ est stable par multiplication, c'est-à-dire que si a appartient à $\mathcal{D}$ et si b appartient à $\mathcal{D}$ alors $a \times b$ appartient à $\mathcal{D}$. En effet :

---

[2] $n! = 1 \times 2 \times \ldots \times (n-1) \times n$, par convention $0! = 1$ et $n!$ est lu « factorielle n ».

$a \in \mathcal{D} \Leftrightarrow a = p_1 \times \ldots \times p_r$ avec p_i premier pour tout $i \in [\![1, r]\!]$.
$b \in \mathcal{D} \Leftrightarrow b = q_1 \times \ldots \times q_s$ avec q_j premier pour tout $j \in [\![1, s]\!]$.
On a alors $a \times b = p_1 \times \ldots \times p_r \times q_1 \times \ldots \times q_s$ et $a \times b$ appartient à $\mathcal{D}$.

- Supposons que $\mathcal{D}$ soit différent de $\mathbb{N} - \{0;1\}$.
  On appelle $\mathcal{D}'$ l'ensemble $\mathbb{N} - (\mathcal{D} \cup \{0;1\})$. L'ensemble $\mathcal{D}'$ est, d'après notre hypothèse, différent de l'ensemble vide et, par conséquent, $\mathcal{D}'$ possède un plus petit élément d' strictement supérieur à 1.
  Comme d' n'appartient pas à $\mathcal{D}$, d' n'est pas premier. On peut écrire d' sous la forme $d' = a \times b$ avec $1 < a \leq b < d'$ (a et b sont des diviseurs stricts de d').
  Comme $a < d'$, on a $a \notin \mathcal{D}'$, or $a \notin \{0;1\}$, donc $a \in \mathcal{D}$; de même $b \in \mathcal{D}$. Il en résulte que $a \times b \in \mathcal{D}$, ce qui est en contradiction avec $d' \in \mathcal{D}'$.
  Par conséquent, $\mathcal{D} = \mathbb{N} - \{0;1\}$ et tout entier naturel strictement supérieur à 1 admet une décomposition en produit de facteurs premiers.

Autre démonstration

Si n est premier c'est fini.
Sinon n possède au moins un diviseur premier p_1. Ainsi il existe n_1 tel que $n_1 < n$ et $n = p_1 n_1$.

Si n_1 est premier c'est fini.

Sinon n_1 possède au moins un diviseur premier p_2. Ainsi il existe n_2 tel que ...

On fabrique ainsi une suite d'entiers naturels strictement décroissante $n_1, n_2, \ldots$ qui est par conséquent finie. Il existe donc un entier naturel k tel que n_k soit premier, avec $n = p_1 p_2 \ldots p_k n_k$, où chaque facteur est premier.

5- Proposition *Soit un entier naturel n strictement supérieur à* 1 *et p un diviseur premier de n, il existe une décomposition de n en produit de facteurs premiers dans laquelle figure le nombre p.*

Démonstration

On peut écrire $n = p \times q$.

1er cas : $q = 1$

Alors $n = p$, donc n est premier et la proposition est vraie.

2ème cas : $q > 1$

Alors q peut être décomposé en produit de facteurs premiers d'après la proposition précédente. Ainsi q peut s'écrire $q = p_1 \times p_2 \times \ldots \times p_r$ avec p_i premier pour tout $i \in [\![1, r]\!]$ et $n = p \times p_1 \times p_2 \times \ldots \times p_r$ ce qui constitue une décomposition de n en produit de facteurs premiers dans laquelle figure le nombre p.

A ce stade, deux démarches sont possibles:

Démarche 1

On démontre l'unicité de la décomposition en produit de facteurs premiers, puis on en déduit le théorème de Gauss (*Soit des entiers naturels b et c supérieurs ou égaux à* 1. *Si a est un entier naturel qui divise bc et qui est premier avec b alors a divise c.*) puis on introduit la division euclidienne.

Démarche 2

On introduit la division euclidienne, puis on démontre le théorème de Gauss, puis on en déduit l'unicité de la décomposition en produit de facteurs premiers.

Remarque

Dans le libellé des programmes l'unicité de la décomposition en produit de facteurs premiers figure avant le théorème de Gauss. Les commentaires des programmes précisent que l'unicité de la décomposition en produit de facteurs premiers est admise.

Gauss (Carl Friedrich) (Brunswick, 1777 - Göttingen, 1855), mathématicien, physicien et astronome allemand.

IV A- DÉMARCHE 1

1- Unicité de la décomposition d'un entier naturel en produit de facteurs premiers

Théorème *La décomposition en produit de facteurs premiers de tout entier naturel n strictement supérieur à 1 sous la forme* $n = p_1 \times \ldots \times p_s$, *est unique, avec, pour tout* $i \in [\![1, s]\!]$, p_i *premier, et, lorsque* $s > 1$, *pour tout* $i \in [\![1, s-1]\!]$, $p_i \leq p_{i+1}$

Démonstration[3]

Soit l'ensemble A des entiers naturels strictement supérieurs à 1 qui admettent plusieurs décompositions en produits de facteurs premiers.

Si $A \neq \varnothing$, il admet un plus petit élément, car tout sous-ensemble non vide de $\mathbb{N}$ admet un plus petit élément.

Soit n cet élément, n est non premier.

Un même nombre premier p ne peut pas figurer dans deux décompositions de n, sinon $\frac{n}{p} \in A$ et $\frac{n}{p} < n$.

Posons $n = p_1 \times \ldots \times p_s$ et $n = q_1 \times \ldots \times q_r$ avec pour tout $i \in [\![1, s]\!]$, pour tout $j \in [\![1, r]\!]$, p_i et q_j premiers et distincts.

On suppose de plus que $p_1 \leq \ldots \leq p_s$ et $q_1 \leq \ldots \leq q_r$.

Comme n n'est pas premier, $r > 1$ et $s > 1$, donc $p_1^2 \leq n$ et $q_1^2 \leq n$. Puisque $p_1 \neq q_1$ on a $p_1 < q_1$ ou $q_1 < p_1$, donc $p_1 q_1 < n$.

On pose $a = n - p_1 \times q_1$.

On a $1 < a < n$.

$1 < a$ car $p_1 | a$ et $a \neq 0$, donc $p_1 \leq a$.

Ainsi a admet une décomposition unique en produit de facteurs premiers.

On sait que $p_1 | a$ et par analogie $q_1 | a$.

Les nombres premiers p_1 et q_1 figurent donc dans l'unique décomposition de a.

Par conséquent $a = (p_1 \times q_1) \times b$, ainsi $n = (p_1 \times q_1) \times (1 + b)$.

Donc $\frac{n}{p_1} = p_2 \times \ldots \times p_s$ est divisible par q_1 ; mais $\frac{n}{p_1} \notin A$ car $\frac{n}{p_1} < n$, donc il existe $i \in [\![2, s]\!]$ tel que $p_i = q_1$.

Ceci est en contradiction avec le fait que pour tout $i \in [\![1, s]\!]$ et pour tout $j \in [\![1, r]\!]$ $p_i \neq q_j$ et l'hypothèse de départ $A \neq \varnothing$ est absurde, ce qui achève la démonstration.

Remarque

D'un point de vue pratique on écrit la décomposition d'un nombre n en produit de facteurs premiers sous la forme $n = p_1^{\alpha_1} \times \ldots \times p_s^{\alpha_s}$, avec pour tout $i \in [\![1, s]\!]$, p_i premier et α_i entier naturel non nul, les p_i étant deux à deux distincts.

Dans tout ce chapitre, on écrira décomposition pour décomposition en produit de facteurs premiers d'un entier.

Corollaire *Soit des entiers naturels a et b strictement supérieurs à 1, si a divise b alors tout nombre premier figurant dans la décomposition de a figure dans celle de b avec un exposant supérieur ou égal à celui qu'il a dans la décomposition de a.*

Démonstration

Comme $b = a \times q$, la décomposition de b s'obtient donc en multipliant la décomposition de a par celle de q.

Dans la décomposition ainsi obtenue, tout nombre premier figurant dans la décomposition de b figure avec un exposant supérieur ou égal à celui qu'il a dans la décomposition de a. Or la décomposition de b est unique...

---

[3] L'idée de cette démonstration provient du livre THE THEORY OF NUMBERS de Hardy and Wright

2- Plus grand commun diviseur

Théorème - Définition *Soit des entiers naturels a et b non nuls, l'ensemble des diviseurs communs à a et b est non vide. Il est majoré par a (et par b) donc il admet un plus grand élément d qui est appelé plus grand commun diviseur de a et b et noté* $PGCD(a\,,b)$.

Soit un entier naturel a non nul, l'ensemble des diviseurs communs à a et 0 *est l'ensemble des diviseurs de a. Il admet un plus grand élément a qui est appelé plus grand commun diviseur de a et* 0 *et noté* $PGCD(a\,,0)$, *ainsi* $PGCD(a\,,0)=a$.

Convention $PGCD(0,0)=0$.

Remarque $PGCD(a\,,b)=PGCD(b\,,a)$.

Proposition (Calcul pratique du *PGCD*) *Soit des entiers naturels a et b non nuls.*
Si $a=1$ *ou* $b=1$ *alors* $PGCD(a,b)=1$.

Sinon, on considère tous les nombres premiers figurant dans les décompositions de a et b, on a $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ *et* $b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r}$ *où pour tout i élément de* $[\![1\,,r]\!]$, p_i *est un nombre premier,* α_i *et* β_i *sont des entiers naturels éventuellement nuls ; on a alors* $PGCD(a,b)=p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_r^{\gamma_r}$ *avec* $\gamma_i=\min(\alpha_i\,,\beta_i)$.

Démonstration
Soit $d=PGCD(a,b)$. On peut écrire $d=p_1^{s_1}p_2^{s_2}\cdots p_r^{s_r}$ avec, pour tout *i* élément de $[\![1\,,r]\!]$, s_i entier naturel, $s_i\le\alpha_i$ et $s_i\le\beta_i$.
Il en résulte $s_i\le\gamma_i$, pour tout *i* élément de $[\![1\,,r]\!]$ et donc $s_i=\gamma_i$ puisque $p_1^{s_1}p_2^{s_2}\cdots p_r^{s_r}$ précédemment défini est un diviseur de *a* et de *b*.

Proposition *Soit des entiers naturels a et b,*

i) tout diviseur commun à a et b est un diviseur de $PGCD(a\,,b)$;

ii) tout diviseur de $PGCD(a\,,b)$ *est un diviseur commun à a et b.*

Autrement dit, on a $\boldsymbol{Div}(a)\cap\boldsymbol{Div}(b)=\boldsymbol{Div}(PGCD(a\,,b))$.

Remarque

Il résulte de cette proposition que, pour les entiers naturels *a* et *b* non nuls, l'expression " plus grand commun diviseur " et la locution " plus grand " peuvent être prises indifféremment au sens de l'ordre naturel ou au sens de la relation " divise ".

3- Plus petit commun multiple

Théorème - Définition *Soit des entiers naturels a et b non nuls. L'ensemble M des multiples non nuls communs à a et b est non vide (car il contient ab) et possède donc un plus petit élément m qui est appelé plus petit commun multiple de a et b. Il est noté* $PPCM(a\,,b)$.

Convention Si *a* ou *b* est nul $PPCM(a\,,b)=0$.

Remarque $PPCM(a\,,b)=PPCM(b\,,a)$.

Proposition (Calcul pratique du *PPCM*) *Soit des entiers naturels a et b non nuls.*
Si $a=1$ *(respectivement* $b=1$*) alors* $PPCM(a,b)=b$ *(respectivement* $PPCM(a,b)=a$*)*

Si $a>1$ *et* $b>1$ *on considère tous les nombres premiers figurant dans les décompositions de a et b, on a* $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ *et* $b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r}$ *où pour tout i élément de* $[\![1\,,r]\!]$, p_i *est un nombre premier,* α_i *et* β_i *sont des entiers naturels éventuellement nuls ; on a alors* $PPCM(a,b)=p_1^{s_1}p_2^{s_2}\cdots p_r^{s_r}$ *avec* $s_i=\max(\alpha_i\,,\beta_i)$.

Démonstration
Soit $m=PPCM(a,b)$. On peut écrire $m=p_1^{m_1}p_2^{m_2}\cdots p_r^{m_r}$ avec m_i entier naturel pour tout *i* élément de $[\![1\,,r]\!]$ et de plus $m_i\ge\alpha_i$ et $m_i\ge\beta_i$.

Il en résulte $m_i \geq s_i$, pour tout $i \in [\![1, r]\!]$. Donc $m_i = s_i$ puisque $p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$ précédemment défini est un multiple de a et de b.

Proposition *Soit des entiers naturels a et b :*

i) tout multiple commun à a et b est un multiple de $PPCM(a, b)$;

ii) tout multiple de $PPCM(a, b)$ est un multiple commun à a et b.

Autrement dit, $a\mathbb{N} \cap b\mathbb{N} = PPCM(a, b)\mathbb{N}$.

Remarque

Il résulte de cette proposition que, pour les entiers naturels a et b non nuls, l'expression " plus petit commun multiple " et la locution " plus petit " peuvent être prises indifféremment au sens de l'ordre naturel ou au sens de la relation " divise ".

4- Théorème de Gauss

Lemme *Tout nombre premier qui divise un produit d'entiers naturels divise au moins l'un d'eux.*

Autre formulation *Soit des entiers naturels b et c supérieurs ou égaux à 1. Si p est un nombre premier qui divise bc et qui ne divise pas b alors p divise c.*

Démonstration

L'entier naturel p figure dans la décomposition de bc. Or celle-ci peut être obtenue en multipliant la décomposition de b par la décomposition de c, mais p ne divisant pas b, p ne figure pas dans la décomposition de b donc il figure dans celle de c et ainsi p divise c.

Lemme *Soit des entiers naturels a et b supérieurs ou égaux à 1. Si p est un nombre premier qui ne divise pas a et si p^α (où α est un entier non nul) divise ab alors p^α divise b.*

Démonstration

L'entier naturel p figure dans la décomposition de ab avec un exposant β supérieur ou égal à α. Or la décomposition de ab peut être obtenue en multipliant une décomposition de a par une décomposition de b, mais p ne divisent pas a, p ne figure pas dans la décomposition de a donc p^β figure dans la décomposition de b avec $\beta \geq \alpha$ et par conséquent p^α divise b.

Définition (Nombres premiers entre eux) *Deux entiers naturels non nuls sont dits premiers entre eux si leur plus grand commun diviseur est 1.*

Théorème de Gauss *Soit des entiers naturels b et c supérieurs ou égaux à 1. Si a est un entier naturel qui divise bc et qui est premier avec b alors a divise c.*

Démonstration

1er cas : $a = 1$ alors $a|c$ et le résultat est établi.

2ème cas : $a > 1$, a peut être décomposé en produit de facteurs premiers et s'écrit $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ où pour tout i élément de $[\![1, r]\!]$, p_i est un nombre premier et $\alpha_i \geq 1$.

Ainsi $p_i^{\alpha_i}$ divise a et a divise bc donc $p_i^{\alpha_i}$ divise bc.

Comme a est premier avec b, $p_i^{\alpha_i}$ divise c pour tout i élément de $[\![1, r]\!]$.

Il en résulte que p_i figure dans la décomposition de c avec un exposant β_i supérieur ou égal à α_i pour tout i élément de $[\![1, r]\!]$. Par conséquent a divise c.

5- Division euclidienne

Théorème - Définition (Division euclidienne) *Pour tout couple d'entiers naturels (a,b), b non nul, il existe un couple d'entiers naturels (q,r) unique tel que $a = bq + r$ avec $0 \leq r < b$.*

Vocabulaire *Les entiers naturels q et r sont respectivement appelés le quotient et le reste de la division euclidienne de a par b.*

Démonstration

a) Existence : soit l'ensemble B des entiers naturels n tels que $nb \leq a$.

L'ensemble B est non vide (car $0 \in B$) et B est majoré par a (car $b \geq 1$), donc B possède un plus grand élément q.

On a $bq \leq a < b(q+1)$.

En posant $r = a - bq$, on a $(bq \leq a < b(q+1)) \Leftrightarrow (a = bq + r \text{ avec } 0 \leq r < b)$.

b) Unicité : soit un couple d'entiers naturels (q',r') tel que $a = bq' + r'$ avec $0 \leq r' < b$.

On déduit de cette double inégalité que $bq' \leq a < b(q'+1)$ et par conséquent q' appartient à B alors que $q'+1$ n'appartient pas à B. Ainsi q' est le plus grand élément de B, c'est-à-dire que $q' = q$ et par conséquent $r' = r$.

Euclide (IV^{e} -III^{e} s. av. J.-C.), mathématicien grec fondateur de l'école d'Alexandrie.

IV B- DÉMARCHE 2

1- Division euclidienne

Théorème - Définition (Division euclidienne) *Pour tout couple d'entiers naturels (a,b), b non nul, il existe un couple d'entiers naturels (q,r) unique tel que $a=bq+r$ avec $0\le r<b$.*

Vocabulaire *Les entiers naturels q et r sont respectivement appelés le quotient et le reste de la division euclidienne de a par b.*

Démonstration

a) Existence : soit l'ensemble B des entiers naturels n tels que $nb\le a$.

L'ensemble B est non vide (car $0\in B$) et B est majoré par a (car $b\ge 1$), donc B possède un plus grand élément q.

On a $bq\le a<b(q+1)$.

En posant $r=a-bq$, on a $(bq\le a<b(q+1))\Leftrightarrow(a=bq+r \quad \text{avec} \quad 0\le r<b)$.

b) Unicité : soit un couple d'entiers naturels (q',r') tel que $a=bq'+r'$ avec $0\le r'<b$.

On déduit de cette double inégalité que $bq'\le a<b(q'+1)$ et par conséquent q' appartient à B alors que $q'+1$ n'appartient pas à B. Ainsi q' est le plus grand élément de B, c'est-à-dire que $q'=q$ et par conséquent $r'=r$.

2- Plus grand commun diviseur

Théorème - Définition *Soit des entiers naturels a et b non nuls, l'ensemble D des diviseurs communs à a et b est non vide. Il est majoré par a (et par b) donc il admet un plus grand élément d qui est appelé plus grand commun diviseur de a et b et noté $PGCD(a,b)$.*

Soit un entier naturel a non nul, l'ensemble D des diviseurs communs à a et 0 est l'ensemble des diviseurs de a. Il admet un plus grand élément a qui est appelé plus grand commun diviseur de a et 0 et noté $PGCD(a,0)$, ainsi $PGCD(a,0)=a$.

Convention $PGCD(0,0)=0$.

Remarque $PGCD(a,b)=PGCD(b,a)$.

Proposition *Soit des entiers naturels a et b :*

i) tout diviseur commun à a et b est un diviseur de $PGCD(a,b)$;

ii) tout diviseur de $PGCD(a,b)$ est un diviseur commun à a et b.

Autrement dit, on a $\boldsymbol{Div}(a)\cap\boldsymbol{Div}(b)=\boldsymbol{Div}(PGCD(a,b))$.

Démonstration (Algorithme d'Euclide)

Si $b=0$, le résultat est immédiat.

Si $b\neq 0$, il existe un couple (q_1,r_1) unique tel que $a=bq_1+r_1$ avec $0\le r_1<b$. Tout diviseur commun à a et b est un diviseur de r_1 donc l'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs communs à b et r_1, c'est-à-dire $\boldsymbol{Div}(a)\cap\boldsymbol{Div}(b)=\boldsymbol{Div}(b)\cap\boldsymbol{Div}(r_1)$, ainsi $PGCD(a,b)=PGCD(b,r_1)$.

Si $r_1=0$, $\boldsymbol{Div}(a)\cap\boldsymbol{Div}(b)=\boldsymbol{Div}(b)\cap\boldsymbol{Div}(0)=\boldsymbol{Div}(b)$ et $PGCD(a,b)=b$.

Sinon on remplace le couple (a,b) par le couple (b,r_1).

On itère le processus précédent, et on obtient ainsi une suite d'entiers naturels $r_1, r_2, \ldots$ strictement décroissante.

Il existe donc un entier naturel k tel que $r_k \neq 0$ et $r_{k+1} = 0$. L'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs communs à r_k et 0, c'est donc l'ensemble des diviseurs de r_k, c'est à dire $\boldsymbol{Div}(a) \cap \boldsymbol{Div}(b) = \boldsymbol{Div}(r_k)$ et $PGCD(a,b) = r_k$.

Commentaire Cette démonstration induit une méthode pratique pour déterminer le plus grand commun diviseur de deux entiers naturels.

Remarque

Il résulte de cette proposition que, pour les entiers naturels a et b non nuls, l'expression " plus grand commun diviseur " et la locution " plus grand " peuvent être prises indifféremment au sens de l'ordre naturel ou au sens de la relation " divise ".

3- Plus petit commun multiple

Théorème - Définition *Soit des entiers naturels a et b non nuls. L'ensemble M des multiples non nuls communs à a et b est non vide (car il contient ab) et possède donc un plus petit élément m qui est appelé plus petit commun multiple de a et b . Il est noté* $PPCM(a,b)$.

Convention $PPCM(0,0) = 0$.

Remarque $PPCM(a,b) = PPCM(b,a)$.

Proposition *Soit des entiers naturels a et b :*

i) tout multiple commun à a et b est un multiple de $PPCM(a,b)$;

ii) tout multiple de $PPCM(a,b)$ *est un multiple commun à a et b.*

Autrement dit, on a $a\mathbb{N} \cap b\mathbb{N} = PPCM(a,b)\mathbb{N}$.

Démonstration

Soit $m = PPCM(a,b)$ et m' un multiple commun non nul à a et b.

Il existe un couple (q,r) d'entiers naturels unique tel que $m' = mq + r$ avec $0 \leq r < m$.

a divise m et a divise m', on a a divise r. De même b divise r, ainsi r est un multiple commun à a et b mais $0 \leq r < m$ donc $r = 0$ et par conséquent m' est un multiple de m.

Remarque

Il résulte de cette proposition que, pour les entiers naturels a et b non nuls, l'expression " plus petit commun multiple " et la locution " plus petit " peuvent être prises indifféremment au sens de l'ordre naturel ou au sens de la relation " divise ".

4- Théorème de Gauss

Définition (Nombres premiers entre eux) *Deux entiers naturels non nuls sont dits premiers entre eux si leur plus grand commun diviseur est* 1.

Propriété *Soit un entier naturel a et un entier naturel p premier, alors p divise a ou p et a sont premiers entre eux.*

Démonstration

Ceci repose sur le fait que $\boldsymbol{Div}(a) \cap \boldsymbol{Div}(p) \subset \{1, p\}$.

Lemme *Soit des entiers naturels a, b et c non nuls et d le plus grand commun diviseur de a et b. Le plus grand commun diviseur de ac et bc est dc ; c'est-à-dire* $PGCD(ac, bc) = cPGCD(a, b)$.

Démonstration

Soit $\delta = PGCD(ac, bc)$.

Il existe des entiers naturels a' et b' tels que $a = da'$ et $b = db'$ donc $ac = dca'$ et $bc = dcb'$, ainsi dc est un diviseur commun de ac et bc donc dc divise δ.

Il existe un entier naturel δ' tel que $\delta = dc\delta'$ et il existe des entiers naturels α et β tels que $ac = \delta\alpha$ et $bc = \delta\beta$. On a alors $ac = dc\delta'\alpha$ et $bc = dc\delta'\beta$ donc $a = d\delta'\alpha$ et $b = d\delta'\beta$.

Ainsi $d\delta'$ est un diviseur commun à a et b, donc $d\delta'$ divise d et par conséquent $\delta'=1$.

En conclusion dc est le plus grand commun diviseur de ac et bc.

Théorème de Gauss *Soit des entiers naturels b et c supérieurs ou égaux à* 1. *Si a est un entier naturel qui divise bc et qui est premier avec b alors a divise c.*

Démonstration

$PGCD(a,b)=1$, donc $PGCD(ac,bc)=c$ d'après le lemme précédent.

Ainsi, a divise ac trivialement et a divise bc par hypothèse, donc a est un diviseur commun à ac et bc ; par conséquent a divise $PGCD(ac,bc)=c$ donc a divise c.

Corollaire *Tout nombre premier p qui divise un produit d'entiers naturels divise au moins l'un de ces entiers.*

Démonstration

Soit un nombre premier p et des entiers naturels a_1 et a_2 tels que $p|a_1a_2$, ou bien $p|a_1$ ou bien p est premier avec a_1, dans ce dernier cas $p|a_2$ d'après le théorème de Gauss.

On démontre alors par récurrence si p est premier et divise $a_1a_2\ldots a_n$ alors il existe i élément de $[\![1,n]\!]$ tel que p divise a_i.

Corollaire *Tout nombre premier p qui divise un produit de nombres premiers est égal à l'un de ces nombres.*

Démonstration

Soit un nombre premier p et des nombres premiers $p_1, p_2, \ldots, p_n$ tels que $p|p_1p_2\ldots p_n$.

D'après le corollaire précédent, il existe i élément de $[\![1,n]\!]$ tel que $p|p_i$ et comme p_i est premier et $p\neq 1$, on a $p=p_i$.

5- Unicité de la décomposition d'un entier naturel en produit de facteurs premiers

Théorème *La décomposition en produit de facteurs premiers de tout entier naturel n strictement supérieur à* 1 *sous la forme* $n=p_1\times\ldots\times p_s$, *est unique, avec, pour tout* $i\in[\![1,s]\!]$, p_i *premier, et, lorsque* $s>1$, *pour tout* $i\in[\![1,s-1]\!]$, $p_i\leq p_{i+1}$.

Démonstration

Si n admet deux décompositions en produits de facteurs premiers :

$n=p_1\times\ldots\times p_s$ avec pour tout i élément de $[\![1,s]\!]$, p_i premier et $p_1\leq p_2\leq\ldots\leq p_s$,

$n=q_1\times\ldots\times q_r$ avec pour tout i élément de $[\![1,r]\!]$, q_i premier et $q_1\leq q_2\leq\ldots\leq q_r$.

On a $p_1|n$ donc il existe j élément de $[\![1,r]\!]$ tel que $p_1=q_j$, donc $q_1\leq p_1$.

De même, $q_1|n$ entraîne $p_1\leq q_1$, ainsi $p_1=q_1$.

En divisant chaque décomposition de n on obtient $n_1=p_2\times\ldots\times p_s=q_2\times\ldots\times q_r$, on a de même $p_2=q_2$.

Si $s=r$, l'unicité est démontrée.

Si $s>r$, on a $p_{r+1}\times\ldots\times p_s=1$, ce qui est impossible car pour tout i élément de $[\![1,s]\!]$, $p_i\neq 1$.

Remarque D'un point de vue pratique on écrit la décomposition d'un entier naturel n en produit de facteurs premiers sous la forme $n=p_1^{\alpha_1}\times\ldots\times p_s^{\alpha_s}$, avec, pour tout $i\in[\![1,s]\!]$, p_i premier et α_i entier naturel non nul, les p_i étant deux à deux distincts.

V- LES BASES DE NUMÉRATION

1- Le problème posé et le principe retenu

a) Problème

Il s'agit de désigner tous les entiers naturels.

On utilise pour cela des symboles appelés chiffres.

L'écriture choisie doit permettre de comparer les nombres et d'effectuer commodément les opérations usuelles.

b) Principe de la numération en base *b*

On choisit un entier naturel b strictement supérieur à 1 qui sera appelé base (la base usuelle est dix). On dispose d'un nombre fini de chiffres désignant les entiers naturels $0,1,2,\ldots,(b-1)$.

On va montrer que chaque entier naturel N non nul s'exprime, de façon unique, en fonction des puissances successives de la base b (cela correspond en base dix aux unités, aux dizaines, aux centaines...).

Il existe un entier naturel n tel que $N=\sum_{i=0}^{n}\alpha_i b^i=\alpha_n b^n+\alpha_{n-1}b^{n-1}+\ldots+\alpha_2 b^2+\alpha_1 b+\alpha_0$

avec, pour i élément de $[\![0,n]\!]$, $\alpha_i\in[\![0,b-1]\!]$ et $\alpha_n\neq 0$.

Cette expression de type polynomial permet la comparaison et les opérations usuelles.
On écrit $N=\overline{\alpha_n\ldots\alpha_1\alpha_0}$.

L'écriture d'un entier naturel apparaît alors comme une suite finie de chiffres dont la position et la valeur sont significatives, on parle de numération de position.
L'écriture de N comporte $(n+1)$ chiffres.

2- Écriture en base *b*

a) Unicité

L'expression d'un entier naturel N non nul sous la forme $N=\alpha_n b^n+\ldots+\alpha_1 b+\alpha_0=\sum_{i=0}^{n}\alpha_i b^i$

avec pour i élément de $[\![0,n]\!]$, $\alpha_i\in[\![0,b-1]\!]$, *et,* $\alpha_n\neq 0$ *est unique.*

Démonstration

Soit une autre expression de $N=\beta_m b^m+\ldots+\beta_1 b+\beta_0=\sum_{j=0}^{m}\beta_j b^j$, avec pour j élément de $[\![0,m]\!]$, $\beta_j\in[\![0,b-1]\!]$ et $\beta_m\neq 0$.

1° $\underline{m=n}$

En utilisant l'écriture $N=\sum_{i=0}^{n}\alpha_i b^i$, on a $b^n\le N\le\sum_{i=0}^{n}(b-1)b^i$; comme $\sum_{i=0}^{n}(b-1)b^i=b^{n+1}-1$,

on en déduit $b^n\le N<b^{n+1}$.

De même en utilisant l'écriture $N=\sum_{j=0}^{m}\beta_j b^j$, on en déduit $b^m\le N<b^{m+1}$.

On déduit de ces deux doubles inégalités $m=n$, car par exemple $m<n$ entraîne $N<b^{m+1}\le b^n\le N$.

2° Nous allons proposer deux méthodes pour terminer la démonstration

- Première méthode : indices croissants.
  - $\alpha_0=\beta_0$ car il s'agit du reste de la division euclidienne de N par b.
  - S'il existe un plus petit entier p tel que $\alpha_p\neq\beta_p$ d'après ce qui précède $p>0$.

$$N = \underbrace{(\alpha_0 + \alpha_1 b + \ldots + \alpha_{p-1} b^{p-1})}_{A} + (\alpha_p b^p + \ldots + \alpha_n b^n)$$

$$N = \underbrace{(\beta_0 + \beta_1 b + \ldots + \beta_{p-1} b^{p-1})}_{B} + (\beta_p b^p + \ldots + \beta_n b^n)$$

De l'égalité $A = B$ on déduit, $\alpha_p b^p + \ldots + \alpha_n b^n = \beta_p b^p + \ldots + \beta_n b^n$.

$$b^p(\alpha_p + \ldots + \alpha_n b^{n-p}) = b^p(\beta_p + \ldots + \beta_n b^{n-p})$$

$$\alpha_p + \ldots + \alpha_n b^{n-p} = \beta_p + \ldots + \beta_n b^{n-p} = M$$

On a alors $\alpha_p = \beta_p$ car il s'agit du reste de la division euclidienne de M par b, ce qui est contradictoire, donc l'unicité est prouvée.

➢ Deuxième méthode : indices décroissants.

- $\alpha_n = \beta_n$ car il s'agit du quotient de la division euclidienne de N par b^n car on a vu que

$$\begin{cases} \alpha_0 + \alpha_1 b + \ldots + \alpha_{n-1} b^{n-1} < b^n \\ \beta_0 + \beta_1 b + \ldots + \beta_{n-1} b^{n-1} < b^n \end{cases}$$

- S'il existe un plus grand entier s tel que $\alpha_s \neq \beta_s$ d'après ce qui précède $s < n$.

$$N = (\alpha_0 + \alpha_1 b + \ldots + \alpha_s b^s) + \underbrace{(\alpha_{s+1} b^{s+1} + \ldots + \alpha_n b^n)}_{C}$$

$$N = (\beta_0 + \beta_1 b + \ldots + \beta_s b^s) + \underbrace{(\beta_{s+1} b^{s+1} + \ldots + \beta_n b^n)}_{D}$$

De l'égalité $C = D$ on déduit,

$$(\alpha_0 + \alpha_1 b + \ldots + \alpha_{s-1} b^{s-1}) + \alpha_s b^s = (\beta_0 + \beta_1 b + \ldots + \beta_{s-1} b^{s-1}) + \beta_s b^s = P.$$

On a $\alpha_s = \beta_s$ car il s'agit des quotients de la division euclidienne de P par b^s car

$$\begin{cases} \alpha_0 + \alpha_1 b + \ldots + \alpha_{s-1} b^{s-1} < b^s \\ \beta_0 + \beta_1 b + \ldots + \beta_{s-1} b^{s-1} < b^s \end{cases}$$

Ainsi $\alpha_s = \beta_s$, ce qui est contradictoire, donc l'unicité est prouvée.

Remarque Cela suggère deux modes d'obtention des α_i.

b) Obtention des α_i dans l'ordre des indices croissants

La division euclidienne de N par b se traduit par $N = bq_0 + r_0$ avec $0 \leq r_0 < b$, ainsi $\alpha_0 = r_0$.

Si $q_0 = 0$, c'est fini.

Sinon la division euclidienne de q_0 par b se traduit par $q_0 = bq_1 + r_1$ avec $0 \leq r_1 < b$, ainsi $\alpha_1 = r_1$.

Si $q_1 = 0$, c'est fini.

Sinon .....

La suite q_0, q_1, ... ainsi obtenue est une suite d'entiers naturels strictement décroissante, il existe donc un entier naturel n tel que $q_n = 0$.

L'écriture $N = ((\ldots((\alpha_n b + \alpha_{n-1})b + \alpha_{n-2})\ldots\alpha_2)b + \alpha_1) + \alpha_0$ montre que $\alpha_0, \alpha_1, \ldots, \alpha_n$ s'obtiennent comme restes successifs de la division de N par b puis des quotients successifs obtenus.

c) Obtention des α_i dans l'ordre des indices décroissants

Soit un entier naturel N non nul, la suite $(b^s)_{s\in\mathbb{N}}$ étant strictement croissante et non majorée, il existe un seul entier naturel n tel que : $b^n \leq N < b^{n+1}$.

Effectuons la division euclidienne de N par b^n, on obtient $N = b^n q'_n + r'_n$ avec $0 \leq r'_n < b^n$.

On a $q'_n < b$ et de plus $q'_n \neq 0$, ainsi $\alpha_n = q'_n$.

Effectuons la division euclidienne de r'_n par b^{n-1}, on obtient $r_n = b^{n-1} q'_{n-1} + r'_{n-1}$ avec $0 \leq r'_{n-1} < b^{n-1}$.

On a $q'_{n-1} < b$, ainsi $\alpha_{n-1} = q'_{n-1}$.

On continue jusqu'à la division par b.

d) Notations et exemples

On note $N = \overline{\alpha_n \alpha_{n-1} \ldots \alpha_2 \alpha_1 \alpha_0}^{\,b}$ (lorsque aucun risque de confusion n'est possible, le " b " est omis).

Pour b inférieur ou égal à dix, on utilise les b premiers symboles de la liste 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

Par exemple, en base deux on utilise les symboles 0 et 1.

Ainsi $\overline{1000110} = 1\times2^6 + 0\times2^5 + 0\times2^4 + 0\times2^3 + 1\times2^2 + 1\times2^1 + 0\times2^0 = 2^6 + 2^2 + 2$.

En base seize, par exemple, (base très utilisée en informatique et appelée base hexadécimale) nous serions obligés de rajouter six symboles pour désigner dix (A), onze (B), douze (C), treize (D), quatorze (E) et quinze (F).

Par exemple quatorze s'écrit $\overline{1110}$ en base deux, $\overline{112}$ en base trois, $\overline{32}$ en base quatre, $\overline{22}$ en base six, $\overline{20}$ en base sept, $\overline{14}$ en base dix, et $\overline{\text{E}}$ en base seize.

Remarque En base b, l'entier naturel b s'écrit $\overline{10}$, b^2 s'écrit $\overline{100}$, b^3 s'écrit $\overline{1000}$.

Les " symboles " utilisés sont au nombre de b et désignent les entiers naturels de 0 à $b-1$.

L'écriture $\overline{1023}$ est une écriture d'un entier naturel dans une base b, $b > 3$.

Dans une telle base, l'écriture $\overline{1023}$ désigne l'entier naturel $1b^3 + 0b^2 + 2b^1 + 3b^0$.

C'est à dire :
- en base quatre $\overline{1023} = 4^3 + 2\times4 + 3$ qui s'écrit 75 en base dix;
- en base sept $\overline{1023} = 7^3 + 2\times7 + 3$ qui s'écrit 360 en base dix.

3- Comparaison de nombres écrits en base *b*

Soit des entiers naturels N et M dont voici les écritures dans la base b,

$N = \overline{\alpha_n \alpha_{n-1} \ldots \alpha_2 \alpha_1 \alpha_0}$ et $M = \overline{\beta_m \beta_{m-1} \ldots \beta_2 \beta_1 \beta_0}$.

Comment comparer N et M à partir de leurs écritures ?

1er cas : $n < m$

On a $N < b^{n+1} \le b^m \le M$, par conséquent $N < M$.

2ème cas : $n = m$.

Si pour tout i élément de $[\![0, n]\!]$, $\alpha_i = \beta_i$ alors $N = M$,

Sinon, soit p le plus grand indice tel que $\alpha_p \neq \beta_p$.

On suppose que $\alpha_p < \beta_p$, alors en retranchant $\alpha_n b^n + \ldots + \alpha_{p+1} b^{p+1}$ à M et N,

il reste à comparer $N_1 = \alpha_p b^p + (\alpha_{p-1} b^{p-1} + \ldots + \alpha_0)$ et $M_1 = \beta_p b^p + (\beta_{p-1} b^{p-1} + \ldots + \beta_0)$.

On a $N_1 < \alpha_p b^p + b^p \le \beta_p b^p \le M_1$, par conséquent $N < M$.

Règles de comparaison

① On compare les longueurs des écritures, c'est à dire $n+1$ et $m+1$.

② On compare " chiffre à chiffre " à partir de la gauche lorsque le nombre de chiffres est le même. On parle alors **d'ordre lexicographique**. Les chiffres jouent pour les écritures des entier naturels un rôle analogue à celui des lettres pour les mots.

4- Opérations en base *b*

Étant donné des entier naturels N et M écrits en base b, comment obtient-on l'écriture de $N+M$ et de $N\times M$ en base b ?

Nous allons traiter un exemple en base sept.

Soit $M=\overline{231}$ et $N=\overline{415}$, on obtient : $M+N=\overline{646}$,

mais lorsque $M=\overline{231}$ et $N=\overline{454}$, on obtient $M+N=\overline{1015}$.

Il est utile d'établir les tables de Pythagore pour l'addition et la multiplication en base sept, c'est-à-dire les tables d'addition et de multiplication des entiers strictement inférieurs à sept.

Addition

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	10
2	2	3	4	5	6	10	11
3	3	4	5	6	10	11	12
4	4	5	6	10	11	12	13
5	5	6	10	11	12	13	14
6	6	10	11	12	13	14	15

Multiplication

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	11	13	15
3	0	3	6	12	15	21	24
4	0	4	11	15	22	26	33
5	0	5	13	21	26	34	42
6	0	6	15	24	33	42	51

On applique les mêmes algorithmes que pour les opérations en base dix.

5- Changements de base

a) Passage de la base dix à la base *b*

• Comment écrire 724 en base trois ?

On applique l'algorithme permettant d'obtenir les α_i dans l'ordre croissant.

Les symboles utilisés dans cette base sont : 0, 1 et 2.

724	3						
1	237	3					
	0	79	3				
		1	26	3			
			2	8	3		
				2	2	3	
					2	0	

Ainsi $724=\mathbf{2}\times3^5+\mathbf{2}\times3^4+\mathbf{2}\times3^3+\mathbf{1}\times3^2+\mathbf{0}\times3^1+\mathbf{1}\times3^0$

C'est à dire : $724=\overline{222101}$

• Comment écrire 10640143 en base hexadécimale ?

10640143	16								
15	665008	16							
	0	41563	16						
		11	2597	16					
			5	162	16				
				2	10	16			
					10	0			

Ainsi : $10640143 = \mathbf{10}\times16^5 + \mathbf{2}\times16^4 + \mathbf{5}\times16^3 + \mathbf{11}\times16^2 + \mathbf{0}\times16^1 + \mathbf{15}\times16^0$.

C'est à dire : $10640143 = \overline{A25B0F}$.

b) Passage de la base *b* à la base dix

• Un entier naturel s'écrit $\overline{20345}$ en base six, comment s'écrit-il en base dix ?

$\overline{20345} = \mathbf{2}\times6^4 + \mathbf{0}\times6^3 + \mathbf{3}\times6^2 + \mathbf{4}\times6^1 + \mathbf{5}\times6^0 = 2729$.

• Un entier naturel s'écrit $\overline{7AE8F}$ en base hexadécimale, comment s'écrit-il en base dix ?

$\overline{7AE8F} = \mathbf{7}\times16^4 + \mathbf{10}\times16^3 + \mathbf{14}\times16^2 + \mathbf{8}\times16^1 + \mathbf{15}\times16^0 = 503439$.

c) Passage de la base *b* à la base *b'*

En général on passe par l'intermédiaire de la base dix.

6- Caractères de divisibilité

Il s'agit de déterminer, à partir de l'écriture d'un entier naturel $N = \overline{\alpha_n\alpha_{n-1}\ldots\alpha_2\alpha_1\alpha_0}$ dans une base b, un critère de divisibilité de N par un entier naturel a.

Remarque $b|n \Leftrightarrow \alpha_0 = 0$.

a) Divisibilité par un diviseur *a* de *b* (En base dix, par 2 ou 5)

$a|N \Leftrightarrow a|\alpha_0$

Il suffit d'examiner le dernier chiffre, par exemple en base dix :

$2|N \Leftrightarrow \alpha_0 \in \{0,2,4,6,8\}$

$5|N \Leftrightarrow \alpha_0 \in \{0,5\}$

b) Divisibilité par un diviseur *a* de b^2 (En base dix, par 4 ou 25)

$a|N \Leftrightarrow a|\overline{\alpha_1\alpha_0}$

Par exemple en base dix ,

$25|N \Leftrightarrow N$ a une écriture se terminant par 00 ou 25 ou 50 ou 75.

c) Divisibilité par un diviseur *a* de (*b* – 1) (pour *b* ≥ 3) (En base dix, par 3 ou 9)

Pour tout entier naturel k il existe un entier naturel u tel que $b^k = u(b-1)+1$ car $b^k - 1$ est divisible par $b-1$.

Le reste de la division euclidienne de $N = \overline{\alpha_n\ldots\alpha_0}$ par $(b-1)$ ou l'un de ses diviseurs est le même que celui de $S_n = \alpha_n + \alpha_{n-1} + \ldots + \alpha_1 + \alpha_0$ par $(b-1)$.

L'itération de ce processus nous ramène à un entier strictement inférieur à b. Ainsi, il suffit de connaître la liste des multiples de a strictement inférieurs à b.

d) Divisibilité par un diviseur de (*b* + 1) (En base dix par 11)

Pour tout entier naturel k il existe un entier naturel u tel que :

si k est pair alors $b^k = ((b+1)-1)^k = u(b+1)+1$;

si k est impair alors $b^k = ((b+1)-1)^k = u(b+1)-1$.

Nous allons traiter ce cas au travers d'un exemple.

L'entier naturel N qui s'écrit 17281948091 en base dix, est-il divisible par 11 ?

1ère méthode

$N = 91+80\times100+94\times100^2+81\times100^3+72\times100^4+1\times100^6$.

Or $100^k - 1 = (100-1)(100^{k-1}+100^{k-2}+\ldots+1)$

$100^k - 1 = 99(100^{k-1}+100^{k-2}+\ldots+1)$

Ainsi le reste de la division euclidienne de 100^k par 11 est 1, donc N a le même reste dans la division euclidienne par 11 que $N_1 = 91+80+94+81+72+1$, c'est à dire que $N_1 = 419$.

Or cet entier naturel $N_1 = 419$ a, par le même processus, le même reste dans la division euclidienne par 11 que $N_2 = 19+4$, c'est à dire que $N_2 = 23$.

Le processus se " stabilise ".

En effectuant la division euclidienne de 23 par 11, on peut conclure.

2ème méthode

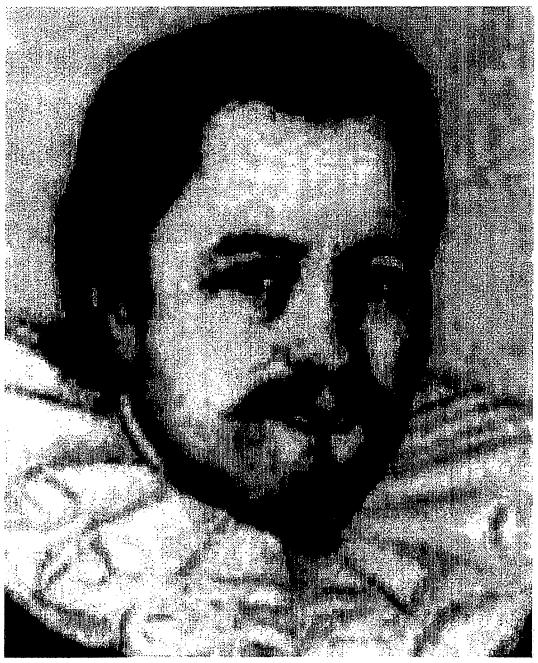
La somme des chiffres d'indices pairs est $P = 1+0+4+1+2+1 = 9$ et d'indices impairs $I = 9+8+9+8+7 = 41$.

L'entier naturel N sera divisible par 11 si et seulement si $41-9 = 32$ est divisible par 11.

Répétons l'algorithme précédent.

L'entier naturel 32 est divisible par 11 si et seulement si $3-2 = 1$ est divisible par 11.

D'où la conclusion.



Stevin (Simon), dit Simon de Bruges (Bruges, 1548 - La Haye, 1620), savant flamand. Il répandit l'usage du système décimal.

Partie B - ARITHMÉTIQUE DANS $\mathbb{Z}$

I. L'ENSEMBLE $\mathbb{Z}$

1- Construction du groupe ($\mathbb{Z}$, +) (symétrisation de $\mathbb{N}$ pour l'addition)

a) Problème

Soit des entiers naturels a et b, l'équation (E) $x+b=a$ n'a pas toujours de solution dans $\mathbb{N}$.

- Si $b \leq a$ la solution de l'équation (E) est $x=a-b$.
- Si $b > a$ l'équation (E) n'a pas de solution dans $\mathbb{N}$.

Nous cherchons un groupe commutatif que nous appellerons $(\mathbb{Z},+)$ tel que $(\mathbb{N},+)$ s'identifie à une partie stable de $(\mathbb{Z},+)$ et que l'équation (E) précédente possède toujours une solution. Nous imposons par ailleurs que ce groupe soit minimal au sens de l'inclusion.

Ce problème est celui de la symétrisation de $\mathbb{N}$ pour l'addition.

Cette construction est classique et les démonstrations qui suivent peuvent être occultées en première lecture.

b) L'ensemble $(\mathbb{N}\times\mathbb{N},+)$

- L'ensemble $\mathbb{N}\times\mathbb{N}$ peut être muni d'une addition notée +, définie pour tous couples d'entiers naturels (a,b) et (a',b') par $(a,b)+(a',b')=(a+b,a'+b')$.

Remarque Si $b \leq a$ (resp. $b' \leq a'$) notons x_1 (resp. x_2) la solution de l'équation $x+b=a$ (resp. $x+b'=a'$) alors x_1+x_2 est la solution de $x+(b+b')=a+a'$.

Propriété *L'addition dans* $\mathbb{N}\times\mathbb{N}$ *est associative, commutative, admet* $(0,0)$ *pour élément neutre et tout élément de* $\mathbb{N}\times\mathbb{N}$ *est régulier.*

- L'ensemble $\mathbb{N}\times\mathbb{N}$ peut être muni d'une relation notée $\mathcal{R}$ définie pour tous couples d'entiers naturels (a,b) et (a',b') par $(a,b)\mathcal{R}(a',b') \Leftrightarrow a+b'=b+a'$.

Remarque Si $b \leq a$ (resp. $b' \leq a'$) notons x_1 (resp. x_2) la solution de l'équation $x+b=a$ (resp. $x+b'=a'$) alors ($x_1=x_2 \Leftrightarrow a+b'=b+a'$).

En effet $(x_1+b)+a'=a+a'=(x_2+b')+a$, donc $x_1=x_2 \Leftrightarrow a+b'=b+a'$.

Propriété *La relation* $\mathcal{R}$ *est une relation d'équivalence compatible avec l'addition dans* $\mathbb{N}\times\mathbb{N}$.

Cela signifie que cette relation vérifie les propriétés suivantes :

Réflexivité $(a,b)\mathcal{R}(a,b)$;

Symétrie $(a,b)\mathcal{R}(a',b') \Rightarrow (a',b')\mathcal{R}(a,b)$;

Transitivité $((a,b)\mathcal{R}(a',b')$ et $(a',b')\mathcal{R}(a'',b'')) \Rightarrow (a,b)\mathcal{R}(a'',b'')$;

Compatibilité avec l'addition

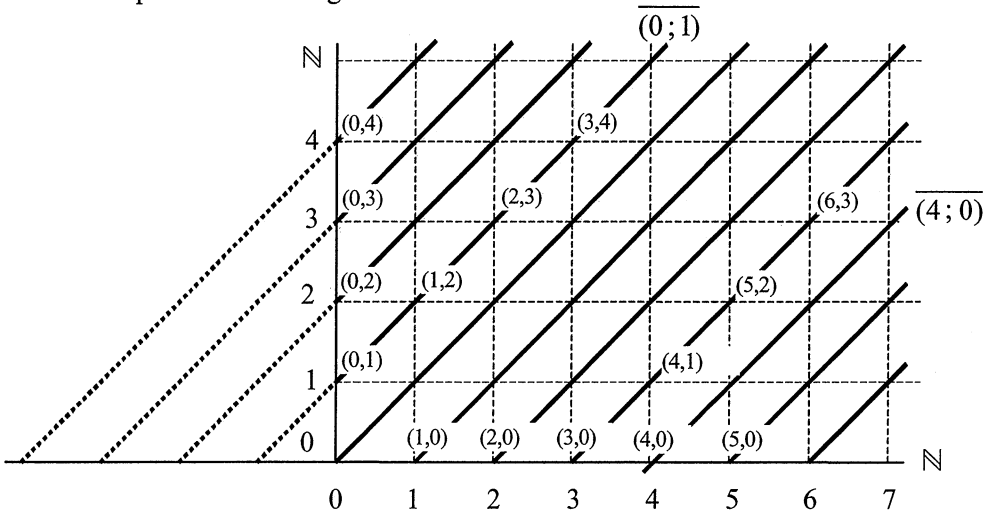
$((a,b)\mathcal{R}(c,d)$ et $(a',b')\mathcal{R}(c',d')) \Rightarrow ((a,b)+(a',b'))\mathcal{R}((c,d)+(c',d'))$.

c) Le groupe $(\mathbb{N}\times\mathbb{N}/\mathcal{R},\dot{+})$

Définition *On appelle classe d'équivalence de l'élément (a,b) que l'on note $\overline{(a,b)}$, l'ensemble des couples (x,y) tels que $(x,y)\mathcal{R}(a,b)$.*

On note $\mathbb{N}\times\mathbb{N}/\mathcal{R}$ l'ensemble des classes d'équivalence de $\mathbb{N}\times\mathbb{N}$ pour la relation $\mathcal{R}$.

En utilisant une représentation cartésienne de l'ensemble $\mathbb{N}\times\mathbb{N}$, une classe d'équivalence est l'ensemble des couples situés sur une parallèle à la diagonale de $\mathbb{N}\times\mathbb{N}$.



La compatibilité de la relation $\mathcal{R}$ avec l'addition de $\mathbb{N}\times\mathbb{N}$ permet de définir dans $\mathbb{N}\times\mathbb{N}/\mathcal{R}$ une addition notée $\dot{+}$ de la manière suivante :

soit x et x' des classes d'équivalences et soit (a,b) et (c,d) (resp. (a',b') et (c',d')) des éléments de la classe x (resp. x') alors $(a+a',b+b')$ et $(c+c',d+d')$ appartiennent à la même classe.

Définition *Pour toutes classes d'équivalences x et x', on note $x\dot{+}x'$ la classe d'équivalence de la somme d'un représentant de x et d'un représentant de x'.*

Propriété *Cette addition dans $\mathbb{N}\times\mathbb{N}/\mathcal{R}$ est associative, commutative, admet $\overline{(0,0)}$ pour élément neutre et tout élément est régulier. De plus tout élément $\overline{(a,b)}$ admet $\overline{(b,a)}$ comme symétrique (dit aussi opposé).*

Il en résulte que $(\mathbb{N}\times\mathbb{N}/\mathcal{R},\dot{+})$ est un groupe commutatif.

Ecriture simplifiée

Si $a\geq b$, $\overline{(a,b)}=\overline{(a-b,0)}$

Si $a<b$, $\overline{(a,b)}=\overline{(0,b-a)}$

Ainsi tout élément de $\mathbb{N}\times\mathbb{N}/\mathcal{R}$ est du type $\overline{(n,0)}$ ou du type $\overline{(0,n)}$ avec n entier naturel.

d) Identification de $(\mathbb{N},+)$ à une partie de $(\mathbb{N}\times\mathbb{N}/\mathcal{R},\dot{+})$

On considère l'application $\varphi:\mathbb{N}\to\mathbb{N}\times\mathbb{N}/\mathcal{R}$

$$x\mapsto\overline{(x,0)}$$

Cette application φ est injective.

Pour tous entiers naturels x et y, $\varphi(x+y)=\varphi(x)\dot{+}\varphi(y)$.

Ceci entraîne que $\varphi(\mathbb{N})$ est stable.

En conséquence $(\mathbb{N},+)$ s'identifie avec une partie stable de $(\mathbb{N}\times\mathbb{N}/\mathcal{R},\dot{+})$.

e) Le groupe $(\mathbb{Z},+)$

Tout groupe contenant l'élément $\overline{(x,0)}$ doit contenir son opposé, c'est à dire $\overline{(0,x)}$, donc tout groupe contenant $\varphi(\mathbb{N})$ contient $\mathbb{N}\times\mathbb{N}/\mathcal{R}$.

Le groupe $(\mathbb{N}\times\mathbb{N}/\mathcal{R},\dot{+})$ est une solution au problème posé. On le note $(\mathbb{Z},+)$. Les éléments de $\mathbb{Z}$ sont appelés entiers relatifs.

Notations On notera désormais + l'addition dans $\mathbb{Z}$, x l'élément $\overline{(x,0)}$ et $-x$ l'élément $\overline{(0,x)}$.

Par abus de notation on note $\mathbb{N}$ l'ensemble des classes $\overline{(x,0)}$ et $-\mathbb{N}$ l'ensemble des classes $\overline{(0,x)}$.
Compte tenu de ces abus de notation on a $\mathbb{Z}=\mathbb{N}\cup(-\mathbb{N})$ et $\mathbb{N}\cap(-\mathbb{N})=\{0\}$.

Conclusion Il existe un ensemble $\mathbb{Z}$, muni d'une addition notée +, tel que :

i) $(\mathbb{Z},+)$ est un groupe commutatif ;

ii) $(\mathbb{N},+)$ est une partie stable de $(\mathbb{Z},+)$;

iii) il n'existe pas de sous-groupe additif de $\mathbb{Z}$, distinct de $\mathbb{Z}$, dont $\mathbb{N}$ est une partie stable.

Théorème *Soit des entiers relatifs a et b, l'équation* $x+b=a$ *admet une et une seule solution dans* $\mathbb{Z}$.

Démonstration

$$\begin{aligned} x+b=a &\Leftrightarrow (x+b)+(-b)=a+(-b)\\ &\Leftrightarrow x+(b+(-b))=a+(-b)\\ &\Leftrightarrow x+0=a+(-b)\\ &\Leftrightarrow x=a+(-b)\end{aligned}$$

Notation et vocabulaire L'entier relatif $a+(-b)$ est noté $a-b$ et s'appelle différence de a et b.

2- Multiplication dans $\mathbb{Z}$

• L'ensemble $\mathbb{N}\times\mathbb{N}$ peut être muni d'une deuxième loi de composition interne appelée multiplication et notée $\times$ définie pour tous couples d'entiers naturels (a,b) et (a',b') par $(a,b)\times(a',b')=(aa'+bb',a'b+ab')$.

Remarque Si $b\le a$ (resp. $b'\le a'$) notons x_1 (resp. x_2) la solution de l'équation $x+b=a$ (resp. $x+b'=a'$) alors x_1x_2 est la solution de $x+(a'b+ab')=aa'+bb'$.

En effet $x_1+b=a$ et $x_2+b'=a'$.

Donc $(x_1+b)(x_2+b')=aa'$

$$x_1x_2+bx_2+b'x_1+bb'=aa'$$
$$x_1x_2+bx_2+bb'+b'x_1+bb'=aa'+bb'$$
$$x_1x_2+b\underbrace{(x_2+b')}_{a'}+b'\underbrace{(x_1+b)}_{a}=aa'+bb'$$
$$x_1x_2+(a'b+ab')=aa'+bb'$$

Propriété *La multiplication dans* $\mathbb{N}\times\mathbb{N}$ *est associative, commutative, admet* (1,0) *pour élément neutre. De plus la relation* $\mathcal{R}$ *est compatible avec la multiplication.*

Dire que $\mathcal{R}$ est compatible avec la multiplication signifie que

$$((a,b)\mathcal{R}(c,d) \text{ et } (a',b')\mathcal{R}(c',d'))\Rightarrow((a,b)\times(a',b'))\mathcal{R}((c,d)\times(c',d'))$$

On peut donc munir $\mathbb{Z}$ d'une multiplication notée $\dot{\times}$.

Écritures simplifiées (règles de calcul) :

- $(\overline{x,0})\dot{\times}(\overline{y,0}) = (\overline{xy,0})$;
- $(\overline{0,x})\dot{\times}(\overline{y,0}) = (\overline{0,xy})$;
- $(\overline{x,0})\dot{\times}(\overline{0,y}) = (\overline{0,xy})$;
- $(\overline{0,x})\dot{\times}(\overline{0,y}) = (\overline{xy,0})$.

Propriété *La multiplication dans $\mathbb{Z}$ est associative, commutative, admet 1 pour élément neutre et de plus elle est distributive par rapport à l'addition.*

La première de ces égalités montre que $\mathbb{N}$ est une partie stable de $\mathbb{Z}$ pour la multiplication..

Ces règles de calculs s'écrivent avec la notation usuelle :

$x\dot{\times}y = xy$ $\quad$ $(-x)\dot{\times}y = -xy$ $\quad$ $x\dot{\times}(-y) = -xy$ $\quad$ $(-x)\dot{\times}(-y) = xy$

Les quatre formules ci-dessus où x et y désignent des entiers naturels sont encore valables lorsque x et y sont des entiers relatifs.

Dans tout ce qui suit on notera $x \times y$ ou xy le produit des entiers relatifs x et y.

En particulier, $(-x)\times y = x\times(-y) = -xy$ et $(-x)\times(-y) = x\times y = xy$.

Autres propriétés *Etant donné des entiers relatifs x, y et z,*

① $0\times x = x\times 0 = 0$;

② $xy = 0 \Leftrightarrow (x = 0$ ou $y = 0)$;

③ $(x \neq 0$ et $xy = xz) \Rightarrow y = z$.

Définition (puissance n-ième) *Soit un entier relatif a et un entier naturel n non nul, l'entier relatif $\underset{1}{a}\times\ldots\times\underset{n}{a}$ est appelé puissance n-ième de a. Il est noté a^n.*

L'entier relatif a^n se lit « a exposant n » ou « a puissance n »

Remarque $a^1 = a$.

Propriétés *Soit des entiers relatifs a et b, et, des entiers naturels m et n non nuls,*

- $a^m \times a^n = a^{m+n}$;
- $a^n \times b^n = (a\times b)^n$;
- $(a^m)^n = a^{mn}$.

Convention *Soit un entier relatif a non nul,* $a^0 = 1$.

Conséquence Les propriétés précédentes sont encore vraies lorsque a et b sont non nuls, et, m ou n nul.

3- Ordre dans $\mathbb{Z}$

a) Définition *Soit des entiers relatifs a et b, on écrit $a \leq b$ pour signifier qu'il existe un entier naturel d tel que $b = a + d$.*

La relation "$a \leq b$" se lit « a est inférieur ou égal à b ».

Remarque Lorsqu'un tel entier naturel d existe, il est unique.

Vocabulaire et notation :

- la relation $a \leq b$, s'écrit aussi $b \geq a$ et se lit « b est supérieur ou égal à a » ;
- le nombre d est noté $b - a$. Il est appelé différence de b et a ;
- lorsque $(a \leq b$ et $a \neq b)$ on écrit $a < b$. Cette relation " $a < b$ " se lit « a est strictement inférieur à b » ;

- la relation $a < b$, s'écrit aussi $b > a$ et se lit « b est strictement supérieur à a ».

b) Théorème *La relation $\leq$ ainsi définie sur $\mathbb{Z}$ est une relation d'ordre total.*

Cela signifie que, étant donné des entiers relatifs a, b et c, cette relation vérifie les propriétés suivantes :

Réflexivité $a \leq a$;

Antisymétrie $(a \leq b \text{ et } b \leq a) \Rightarrow a = b$;

Transitivité $(a \leq b \text{ et } b \leq c) \Rightarrow a \leq c$.

Cette relation est alors une relation d'ordre.
Cet ordre est de plus total car pour tous entiers relatifs a et b on a : $a \leq b$ ou $b \leq a$.

Propriété *L'ordre ainsi défini dans $\mathbb{Z}$ prolonge l'ordre naturel de $\mathbb{N}$.*

Propriété (Compatibilité de cette relation avec l'addition dans $\mathbb{Z}$) *Soit des entiers relatifs p, q et r,*

$$p \leq q \Rightarrow p + r \leq q + r$$

Corollaire *Soit des entiers relatifs p, q, p' et q',* $(p \leq q \text{ et } p' \leq q') \Rightarrow p + p' \leq q + q'$.

Corollaire *Soit des entiers relatifs p et q,* $p \leq q \Leftrightarrow -q \leq -p$.

Propriété (Compatibilité de cette relation avec la multiplication par un entier naturel non nul) *Soit des entiers relatifs p* et *q et un entier naturel r non nul,*

$$p \leq q \Leftrightarrow pr \leq qr.$$

Corollaire *Soit des entiers relatifs p, q et un élément r non nul de* $-\mathbb{N}$

$$p \leq q \Leftrightarrow pr \geq qr.$$

c) Propriétés de $\mathbb{Z}$ liées à l'ordre

- *L'ensemble $\mathbb{Z}$ ne possède pas de plus grand élément.*
- *L'ensemble $\mathbb{Z}$ ne possède pas de plus petit élément.*
- *Toute partie non vide majorée de $\mathbb{Z}$ admet un plus grand élément.*
- *Toute partie non vide minorée de $\mathbb{Z}$ admet un plus petit élément.*

d) Vocabulaire, notations

Soit un entier relatif x :

- lorsque $x \geq 0$ on dit que x est positif ;
- lorsque $x > 0$ on dit que x est strictement positif ;
- lorsque $x \leq 0$ on dit que x est négatif ;
- lorsque $x < 0$ on dit que x est strictement négatif ;
- l'ensemble des entiers relatifs positifs est $\mathbb{N}$ et se note $\mathbb{Z}_+$;
- l'ensemble des entiers relatifs négatifs est $-\mathbb{N}$ et se note $\mathbb{Z}_-$.

4- Valeur absolue

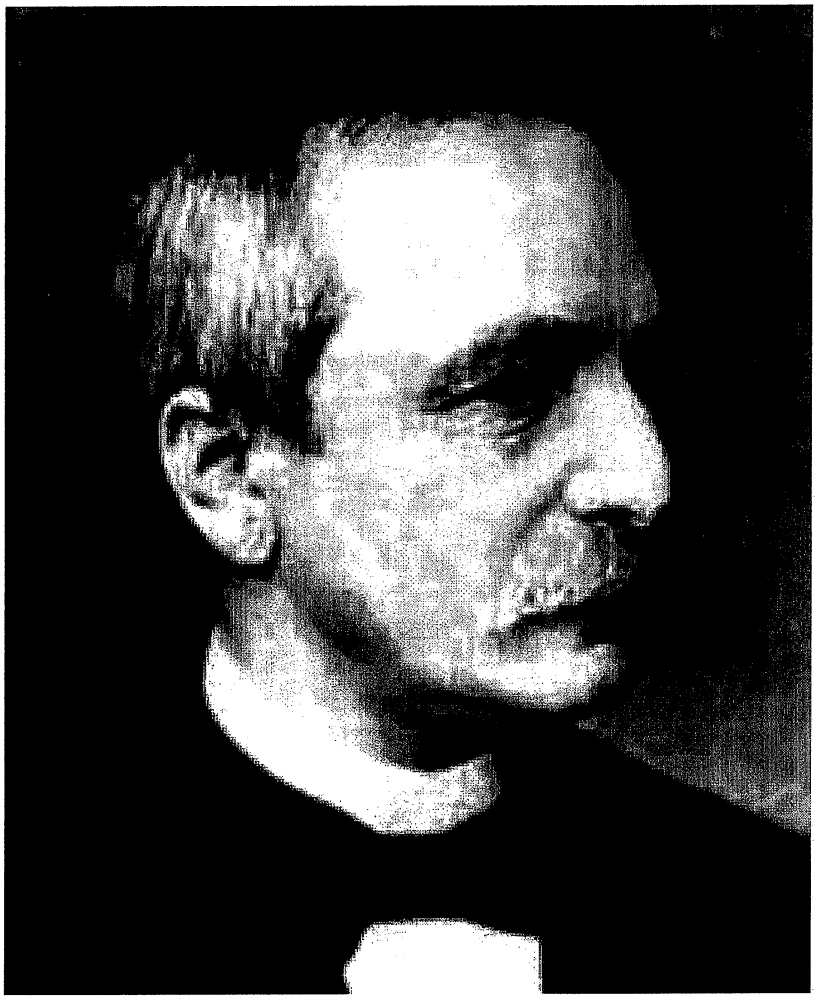
a) Définition *Soit un entier relatif x, l'un des entiers x ou $-x$ est élément de $\mathbb{N}$. Cet entier naturel est appelé valeur absolue de x. Il est noté $|x|$.*

b) Caractérisation de la valeur absolue *Soit un entier relatif x,* $|x| = x$ *si* $x \geq 0$ *et* $|x| = -x$ *si* $x \leq 0$.

c) Propriétés

Soit des entiers relatifs x et y et un entier naturel a :

- $|x| = 0 \Leftrightarrow x = 0$;
- $|x| = |-x|$;
- $|x| = |y| \Leftrightarrow (x = y \text{ ou } x = -y)$;
- $|xy| = |x| \times |y|$;
- $|x + y| \leq |x| + |y|$;
- $a \in \mathbb{N}$, $|x| \leq a \Leftrightarrow -a \leq x \leq a$;
- $a \in \mathbb{N}$, $|x| = a \Leftrightarrow (x = a \text{ ou } x = -a)$.



Kronecker (Leopold) (Liegnitz, auj. Legnica, 1823 - Berlin, 1891), mathématicien allemand.

II. MULTIPLE ET DIVISEUR D'UN ENTIER RELATIF

1- Définition (Multiple et diviseur) *Soit des entiers relatifs a et b , on dit que b est un diviseur de a pour signifier qu'il existe un entier relatif q tel que* $a = bq$. *Dans ce cas, on dit également que b divise a et que a est un multiple de b .*

a) Vocabulaire et notations

- b divise a est noté $b|a$;
- l'ensemble des diviseurs de a est noté $\boldsymbol{Div}(a)$;
- l'ensemble des multiples de b est noté $b\mathbb{Z}$.

b) Exemples

- $\boldsymbol{Div}(0) = \mathbb{Z}$;
- $\boldsymbol{Div}(1) = \{1;-1\}$;
- $\boldsymbol{Div}(12) = \{1;2;3;4;6;12;-1;-2;-3;-4;-6;-12\}$;
- $0\mathbb{Z} = \{0\}$;
- $1\mathbb{Z} = \mathbb{Z}$;
- $2\mathbb{Z} = \{\ldots;-2n;\ldots;-6;-4;-2;0;2;4;6;\ldots;2n;\ldots\}$.

c) Propriétés immédiates *Soit des entiers relatifs x et y,*

- $\boldsymbol{Div}(x) = \boldsymbol{Div}(-x) = \boldsymbol{Div}(|x|)$;
- $a \in \boldsymbol{Div}(x) \Leftrightarrow (-a) \in \boldsymbol{Div}(x)$;
- $1 \in \boldsymbol{Div}(x)$ et $x \in \boldsymbol{Div}(x)$;
- $0 \in x\mathbb{Z}$ et $x \in x\mathbb{Z}$;
- $x\mathbb{Z} = (-x)\mathbb{Z} = |x|\mathbb{Z}$;
- $x|y \Leftrightarrow |x|$ divise $|y|$.

2- Étude de la relation divise dans $\mathbb{Z}$

a) Théorème (Lien entre la relation " divise " et la relation " est inférieur ou égal à") *Soit des entiers relatifs a et b, a non nul,* $b|a \Rightarrow |b| \leq |a|$.

Démonstration

On a vu que $b|a \Leftrightarrow |b|$ divise $|a|$, et nous avons vu dans $\mathbb{N}$ que $|b|$ divise $|a| \Rightarrow |b| \leq |a|$.

b) Théorème *La relation " divise " dans $\mathbb{Z}$ est réflexive et transitive mais n'est pas antisymétrique.*

Démonstration

Les démonstrations concernant la réflexivité et la transitivité sont analogues à celles que l'on a faites dans $\mathbb{N}$.

Cette relation n'est pas antisymétrique car $(a|b$ et $b|a) \Rightarrow (a = b$ ou $a = -b)$.

c) La relation divise et opérations dans $\mathbb{Z}$

Proposition *Soit des entiers relatifs a, b, c, d et un entier naturel n non nul,*

i) $(a|b$ et $a|c) \Rightarrow a|(b+c)$;

ii) $(a|b$ et $a|c) \Rightarrow a|(b-c)$;

iii) $a|b \Rightarrow a|bc$;

iv) $a|b \Rightarrow ac|bc$;

v) $(a|b$ et $c|d) \Rightarrow ac|bd$;

vi) $a|b \Rightarrow a^n|b^n$.

Les démonstrations sont analogues à celles que l'on a faites dans $\mathbb{N}$.

3- Caractérisations ensemblistes de la relation divise dans $\mathbb{Z}$

Théorème *Soit des entiers relatifs a et b non nuls,*

i) $a|b \Leftrightarrow \boldsymbol{Div}(a) \subset \boldsymbol{Div}(b)$;

ii) $a|b \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$.

Démonstration de *i)*

Dans $\mathbb{N}$ *i)* est vraie, or $a|b \Leftrightarrow |a|$ divise $|b|$ et $\boldsymbol{Div}(|a|) = \boldsymbol{Div}(a)$.

Démonstration de *ii)*

Dire " a divise b " équivaut à dire " tout multiple de b est un multiple de a "

Remarque *L'ensemble des diviseurs d'un entier relatif non nul est fini et a un nombre pair d'éléments,* en effet si a divise b alors $-a$ divise b.

Proposition *L'ensemble des multiples d'un entier relatif muni de l'addition est un sous-groupe de* $(\mathbb{Z},+)$ *stable pour la multiplication par un entier relatif quelconque.*

Démonstration

Soit a un entier relatif et $a\mathbb{Z}$ l'ensemble de ses multiples.

Il suffit de démontrer que :

- $a\mathbb{Z} \neq \varnothing$

  Ceci est évident car $a \in a\mathbb{Z}$.
- Soit des éléments b et b' de $a\mathbb{Z}$, on a : $(b-b') \in a\mathbb{Z}$.

  En effet, $b \in a\mathbb{Z}$, donc il existe un entier relatif k tel que $b = ak$,

  $b' \in a\mathbb{Z}$, donc il existe un entier relatif k' tel que $b' = ak'$.

  Donc $b-b' = ak-ak' = a(k-k')$, donc $(b-b') \in a\mathbb{Z}$.
- $(a\mathbb{Z},+)$ est stable pour la multiplication par un entier relatif quelconque.

  Soit un élément b de $a\mathbb{Z}$ et un entier relatif c.

  Il existe un entier relatif k tel que $b = ak$, d'où $bc = (ak)c = a(kc)$, donc $(bc) \in a\mathbb{Z}$.

Archimède (Syracuse, –287., -212).

III- NOMBRES PREMIERS DANS $\mathbb{Z}$

Soit un entier relatif a non nul, $\boldsymbol{Div}(a)$ a au moins deux éléments 1 et -1, de plus $\boldsymbol{Div}(a)$ a un nombre fini et pair d'éléments.

1- Définition *Un entier relatif est premier lorsqu'il admet exactement quatre diviseurs,* 1, -1, *lui-même et son opposé.*

Exemple :

- $\boldsymbol{Div}(0) = \mathbb{Z}$, donc 0 n'est pas premier ;
- $\boldsymbol{Div}(1) = \{1;-1\}$, donc 1 n'est pas premier ;
- $\boldsymbol{Div}(2) = \boldsymbol{Div}(-2) = \{1;-1;2;-2\}$, donc 2 et -2 sont premiers ;
- $\boldsymbol{Div}(3) = \boldsymbol{Div}(-3) = \{1;-1;3;-3\}$, donc 3 et -3 sont premiers ;
- $\boldsymbol{Div}(4) = \boldsymbol{Div}(-4) = \{1;-1;2;-2;4;-4\}$, donc 4 et -4 ne sont pas premiers.

2- Proposition *Un entier relatif x est premier si et seulement si l'entier naturel $|x|$ est premier dans* $\mathbb{N}$.

Corollaire *L'ensemble des entiers relatifs premiers est infini.*

3- Proposition *Tout entier relatif n'appartenant pas à* $\{-1;0;1\}$ *admet une décomposition en produit de facteurs premiers.*

Démonstration

Soit un entier relatif x n'appartenant pas à $\{-1;0;1\}$, $|x|$ est un entier naturel strictement supérieur à 1 et admet donc une décomposition en produit de facteurs premiers.

On a : $|x| = p_1 \times \ldots \times p_r$ avec p_i entier naturel premier pour tout $i \in [\![1,r]\!]$; or $x = |x|$ ou $x = -|x|$,

Donc $x = p_1 \times \ldots \times p_r$ ou $x = -(p_1 \times \ldots \times p_r) = (-p_1) \times \ldots \times p_r$ avec p_1, $-p_1$, p_2, ,…, p_r entiers relatifs premiers.

4- Proposition (" Unicité " de la décomposition en produit de facteurs premiers) *La décomposition en produit de facteurs premiers de tout entier relatif x différent de* -1, 0 *et* 1 *sous la forme* $x = p_1^{\alpha_1} \times \ldots \times p_s^{\alpha_s}$ *ou* $x = (-1) \times p_1^{\alpha_1} \times \ldots \times p_s^{\alpha_s}$ *avec pour tout* $i \in [\![1,s]\!]$, p_i *premier et* α_i *entier naturel non nul est unique (Les* p_i *sont des entiers naturels deux à deux distincts).*

Démonstration

Cette proposition résulte directement de l'unicité de la décomposition en produit de facteurs premiers dans $\mathbb{N}$.

IV- DIVISION EUCLIDIENNE DANS $\mathbb{Z}$

1- Théorème et définition (Division euclidienne) *Pour tout couple d'entiers (a,b), b non nul, il existe un couple d'entiers (q,r) unique tel que $a=bq+r$ avec $0\le r<|b|$.*

Vocabulaire *Les entiers q et r sont respectivement appelés le quotient et le reste de la division euclidienne de a par b.*

Remarque Dans cette définition q est un entier relatif et n est un entier naturel.

Démonstration

a) Existence

Considérons l'ensemble E des multiples de b inférieurs ou égaux à a.

Cet ensemble E n'est pas vide (car $-|ab|\in E$) et est majoré par a.

L'ensemble E admet donc un plus grand élément bq et l'on a $bq\le a<bq+|b|$.

Par conséquent $0\le a-bq<|b|$.

En posant $r=a-bq$, on a un couple (q,r) qui est solution.

b) Unicité

Soit un couple d'entiers relatifs (q',r') tel que $a=bq'+r'$ avec $0\le r'<|b|$.

On a $bq+r=bq'+r'$ et donc $b(q-q')=r'-r$ d'où l'on déduit $|b|\times|q-q'|=|r'-r|$.

On a, $0\le r<|b|$ et $0\le r'<|b|$ donc $0\le|r'-r|<|b|$, or, $r'-r$ est un multiple de b, donc $r'-r=0$.

Par conséquent, $r=r'$ et $q=q'$, d'où l'unicité de la solution.

2-Les sous-groupes additifs de $\mathbb{Z}$

Théorème *Les sous-groupes du groupe additif $(\mathbb{Z},+)$ sont les ensembles $n\mathbb{Z}$ où n est un entier naturel (c'est-à-dire les ensembles des multiples des divers entiers naturels).*

Démonstration

Nous savons que pour tout entier naturel n, $(n\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Z},+)$.

Soit G un sous-groupe de $(\mathbb{Z},+)$.

- Si $G=\{0\}$ alors $G=0\mathbb{Z}$.
- Sinon $G\cap\mathbb{N}^*$ est une partie non vide de $\mathbb{N}$ et admet donc un plus petit élément n non nul. On a $n\mathbb{Z}\subset G$.
  Pour tout élément x de G il existe un couple (q,r) unique tel que $x=qn+r$ avec $0\le r<n$ d'après le théorème précédent. Or x et qn sont des éléments de G, il en résulte $x-qn$ est un élément de $G\cap\mathbb{N}$. A ce titre $r=0$ ou $r\ge n$ puisque n est le plus petit élément de $G\cap\mathbb{N}^*$ et comme $0\le r<n$, on a $r=0$.

On a ainsi montré que $G\subset n\mathbb{Z}$, donc $G=n\mathbb{Z}$.

V. CONGRUENCES

1- Définition *Soit un entier naturel n et des entiers relatifs x et y, on dit que x est congru à y modulo n pour signifier que* $x-y$ *est un multiple de n . S'il en est ainsi, on écrit* $x \equiv y \pmod{n}$. *La relation " est congru à ... modulo n " définie sur* $\mathbb{Z}$ *est appelée congruence modulo n .*

Théorème *Pour tout entier naturel n la relation de congruence modulo n est une relation d'équivalence.*

Démonstration

Réflexivité Pour tout entier relatif x, on a $x-x=n\times 0$, donc $x \equiv x \pmod{n}$.

Symétrie Pour tout couple d'entiers relatifs (x, y),

$x \equiv y \pmod{n} \Leftrightarrow (x-y) \in n\mathbb{Z} \Leftrightarrow (y-x) \in n\mathbb{Z} \Leftrightarrow y \equiv x \pmod{n}$.

Transitivité Pour tout triplet (x, y, z) d'entiers relatifs,

$(x \equiv y \pmod{n}$ et $y \equiv z \pmod{n}) \Rightarrow ((y-x) \in n\mathbb{Z}$ et $(z-y) \in n\mathbb{Z})$.

Comme $(n\mathbb{Z},+)$ est un groupe, $((z-y)+(y-x)) \in n\mathbb{Z}$, donc $(z-x) \in n\mathbb{Z}$, $x \equiv z \pmod{n}$.

Remarques

- deux entiers relatifs quelconques sont congrus modulo 1 ;
- la congruence modulo 0 n'est autre que l'égalité dans $\mathbb{Z}$.

2- Dans tout ce qui suit n désigne un entier naturel non nul.

Proposition (Caractérisation de la congruence modulo *n*) *Soit des entiers relatifs x et y,*

$x \equiv y \pmod{n} \Leftrightarrow$ *x et y ont le même reste dans la division euclidienne par n.*

Démonstration

Il existe un couple (q, r) unique d'entiers relatifs tels que $x = nq + r$ avec $0 \le r < n$.

Il existe un couple (q', r') unique d'entiers relatifs tels que $y = nq' + r'$ avec $0 \le r' < n$.

$x \equiv y \pmod{n} \Leftrightarrow (y-x) \in n\mathbb{Z} \Leftrightarrow (n(q'-q)+(r'-r)) \in n\mathbb{Z} \Leftrightarrow (r'-r) \in n\mathbb{Z}$.

Comme $|r'-r| < n$, on a $r'-r = 0$.

$x \equiv y \pmod{n} \Leftrightarrow r = r'$.

Proposition (Compatibilité de la congruence modulo *n* avec l'addition) *Soit des entiers relatifs x, y et z,*

$x \equiv y \pmod{n} \Leftrightarrow x+z \equiv y+z \pmod{n}$.

Démonstration

$x \equiv y \pmod{n} \Leftrightarrow (y-x) \in n\mathbb{Z} \Leftrightarrow ((y+z)-(x+z)) \in n\mathbb{Z} \Leftrightarrow x+z \equiv y+z \pmod{n}$.

Corollaire *Soit des entiers relatifs x, y, z et t,*

$(x \equiv y \pmod{n}$ et $z \equiv t \pmod{n}) \Rightarrow x+z \equiv y+t \pmod{n}$

Démonstration

$x \equiv y \pmod{n} \Rightarrow x+z \equiv y+z \pmod{n}$ et $z \equiv t \pmod{n}) \Rightarrow y+z \equiv y+t \pmod{n}$

donc $x+z \equiv y+t \pmod{n}$.

Proposition (Compatibilité de la congruence modulo *n* avec la multiplication) *Soit des entiers relatifs x, y et z,*

$x \equiv y \pmod{n} \Rightarrow xz \equiv yz \pmod{n}$.

Démonstration

$x \equiv y \pmod{n} \Rightarrow (y-x) \in n\mathbb{Z} \Rightarrow (z(y-x)) \in n\mathbb{Z} \Rightarrow (zy-zx) \in n\mathbb{Z} \Rightarrow xz \equiv yz \pmod{n}$.

Corollaire *Soit des entiers relatifs x, y, z et t* $(x \equiv y \pmod{n}$ et $z \equiv t \pmod{n}) \Rightarrow xz \equiv yt \pmod{n}$.

Démonstration

$x \equiv y \pmod{n} \Rightarrow xz \equiv yz \pmod{n}$ et $z \equiv t \pmod{n}) \Rightarrow yz \equiv yt \pmod{n}$, donc $xz \equiv yt \pmod{n}$.

Proposition *Soit des entiers relatifs x et y et un entier naturel k non nul,*
$x \equiv y \pmod{n} \Rightarrow x^k \equiv y^k \pmod{n}$.

Démonstration

Cette démonstration se fait aisément par récurrence.

Proposition *Soit des entiers relatifs x et y et un entier naturel p non nul,*
$x \equiv y \pmod{n} \Leftrightarrow px \equiv py \pmod{pn}$.

Démonstration

$x \equiv y \pmod{n} \Leftrightarrow$ il existe un entier k tel que $y - x = kn$.

Comme p est non nul, $y - x = kn \Leftrightarrow p(y-x) = p(kn) \Leftrightarrow py - px = k(pn) \Leftrightarrow px \equiv py \pmod{pn}$.

Proposition *Soit des entiers relatifs x et y et un entier naturel p qui divise n,*
$x \equiv y \pmod{n} \Rightarrow x \equiv y \pmod{p}$.

Démonstration

$x \equiv y \pmod{n} \Leftrightarrow$ il existe un entier k tel que $y - x = kn$.

Comme p est un diviseur de n, il existe un entier naturel λ tel que $n = \lambda p$.

$y - x = kn \Rightarrow y - x = k(\lambda p) \Rightarrow y - x = (k\lambda)p \Rightarrow x \equiv y \pmod{p}$.

3- Exemples

a) • Tout nombre pair est congru à 0 modulo 2.

• Tout nombre impair est congru à 1 modulo 2.

• Il y a trois classes d'équivalence dans la congruence modulo 3 : la classe de 0, celle de 1 et celle de 2.

• Plus généralement pour un entier naturel n non nul la classe d'équivalence d'un entier x pour la congruence modulo n contient un élément unique de $[\![0, n-1]\!]$ qui est le reste de la division euclidienne dans $\mathbb{Z}$ de x par n. Il y a donc n classes d'équivalence pour la congruence modulo n.

b) Calculs avec les congruences

• Si $x \equiv 3 \pmod{4}$ et $y \equiv 2 \pmod{4}$ alors

d'une part $x + y \equiv 5 \pmod{4}$ et donc $x + y \equiv 1 \pmod{4}$;

d'autre part $xy \equiv 6 \pmod{4}$ et donc $xy \equiv 2 \pmod{4}$.

• Soit un entier naturel n, $3^{2n} - 2^n \equiv 0 \pmod{7}$.

En effet $3^{2n} = 9^n$ or $9 \equiv 2 \pmod{7}$ donc $9^n \equiv 2^n \pmod{7}$ et $3^{2n} - 2^n \equiv 0 \pmod{7}$.

• Soit un entier naturel n, $3^{2n+1} + 2^{n+2} \equiv 0 \pmod{7}$.

$$\begin{aligned} 3^{2n+1} + 2^{n+2} &\equiv 3 \times 3^{2n} + 2^2 \times 2^n \pmod{7} \\ &\equiv 3 \times 2^n + 4 \times 2^n \pmod{7} \\ &\equiv (3+4) \times 2^n \pmod{7} \\ &\equiv 7 \times 2^n \pmod{7} \\ &\equiv 0 \pmod{7} \end{aligned}$$

• Vérifier que $10^3 \equiv -1 \pmod{7}$ et en déduire un critère de divisibilité par 7.

Cours de Mathématiques à l'usage des gardes du Pavillon
Par M. Bézout MDCCLXX

Bézout (Étienne) (Nemours, 1730 - Les Basses-Loges, près de Fontainebleau, 1783), mathématicien français: *Théorie générale des équations algébriques (1779).*

Preuve par 9.

76. Suppoſons qu'après avoir multiplié 65498 par 454, & trouvé que le produit eſt 29736092, on veuille éprouver ſi ce produit eſt exact.

On ajoutera tous les chiffres 6,5,4,9,8 du multiplicande, comme s'ils ne contenoient que des unités ſimples, & on retranchera 9, à meſure qu'il ſe trouvera dans la ſomme; on aura un reſte qui ſera ici 5.

On ajoutera pareillement les chiffres 4,5,4, du multiplicateur, & retranchant pareillement tous les 9 que produira cette addition, on aura pour reſte 4.

On multipliera le reſte 5 du multiplicande par le reſte 4 du multiplicateur, & du produit 20, on retranchera les 9 qu'il peut renfermer; il reſtera 2.

Si le produit eſt exact, il faut qu'ajoutant de même tous les chiffres 2, 9, 7, 3, 6, 0, 9, 2 de ce produit, & retranchant

tous les 9, il ne reſte auſſi que 2 ; ce qui a lieu en effet.

Cette regle eſt fondée ſur ce principe, que pour avoir le reſte de la ſouſtraction de tous les 9 qu'un nombre peut renfermer, il n'y a qu'à chercher le reſte que ſes chiffres ajoutés comme des unités ſimples, donneroient après la ſuppreſſion des 9.

En effet, ſi d'un nombre exprimé par un ſeul chiffre ſuivi de pluſieurs zéros, on retranche tous les 9, le reſte ſera exprimé par ce ſeul chiffre, ſi de 4000 ou de 500 ou de 60000 vous retranchez tous les 9, le reſte ſera 4 ou 5 ou 6, &c. ce qui eſt aiſé à voir.

Donc le reſte que donneroit, par la ſuppreſſion des 9, un nombre tel que 65498, (qui eſt la même choſe que 60000, plus 5000, plus 400, plus 90, plus 8), ſera le même que celui que donneroient 6 plus 5, plus 4, plus 9, plus 8 ; c'eſt-à-dire, le même que ſi l'on ajoutoit ſes chiffres comme contenant des unités ſimples.

En voici maintenant l'application à la preuve de la multiplication.

Puiſque 65498 eſt compoſé d'un certain nombre de 9 & d'un reſte 5, & que le multiplicateur 454 eſt compoſé auſſi d'un

certain nombre de 9 & d'un reſte 4, il ne peut s'en falloir que du produit de 5 par 4 ou 20 que le produit total ne ſoit diviſible par 9 ; ou, en ôtant les 9, il ne doit s'en falloir que de 2, que le produit total ne ſoit diviſible par 9 : donc il doit reſter au produit la même quantité que dans le produit des deux reſtes après la ſuppreſſion des 9 qu'il renferme.

On pourroit faire auſſi cette preuve de la même maniere par le nombre 3.

A l'égard de la diviſion, elle devient facile à éprouver, après ce qui a été dit (70). Après avoir ôté du dividende, le reſte qu'a donné la diviſion, on regardera le réſultat comme un produit dont le diviſeur & le quotient ſont les facteurs ; & par conſéquent on y appliquera la preuve par 9, de la même maniere qu'on vient de le faire.

A parler exactement, cette vérification n'eſt pas infaillible, parce que, dans la multiplication, par exemple, ſi l'on s'étoit trompé de quelques unités ſur quelque chiffre du produit, & qu'en même temps, on eût fait une erreur égale, mais en ſens contraire, ſur quelque autre chiffre du même produit ; comme cela ne changeroit rien au reſte que l'on auroit après la ſuppreſſion des 9, cette regle ne feroit point appercevoir l'erreur ; mais comme il faut, ainſi qu'on le voit, au moins deux erreurs, & deux erreurs qui ſe compenſent, ou qui ne diffèrent que d'un certain nombre de fois 9, les cas où cette vérification ſeroit fautive, ſeront très-rares dans l'uſage.

c) Critère de divisibilité par 11 en base dix

Soit un entier naturel N strictement supérieur à 10, dont l'écriture en base dix est $N = \overline{\alpha_n \alpha_{n-1} \ldots \alpha_{2k+1} \alpha_{2k} \ldots \alpha_2 \alpha_1 \alpha_0}$. *On pose* $S_0 = \sum_{0 \le 2k \le n} \alpha_{2k}$ *et* $S_1 = \sum_{0 \le 2k+1 \le n} \alpha_{2k+1}$.

N est divisible par 11 *si et seulement si* $S_0 - S_1$ *est divisible par* 11.

Démonstration

$N = \alpha_n 10^n + \alpha_{n-1} 10^{n-1} + \ldots + \alpha_{2k+1} 10^{2k+1} + \alpha_{2k} 10^{2k} \ldots \alpha_1 10 + \alpha_0$.

Or $10 \equiv -1 \pmod{11}$ et $10^2 \equiv 1 \pmod{11}$,

par conséquent pour tout entier naturel k, $10^{2k+1} \equiv -1 \pmod{11}$ et $10^{2k} \equiv 1 \pmod{11}$.

Donc $N \equiv S_0 - S_1 \pmod{11}$ et ainsi N est divisible par 11 si et seulement si $S_0 - S_1$ est divisible par 11.

On en déduit ainsi un critère de divisibilité par 11.

On a $|S_0 - S_1| \le S_0 + S_1 = \sum_{i=0}^{n} \alpha_i < N$ si $N \ge 10$.

En effet, $N = \sum_{i=0}^{n} \alpha_i 10^i \ge \sum_{i=0}^{n} \alpha_i$ car pour tout i élément de $[\![0, n]\!]$ on a $10^i \ge 1$ (l'égalité n'a lieu que pour $i = 0$).

Ainsi, $|S_0 - S_1| < N$.

- Si $|S_0 - S_1| \le 10$, on peut conclure.
- Si $|S_0 - S_1| > 10$, on itère le procédé.

L'inégalité $|S_0 - S_1| < N$ nous assure que le processus converge.

Minkowski (Hermann) (Aleksotas, près de Kaunas, 1864 - Göttingen, 1909), mathématicien lituanien qui fonda une géométrie des nombres.

VI- DIVISEURS ET MULTIPLES COMMUNS A DEUX ENTIERS RELATIFS

1- Plus grand commun diviseur

Définition *Soit des entiers relatifs a et b, on appelle plus grand commun diviseur de a et b le* $PGCD(|a|,|b|)$ *qui a été défini dans* $\mathbb{N}$. *On le note* $PGCD(a,b)$.

Conséquences

- $PGCD(a,b) = PGCD(-a,b) = PGCD(a,-b) = PGCD(-a,-b)$;
- $PGCD(a,b) = PGCD(b,a)$;
- *Lorsque l'un des entiers a et b est non nul, l'ensemble des diviseurs communs à a et b est majoré par* $PGCD(a,b)$ *(ce qui justifie son appellation) et est minoré par* $-PGCD(a,b)$.

Rappelons que $PGCD(0,0) = 0$ par convention.

Propriétés *Etant donné des entiers relatifs a, b et k,*

- $PGCD(1\ ,\ a) = 1$;
- $PGCD(a\ ,\ a) = |a|$;
- $PGCD(ka\ ,\ kb) = |k|PGCD(a\ ,\ b)$.

Proposition *Soit des entiers relatifs a, b et d' non nuls, " d' est un diviseur commun à a et b " équivaut à " d' est un diviseur de* $PGCD(a,b)$ *", autrement dit* $\mathbf{Div}(a) \cap \mathbf{Div}(b) = \mathbf{Div}(PGCD(a,b))$.

Démonstration

Soit $d = PGCD(a\ ,\ b)$ et un diviseur commun d' de a et b, alors $|d'|$ est un diviseur commun à a et b et comme $|d'|$ est un entier naturel, c'est un diviseur commun à $|a|$ et $|b|$. Par conséquent, $|d'|$ divise d, donc d' divise d.

La réciproque est évidente.

2- Théorème de Bézout

Ce paragraphe peut constituer une présentation du plus grand commun diviseur.

Dans l'ensemble des entiers relatifs, $d'|a \Leftrightarrow a\mathbb{Z} \subset d'\mathbb{Z}$.

Ainsi, d' diviseur commun à a et $b \Leftrightarrow (a\mathbb{Z} \subset d'\mathbb{Z}$ et $b\mathbb{Z} \subset d'\mathbb{Z})$

$$\Leftrightarrow a\mathbb{Z} \cup b\mathbb{Z} \subset d'\mathbb{Z}$$

Ainsi, $(d'\mathbb{Z}\ ,\ +)$ est un sous-groupe de $(\mathbb{Z}\ ,\ +)$ contenant $a\mathbb{Z} \cup b\mathbb{Z}$.

Tout groupe additif contenant $a\mathbb{Z} \cup b\mathbb{Z}$ contient les entiers relatifs de la forme $au + bv$ où u et v sont des entiers relatifs (stabilité pour l'addition et la multiplication par un entier relatif quelconque).

Théorème *Soit* $G = \{x | x \in \mathbb{Z}$ et $\exists (u,v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $x = au + bv\}$, *G est un sous-groupe additif de* $\mathbb{Z}$. *De plus G est le plus petit sous-groupe de* $\mathbb{Z}$ *contenant* $a\mathbb{Z} \cup b\mathbb{Z}$.

Démonstration

- $G \neq \varnothing$, en effet $0 \in G$, $a \in G$ et $b \in G$.
- Soit des éléments x et x' de G, il suffit de démontrer que $(x - x') \in G$.

  On a $x = au + bv$ et $x' = au' + bv'$, donc $x - x' = a(u - u') + b(v - v')$, donc $(x - x') \in G$.

  Par conséquent $(G,+)$ est bien un sous-groupe de $(\mathbb{Z},+)$, c'est le plus petit c'après ce qui précède l'énoncé du théorème.

Théorème *L'ensemble* $G = \{x | x \in \mathbb{Z}$ et $\exists (u,v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $x = au + bv\}$ *est de la forme* $d\mathbb{Z}$, *avec* $d = PGCD(a,b)$.

Démonstration

Comme tout sous-groupe de $(\mathbb{Z},+)$, l'ensemble G est de la forme $d\mathbb{Z}$ avec d entier naturel.

On a $d|a$ car $a\in G$ et $d|b$ car $b\in G$.

Ainsi d est un diviseur commun à a et b, donc d divise $PGCD(a,b)$.

Soit d' un diviseur commun à a et b, d' est un diviseur de tout élément de la forme $au+bv$ avec u et v entiers relatifs, en particulier d' divise d, donc $PGCD(a,b)$ divise d.

En conclusion $d=PGCD(a,b)$, ces deux éléments étant des entiers naturels.

Théorème de Bézout *Soit des entiers relatifs a et b, et, d leur plus grand commun diviseur, il existe des entiers relatifs u et v tels que* $d=au+bv$.

Démonstration C'est une conséquence immédiate de ce qui précède.

3- Entiers relatifs premiers entre eux

Définition *Des entiers relatifs a et b sont dits premiers entre eux lorsque leur plus grand commun diviseur est* 1.

Remarques

- Deux entiers relatifs sont premiers entre eux lorsque leurs seuls diviseurs communs sont 1 et -1.
- Soit des entiers relatifs a et p tels que p soit premier,
  p ne divise pas $a \Leftrightarrow a$ et p premiers entre eux.
- En reprenant les notations du paragraphe précédent,
  a et b premiers entre eux $\Leftrightarrow G=\mathbb{Z}$.

Théorème (Caractérisation de " *a* et *b* sont premiers entre eux ") *Des entiers relatifs a et b sont premiers entre eux, si et seulement si il existe des entiers relatifs u et v tels que* $au+bv=1$.

Démonstration

C'est un cas particulier du théorème de Bézout.

Propriété *Soit des entiers relatifs a et b non tous deux nuls et d un diviseur commun à a et b. Il existe des entiers relatifs a' et b' tels que* $a=da'$ *et* $b=db'$,

$|d|=PGCD(a,b) \Leftrightarrow a'$ *et* b' *sont premiers entre eux.*

4- Théorème de Gauss *Soit des entiers relatifs b et c non nuls. Si a est un entier relatif qui divise bc et qui est premier avec b alors a divise c.*

Première démonstration

Il existe des entiers relatifs u et v tels que $au+bv=1$.

On a alors $c=acu+bcv$, or comme a divise ac et bc, a divise c.

Deuxième démonstration

$PGCD(ac,bc)=|c|PGCD(a,b)=|c|$ car $PGCD(a,b)=1$.

Comme a divise ac et bc, a divise $|c|$, d'où a divise c.

Corollaire *Soit des entiers relatifs a, b et c tels que b et c soient premiers entre eux, si b et c divisent a alors bc divise a.*

Démonstration

Comme $b|a$, il existe q tel que $a=bq$. Or $c|a$ et c est premier avec b, d'après le théorème de Gauss, $c|q$, donc $(bc)|(bq)$, donc $(bc)|a$.

Cas particulier *Tout entier relatif premier qui divise un produit d'entiers relatifs divise au moins l'un d'eux.*

Application Recherche de tous les couples d'entiers relatifs (u, v) tels que $5u+3v=1$ ①

Le couple $(-1\,;2)$ est une solution du problème posé, en effet $5\times(-1)+3\times2=1$. ②

En retranchant membre à membre les égalités ① et ②, on obtient $5(u+1)+3(v-2)=0$, c'est à dire, $5(u+1)=-3(v-2)$. Le nombre 5 divise $-3(v-2)$ et est premier avec -3, donc il divise $v-2$. Par conséquent, il existe un entier relatif k tel que $v-2=5k$. On en déduit $v=5k+2$ et $u=3k-1$.

Réciproquement, pour tout k entier relatif $5(-3k-1)+3(5k+2)=1$. L'ensemble des solutions de ① est donc l'ensemble des couples $(-3k-1\ ,5k+2)$ avec $k\in\mathbb{Z}$.

5- Une conséquence du théorème de Bézout

Théorème *Soit un entier naturel n supérieur ou égal à 2 et des entiers relatifs $a,b_1,b_2,\ldots,b_n$. Si a est premier avec chacun des b_i pour tout i élément de $[\![1,n]\!]$ alors a est premier avec le produit $b_1\times b_2\times\ldots\times b_n$.*

Démonstration

Pour tout élément i de $[\![1,n]\!]$, il existe des entiers relatifs u_i et v_i tels que $au_i+b_iv_i=1$.

Par conséquent $b_iv_i=1-au_i$, donc $\prod_{i=1}^{n}(b_iv_i)=\prod_{i=1}^{n}(1-au_i)$.

L'entier relatif $\prod_{i=1}^{n}(1-au_i)$ peut s'écrire sous la forme $1-au$ avec u entier relatif.

On pose $\prod_{i=1}^{n}v_i=v$, et on obtient $\left(\prod_{i=1}^{n}b_i\right)v=1-au$, donc $au+\left(\prod_{i=1}^{n}b_i\right)v=1$, donc a et $\prod_{i=1}^{n}b_i$ sont premiers entre eux d'après le théorème de Bézout.

Remarque *Soit des entiers relatifs a et p tels que p soit premier et un entier naturel n non nul,*
$p|a^n \Leftrightarrow p|a$.

6- Plus petit commun multiple

Définition *Soit des entiers relatifs a et b, on appelle plus petit commun multiple de a et b le $PPCM(|a|,|b|)$ qui a été défini dans $\mathbb{N}$. On le note $PPCM(a,b)$.*

Conséquences

- $PPCM(a,b)=PPCM(-a,b)=PPCM(a,-b)=PPCM(-a,-b)$;
- $PPCM(a,b)=PPCM(b,a)$;
- *Lorsque l'un des entiers a et b est non nul, l'ensemble des entiers naturels multiples communs à a et b est minoré par $PPCM(a,b)$ (ce qui justifie son appellation).*

Rappelons que $PPCM(0,0)=0$.

Propriétés *Étant donné des entiers relatifs a, b et k,*

- $PPCM(1\ ,a)=|a|$;
- $PPCM(a\ ,a)=|a|$;
- $PPCM(ka\ ,kb)=|k|PPCM(a\ ,b)$.

Proposition *Soit des entiers relatifs a et b non nuls, " m' est un multiple commun à a et b " équivaut à " m' est un multiple de $PPCM(a,b)$ ".*

Démonstration

Soit $m=PPCM(a\ ,b)$ et un multiple commun m' à a et b, alors $|m'|$ est un multiple commun à a et b et comme $|m'|$ est un entier naturel, c'est un multiple commun à $|a|$ et $|b|$. Par conséquent, $|m'|$ est un multiple de $|m|$, en utilisant la propriété analogue à celle-ci que nous avons établie sur les entiers naturels non nuls, on a donc m' est un multiple de m. La réciproque est évidente.

7- Résultat pouvant permettre une autre présentation du plus petit commun multiple

Soit des entiers relatifs a et b, on a

m' est un multiple commun de a et $b \Leftrightarrow (m'\mathbb{Z} \subset a\mathbb{Z}$ et $m'\mathbb{Z} \subset b\mathbb{Z})$

$$\Leftrightarrow m'\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$$

Ainsi $(m'\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Z},+)$ inclus dans $a\mathbb{Z} \cap b\mathbb{Z}$.

Théorème *Soit des entiers relatifs a et b, $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$.*

Démonstration

• $a\mathbb{Z} \cap b\mathbb{Z} \neq \varnothing$ car $0 \in a\mathbb{Z} \cap b\mathbb{Z}$.

• Soit des entiers relatifs x et x' éléments de $a\mathbb{Z} \cap b\mathbb{Z}$.

On a $x \in a\mathbb{Z}$ et $x' \in a\mathbb{Z}$, donc $(x-x') \in a\mathbb{Z}$, de même $x \in b\mathbb{Z}$ et $x' \in b\mathbb{Z}$, donc $(x-x') \in b\mathbb{Z}$.

Ainsi, $(x-x') \in a\mathbb{Z} \cap b\mathbb{Z}$.

Par conséquent $(a\mathbb{Z},+) \cap (b\mathbb{Z},+)$ est un sous-groupe de s $(\mathbb{Z},+)$.

Théorème *L'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est de la forme $m\mathbb{Z}$ avec $m = PPCM(a,b)$.*

Démonstration

Comme tout sous-groupe de $(\mathbb{Z},+)$, l'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est de la forme $m\mathbb{Z}$ avec m entier naturel.

L'entier relatif m est un multiple de a et b donc m est un multiple de $PPCM(a,b)$.

Soit m' un multiple commun à a et b, m' est un élément de $a\mathbb{Z}$ et de $b\mathbb{Z}$, donc de $m\mathbb{Z}$.

En particulier $PPCM(a,b)$ est un multiple de m.

En conclusion $m = PPCM(a,b)$, car ces éléments sont des entiers naturels.

8- Relation entre *PPCM* et *PGCD*

Propriété *Soit des entiers relatifs a et b non nuls,*

a et b sont premiers entre eux $\Leftrightarrow PPCM(a,b) = |ab|$

Démonstration

Soit $m = PPCM(a,b)$ on a $m \leq |ab|$.

Deux cas sont à envisager:

• a et b sont premiers entre eux..

Comme $a|m$ et $b|m$, d'après le théorème de Gauss $(ab)|m$ donc $|ab| \leq m$.

Par conséquent $|ab| = m$, ce qui s'énonce $PPCM(a,b) = |ab|$.

• a et b sont non premiers entre eux..

Soit $d = PGCD(a,b)$ alors $a = a'd$ et $b = b'd$ et $d \times |a'b'|$ est un multiple commun à a et b strictement inférieur à $|ab|$.

Théorème (Relation entre *PPCM* et *PGCD*) *Soit des entiers relatifs a et b non nuls, on a* $PPCM(a,b) \times PGCD(a,b) = |ab|$.

Démonstration

On pose $d = PGCD(a,b)$.

On peut écrire $a = da'$ et $b = db'$, avec a' et b' entiers relatifs premiers entre eux.

On a $PGCD(a',b') = 1$ et $PPCM(a',b') = |a'b'|$.

De plus $PPCM(a,b) = PPCM(da',db') = d \times PPCM(a',b') = d \times |a'b'|$.

Ainsi $PPCM(a,b) \times PGCD(a,b) = d^2 \times |a'b'| = |da'db'| = |ab|$.

Partie C - COMPLÉMENTS

I. ETUDE DE L'ENSEMBLE $\mathbb{Z}/n\mathbb{Z}$

L'étude de cet ensemble est en dehors du programme de la terminale scientifique.

Dans ce paragraphe n désigne un entier naturel supérieur ou égal à 2.

1- L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Définition *On désigne par $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour la congruence modulo n.*

Notation Soit n un entier relatif, on convient de noter $\dot{x}$ la classe de n. Chaque élément de $\mathbb{Z}/n\mathbb{Z}$ contient un élément unique de $[\![0, n-1]\!]$. vérifiant $0 \leq x \leq n-1$.

Ainsi $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}\,;\dot{1}\,;\dot{2}\}$.

2- Addition et multiplication dans $\mathbb{Z}/n\mathbb{Z}$

Définitions *Soit des éléments $\dot{x}$ et $\dot{y}$ de $\mathbb{Z}/n\mathbb{Z}$, un entier relatif z élément de $\dot{x}$ et un entier relatif t élément de $\dot{y}$, on a $z + t \equiv x + y \pmod{n}$, c'est-à-dire $\dot{\overline{z+t}} = \dot{\overline{x+y}}$.*

Ceci justifie la notation $\dot{x} + \dot{y} = \dot{\overline{x+y}}$.

De la même manière, on définit une multiplication dans $\mathbb{Z}/n\mathbb{Z}$ de la façon suivante : $\dot{x} \times \dot{y} = \dot{\overline{xy}}$.

Exemple Tables d'addition et de multiplication de $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.

+	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$

×	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{1}$	$\dot{3}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{1}$	$\dot{4}$	$\dot{2}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

+	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{5}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$

×	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{0}$	$\dot{2}$	$\dot{4}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{2}$	$\dot{0}$	$\dot{4}$	$\dot{2}$
$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

Propriétés

- $(\mathbb{Z}/n\mathbb{Z},+)$ *est un groupe commutatif.*
- *La multiplication dans* $\mathbb{Z}/n\mathbb{Z}$ *est associative, commutative et admet* $\dot{1}$ *pour élément neutre.*
- *La multiplication dans* $\mathbb{Z}/n\mathbb{Z}$ *est distributive par rapport à l'addition.*

Démonstration

Ces propriétés découlent des résultats démontrés sur les congruences.

Remarques

- Soit $\dot{a}$ et $\dot{b}$ des éléments de $\mathbb{Z}/n\mathbb{Z}$, l'équation $\dot{x}+\dot{a}=\dot{b}$ d'inconnue $\dot{x}$ admet une solution unique $\dot{x}=\dot{b}+\dot{-a}$.

  Notation : $\dot{-a}$ est l'opposé de $\dot{a}$ dans $\mathbb{Z}/n\mathbb{Z}$, on note $-\dot{a}$ l'élément $\dot{-a}$ et $\dot{b}-\dot{a}$ l'élément $\dot{b}+\dot{-a}$.

- Soit un élément $\dot{a}$ de $\mathbb{Z}/n\mathbb{Z}$ différent de $\dot{0}$.

Dans $\mathbb{Z}/5\mathbb{Z}$.	L'équation $\dot{a}\dot{x}=\dot{0}$ admet une unique solution $\dot{x}=\dot{0}$.	L'équation $\dot{a}\dot{x}=\dot{1}$ admet une unique solution. Par exemple $\dot{2}\dot{x}=\dot{1}$ admet comme unique solution $\dot{x}=\dot{3}$.
Dans $\mathbb{Z}/6\mathbb{Z}$.	L'équation $\dot{3}\dot{x}=\dot{0}$ a comme solutions $\dot{x}=\dot{0}$, $\dot{x}=\dot{2}$ et $\dot{x}=\dot{4}$.	L'équation $\dot{3}\dot{x}=\dot{1}$ n'a pas de solution. (Voir table de multiplication)

3- Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

Problème

Soit des éléments $\dot{a}$ et $\dot{b}$ de $\mathbb{Z}/n\mathbb{Z}$ avec $\dot{a}\neq\dot{0}$.

On cherche à résoudre l'équation $\dot{a}\dot{x}=\dot{b}$ d'inconnue $\dot{x}$.

➢ Si l'équation $\dot{a}\dot{x}=\dot{1}$ admet une solution notée $\dot{a}'$ alors l'équation $\dot{a}\dot{x}=\dot{b}$ admet une unique solution $\dot{x}=\dot{a}'\dot{b}$.

➢ Ceci nous conduit à nous intéresser à l'étude de l'équation $\dot{a}\dot{x}=\dot{1}$.

Théorème - Définition *L'équation* $\dot{a}\dot{x}=\dot{1}$ *admet au plus une solution. Lorsqu'elle admet une solution celle-ci est appelée inverse de* $\dot{a}$ *et on dit que* $\dot{a}$ *est inversible dans* $\mathbb{Z}/n\mathbb{Z}$.

Démonstration

Soit $\dot{a}_1$ et $\dot{a}_2$ des solutions de l'équation $\dot{a}\dot{x}=\dot{1}$, on a $\dot{a}_1\dot{a}=\dot{1}$ et $\dot{a}\dot{a}_2=\dot{1}$.

Ainsi, $\dot{a}_1\dot{a}\dot{a}_2=(\dot{a}_1\dot{a})\dot{a}_2=\dot{a}_2$ et $\dot{a}_1\dot{a}\dot{a}_2=\dot{a}_1(\dot{a}\dot{a}_2)=\dot{a}_1$, ce qui prouve que l'équation $\dot{a}\dot{x}=\dot{1}$ a au plus une solution.

Théorème *Soit un entier relatif a et un entier naturel n supérieur ou égal à* 2.

$\dot{a}$ *est inversible dans* $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow$ *a est premier avec n.*

Démonstration

$\dot{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ $\Leftrightarrow$ il existe un entier relatif b tel que $\dot{a}\dot{b} = \dot{1}$.

$\Leftrightarrow$ il existe un entier relatif b tel que $(ab-1) \in n\mathbb{Z}$.

$\Leftrightarrow$ il existe des entiers relatifs b et c tels que $ab - 1 = cn$.

$\Leftrightarrow$ il existe des entiers relatifs b et c tels que $ab - cn = 1$.

$\Leftrightarrow$ a est premier avec n. (Théorème de Bézout)

Exemples

- Dans $\mathbb{Z}/5\mathbb{Z}$ tout élément non nul est inversible, car 5 est premier.
- Dans $\mathbb{Z}/6\mathbb{Z}$ seuls $\dot{1}$ et $\dot{5}$ sont inversibles.

Théorème *Tout élément non nul de* $\mathbb{Z}/n\mathbb{Z}$ *est inversible si et seulement si n est premier.*

Démonstration

Elle découle directement du théorème précédent.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obſervationibus D. P. de FERMAT Senatoris Tolosani.
Acceſſit Doctrinæ Analyticæ inventum novum, collectum
ex variis ejuſdem D. de FERMAT Epiſtolis.
TOLOSÆ,
M. DC. LXX.

Diophante (v. 325 - v. 410), mathématicien grec de l'école d'Alexandrie.

II. ETUDE DE L'EQUATION $ax+by=c$

Problème

Soit des entiers relatifs a, b et c, résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $ax+by=c$ où (x,y) est l'inconnue.

Remarque Nous avons déjà résolu précédemment une équation de ce type : $5u+3v=1$.
Soit $d=PGCD(a,b)$.

- Existence de solutions
  - ➢ Condition nécessaire

    Il existe des entiers relatifs a' et b' tels que $a=a'd$ et $b=b'd$ (a' et b' premiers entre eux).
    Pour tous entiers relatifs x et y, $d|(ax+by)$, d'où $d|c$ est une condition nécessaire.

  - ➢ Condition suffisante

    Si $d|c$, il existe des entiers relatifs a', b' et c' tels que $a=a'd$, $b=b'd$ et $c=c'd$.

    On a a' et b' premiers entre eux, donc il existe des entiers relatifs u et v tels que $a'u+b'v=1$, donc en multipliant chaque membre par $c'd$ on obtient $(a'd)(uc')+(b'd)(vc')=c'd$, soit $a(uc')+b(vc')=c$.

    Ainsi le couple (uc', vc') est une solution de notre problème.

En résumé *Une condition nécessaire et suffisante pour que l'équation $ax+by=c$ admette une solution est que $PGCD(a,b)$ divise c.*

- **Résolution**

  Les notations précédentes étant conservées, plaçons nous dans le cas où l'équation $ax+by=c$ admet une solution (x_0,y_0), c'est-à-dire $ax_0+by_0=c$.

$$\begin{aligned} ax+by=c &\Leftrightarrow a(x-x_0)+b(y-y_0)=0 \\ &\Leftrightarrow a(x-x_0)=(-b)(y-y_0) \\ &\Leftrightarrow a'd(x-x_0)=(-b'd)(y-y_0) \\ &\Leftrightarrow a'(x-x_0)=(-b')(y-y_0) \end{aligned}$$

  Comme a' et b' sont premiers entre eux, d'après le théorème de Gauss, b' divise $(x-x_0)$.

  Ainsi il existe un entier relatif k tel que $x-x_0=kb'$, donc $x=x_0+kb'$.

  Ainsi $a'kb'=(-b')(y-y_0)$, donc $ka'=-(y-y_0)$, soit $y=y_0-ka'$.

  Réciproquement, on vérifie que pour tout entier relatif k le couple (x_0+kb', y_0-ka') est solution de l'équation $ax+by=c$.

En conclusion *L'ensemble des solutions dans $\mathbb{Z}\times\mathbb{Z}$ de l'équation $ax+by=c$ est l'ensemble des couples (x_0+kb', y_0-ka') où k décrit $\mathbb{Z}$, avec (x_0,y_0) une solution de l'équation et a' et b' les quotients de a et b par $PGCD(a,b)$.*

1er exemple

Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $10x+6y=2$.

- On a $PGCD(10,6)=2$ donc nous sommes ramenés à résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $5x+3y=1$.

  Nous avons résolu cette équation. Ses solutions sont les couples $(-1-3k, 2+5k)$ où k décrit $\mathbb{Z}$.

- Autres méthodes de résolution.
  - ➢ Utilisation des congruences modulo 6.

    L'équation donnée conduit à étudier $\dot{10}\dot{x}+\dot{6}\dot{y}=\dot{2}$ dans $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.

$10x+6y=2 \Rightarrow \dot{10}\dot{x}+\dot{6}\dot{y}=\dot{2}$

$\Rightarrow \dot{10}\dot{x}=\dot{2}$

$\Rightarrow \dot{4}\dot{x}=\dot{2}$

$\Rightarrow \dot{x}=\dot{5}$ ou $\dot{x}=\dot{2}$

$\Rightarrow x=5+6k_1$ ou $x=2+6k_1$ avec $k_1 \in \mathbb{Z}$

$\Rightarrow x=2+3k_2$ avec $k_2 \in \mathbb{Z}$

En reportant cette expression de x dans l'équation donnée on obtient $y=-3+5k_2$ avec $k_2 \in \mathbb{Z}$.

Réciproquement, on vérifie que pour tout entier relatif k_2 le couple $(2+3k_2,-3-5k_2)$ est solution de l'équation $10x+6y=2$.

En remplaçant k_2 par $k-1$, on retrouve l'expression précédente des solutions.

➢ Utilisation des congruences modulo 10.

L'équation donnée conduit à étudier $\dot{10}\dot{x}+\dot{6}\dot{y}=\dot{2}$ dans $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

$10x+6y=2 \Rightarrow \dot{10}\dot{x}+\dot{6}\dot{y}=\dot{2}$

$\Rightarrow \dot{6}\dot{y}=\dot{2}$

$\Rightarrow \dot{y}=\dot{2}$ ou $\dot{y}=\dot{7}$

$\Rightarrow y=2+10k_1$ ou $y=7+10k_1$ avec $k_1 \in \mathbb{Z}$

$\Rightarrow y=2+5k$ avec $k \in \mathbb{Z}$

En reportant cette expression de x dans l'équation donnée on obtient $x=-1-3k$ avec $k \in \mathbb{Z}$.

Réciproquement, on vérifie que pour tout entier relatif k le couple $(-1+3k,2-5k)$ est solution de l'équation $10x+6y=2$.

2ème exemple

Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ $165x+267y=c$ où c désigne un entier relatif.

On a $PGCD(165,267)=3$ donc si 3 ne divise pas c l'équation n'a pas de solution.

Si 3 divise c, l'équation admet une infinité de solutions.

Prenons par exemple $c=9$, on est amené à résoudre $55x+89y=3$

Résolvons dans $\mathbb{Z}/55\mathbb{Z} \times \mathbb{Z}/55\mathbb{Z}$, $\dot{55}\dot{x}+\dot{89}\dot{y}=\dot{3}$.

Nous avons alors à résoudre $\dot{89}\dot{y}=\dot{3}$, soit encore $\dot{34}\dot{y}=\dot{3}$.

L'équation $\dot{34}\dot{y}=\dot{3}$ admet une solution unique dans $\mathbb{Z}/55\mathbb{Z}$ car $\dot{34}$ est inversible (34 est premier avec 55).

On peut rechercher cette solution dans la table de multiplication de $\dot{34}$ dans $\mathbb{Z}/55\mathbb{Z}$ (on trouve $\dot{y}=\dot{47}$), ou encore, rechercher dans la même table l'inverse de $\dot{34}$ (on trouve alors $\dot{34}\times\dot{34}=\dot{1}$, donc $\dot{y}=\dot{3}\times\dot{34}=\dot{47}$), …

Comme précédemment on en déduit l'ensemble des solutions $(-76-89k,47+55k)$ où k décrit $\mathbb{Z}$.

III- PLUS GRAND COMMUN DIVISEUR ET PLUS PETIT COMMUN MULTIPLE DE PLUSIEURS ENTIERS

Les définitions du *PGCD* et du *PPCM* de deux entiers naturels et de deux entiers relatifs énoncées précédemment s'étendent à plusieurs entiers naturels et à plusieurs entiers relatifs.
Nous présentons ici une généralisation de ces définitions.

1- Plus grand commun diviseur de plusieurs entiers

Théorème - Définition (Plus Grand Commun Diviseur de plusieurs entiers naturels) *Soit un entier naturel n supérieur ou égal à 2 et des entiers naturels* $a_1, a_2, \ldots, a_n$ *non tous nuls. L'ensemble* $\bigcap_{i=1}^{n} \mathbf{Div}(a_i)$ *admet un plus grand élément (pour l'ordre naturel dans* $\mathbb{N}$*). Cet élément est appelé plus grand commun diviseur des entiers naturels* $a_1, a_2, \ldots, a_n$*. On le note* $PGCD(a_1, a_2, \ldots, a_n)$.

Définition (Plus Grand Commun Diviseur de plusieurs entiers relatifs) *On appelle plus grand commun diviseur des entiers relatifs* $a_1, a_2, \ldots, a_n$ *le* $PGCD(|a_1|, |a_2|, \ldots, |a_n|)$. *On le note* $PGCD(a_1, a_2, \ldots, a_n)$.

Proposition *Soit des entiers relatifs* $a_1, a_2, \ldots, a_n$ *non tous nuls,* $\bigcap_{i=1}^{n} \mathbf{Div}(a_i) = \mathbf{Div}(PGCD(a_1, a_2, \ldots, a_n))$

Remarques

- Le procédé qui permet d'obtenir le plus grand commun diviseur de deux entiers naturels non nuls à partir de leurs décompositions en produit de facteurs premiers s'applique de la même manière pour calculer le plus grand commun diviseur d'un nombre fini d'entiers naturels non tous nuls.
- Le théorème de Bézout s'étend à un nombre fini d'entiers relatifs. C'est-à-dire :
  Soit un entier naturel n supérieur ou égal à 2, des entiers relatifs $a_1, a_2, \ldots, a_n$ *non tous nuls et* $d = PGCD(a_1, a_2, \ldots, a_n)$.
  Il existe des entiers relatifs $u_1, u_2, \ldots, u_n$ *tels que* $a_1u_1 + a_2u_2 + \ldots + a_nu_n = d$.
- Par convention $PGCD(0,0,\ldots,0) = 0$.

2- Plus petit commun multiple de plusieurs entiers

Théorème - Définition (Plus Petit Commun Multiple de plusieurs entiers naturels) *Soit un entier naturel n supérieur ou égal à 2 et des entiers naturels* $a_1, a_2, \ldots, a_n$ *non tous nuls. L'ensemble* $\bigcap_{i=1}^{n} (a_i\mathbb{N})$ *admet un plus petit élément non nul (pour l'ordre naturel dans* $\mathbb{N}$*). Cet élément est appelé plus petit commun multiple des entiers naturels* $a_1, a_2, \ldots, a_n$*. On le note* $PPCM(a_1, a_2, \ldots, a_n)$.

Définition (Plus Petit Commun Multiple de plusieurs entiers relatifs) *On appelle plus petit commun multiple des entiers relatifs* $a_1, a_2, \ldots, a_n$ *le* $PPCM(|a_1|, |a_2|, \ldots, |a_n|)$. *On le note* $PPCM(a_1, a_2, \ldots, a_n)$.

Proposition *Soit des entiers relatifs* $a_1, a_2, \ldots, a_n$ *non tous nuls,* $\bigcap_{i=1}^{n} (a_i\mathbb{Z}) = (PPCM(a_1, a_2, \ldots, a_n))\mathbb{Z}$.

Remarques

- Le procédé qui permet d'obtenir le plus petit commun multiple de deux entiers naturels non nuls à partir de leurs décompositions en produit de facteurs premiers s'applique de la même manière pour calculer le plus petit commun multiple d'un nombre fini d'entiers naturels non tous nuls.
- Lorsque l'un des a_i est nul, $PPCM(a_1, a_2, \ldots, a_n) = 0$.

3- Lois de composition interne définies à partir du PGCD et du PPCM

• A tout couple d'entiers relatifs $(a\,,\,b)$ nous savons associer l'entier relatif $PGCD(a\,,\,b)$ que nous noterons $a \wedge b$ dans ce paragraphe.

$\mathbb{Z}\times\mathbb{Z} \rightarrow \mathbb{Z}$

$(a\,,\,b) \mapsto a \wedge b$ est une loi de composition interne dans $\mathbb{Z}$.

Les propriétés établies dans les chapitres précédents nous permettent d'écrire :

$a \wedge b = b \wedge a$ (commutativité de la loi $\wedge$).

$a \wedge 0 = |a|$

$a \wedge 1 = 1$

$a \wedge a = a \wedge (-a) = |a|$

Proposition *Quels que soient les entiers relatifs a, b et c,*
$PGCD(a\,,b\,,c) = PGCD(PGCD(a\,,b)\,,c) = PGCD(a\,,PGCD(b\,,c))$.

Démonstration

Cela résulte de l'associativité de l'intersection.

Remarque (Associativité du plus grand commun diviseur) Quels que soient les entiers relatifs a, b et c, $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, ce qui justifie la notation, $a \wedge b \wedge c$.

Exemple Soit à calculer $72 \wedge 540 \wedge 120$.

On peut procéder de deux manières :

$(72 \wedge 540) \wedge 120 = 36 \wedge 120 = 12$

$72 \wedge (540 \wedge 120) = 72 \wedge 60 = 12$

• A tout couple d'entiers relatifs $(a\,,\,b)$ nous savons associer l'entier relatif $PPCM(a\,,b)$ que nous noterons $a \vee b$ dans ce paragraphe.

$\mathbb{Z}\times\mathbb{Z} \rightarrow \mathbb{Z}$

$(a\,,\,b) \mapsto a \vee b$ est une loi de composition interne dans $\mathbb{Z}$.

Les propriétés établies dans les chapitres précédents nous permettent d'écrire :

$a \vee b = b \vee a$ (commutativité de la loi $\vee$).

$a \vee 0 = 0$

$a \vee 1 = |a|$

$a \vee a = a \vee (-a) = |a|$

Proposition *Quels que soient les entiers relatifs a, b et c,*
$PPCM(a\,,b,c) = PPCM(PPCM(a\,,b)\,,c) = PPCM(a\,,PPCM(b\,,c))$.

Démonstration

Cela résulte de l'associativité de l'intersection.

Remarque (Associativité du plus petit commun multiple) Quels que soient les entiers relatifs a, b et c, $(a \vee b) \vee c = a \vee (b \vee c)$, ce qui justifie la notation, $a \vee b \vee c$.

Exemple Soit à calculer $18 \vee 60 \vee 21$.

On peut procéder de deux manières :

$(18 \vee 60) \vee 21 = 180 \vee 21 = 1260$

$18 \vee (60 \vee 21) = 18 \vee 420 = 1260$

Proposition (Distributivités du plus grand commun diviseur et plus petit commun multiple dans $\mathbb{Z}$)

Quels que soient les entiers relatifs a, b et c non nuls,

$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ *et* $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Démonstration

Quatre cas sont à envisager.

➢ L'un des entiers est nul.

☞ $a = 0$

$0 \wedge (b \vee c) = b \vee c$ $\qquad$ $0 \vee (b \wedge c) = 0$

$(0 \wedge b) \vee (0 \wedge c) = |b| \vee |c| = b \vee c$ $\qquad$ $(0 \vee b) \wedge (0 \vee c) = 0 \wedge 0 = 0$

☞ $b = 0$ (ou $c = 0$, b et c jouant des rôles symétriques).

$a \wedge (0 \vee c) = a \wedge 0 = |a|$ $\qquad$ $a \vee (0 \wedge c) = a \wedge |c| = a \wedge c$

$(a \wedge 0) \vee (a \wedge c) = |a| \vee (a \wedge c) = |a|$ $\qquad$ $(a \vee 0) \wedge (a \vee c) = 0 \wedge (a \vee c) = a \wedge c$

➢ $|a| = 1$

$1 \wedge (b \vee c) = 1$ $\qquad$ $(1 \wedge b) \vee (1 \wedge c) = 1 \vee 1 = 1$

➢ $|b| = 1$ (ou $|c| = 1$, b et c jouent des rôles symétriques).

$a \wedge (b \vee c) = a \wedge |c| = a \wedge c$ $\qquad$ $(a \wedge b) \vee (a \wedge c) = 1 \vee (a \wedge c) = a \wedge c$

➢ Les entiers relatifs a, b et c sont de valeurs absolues strictement supérieures à 1.

On considère la liste non répétitive $p_1, p_2, \ldots, p_r$ de tous les facteurs premiers figurant dans l'une ou l'autre des décompositions de $|a|$, $|b|$ et $|c|$. On peut écrire $|a| = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, $|b| = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$ et $|c| = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_r^{\gamma_r}$ où pour chaque entier naturel i élément de $[\![1, r]\!]$ les exposants α_i, β_i et γ_i sont des entiers naturels pouvant éventuellement être nuls.

On a alors $a \wedge (b \vee c) = p_1^{u_1} p_2^{u_2} \ldots p_r^{u_r}$ et $(a \wedge b) \vee (a \wedge c) = p_1^{v_1} p_2^{v_2} \ldots p_r^{v_r}$ avec pour tout i élément de $[\![1, r]\!]$, $u_i = \min(\alpha_i, \max(\beta_i, \gamma_i))$ et $v_i = \max(\min(\alpha_i, \beta_i), \min(\alpha_i, \gamma_i))$ et six cas peuvent se présenter et sont répertoriés dans le tableau ci-dessous :

	$\alpha_i \le \beta_i \le \gamma_i$	$\alpha_i \le \gamma_i \le \beta_i$	$\beta_i \le \alpha_i \le \gamma_i$	$\gamma_i \le \alpha_i \le \beta_i$	$\beta_i \le \gamma_i \le \alpha_i$	$\gamma_i \le \beta_i \le \alpha_i$
u_i	α_i	α_i	α_i	α_i	γ_i	β_i
v_i	α_i	α_i	α_i	α_i	γ_i	β_i

On a donc, pour tout i élément de $[\![1, r]\!]$, $u_i = v_i$, et par conséquent, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

On démontre de la même manière que $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

IV- PETIT THÉORÈME DE FERMAT – THÉORÈME DE WILSON

Petit théorème de Fermat *Soit un entier naturel p premier et un entier naturel a premier avec p,* $a^{p-1} \equiv 1 \pmod{p}$.

Démonstration

Considérons l'ensemble des entiers naturels $E = \{a, 2a, \ldots, ka, \ldots, (p-1)a\}$.

Les restes de la division par p de deux éléments distincts de E sont distincts. En effet, $a(k-k') \equiv 0 \pmod{p}$ entraîne $k = k'$ car a et p sont premiers entre eux.

Ainsi l'ensemble des restes obtenus est $[\![1, p-1]\!]$.

On en déduit que $1 \times 2a \times \ldots \times ka \times \ldots \times (p-1)a \equiv 1 \times 2 \times \ldots \times k \times \ldots \times (p-1) \pmod{p}$,

donc $a^{p-1} \times (p-1)! \equiv (p-1)! \pmod{p}$.

L'entier naturel p étant premier, les entiers $(p-1)!$ et p sont premiers entre eux, donc $a^{p-1} \equiv 1 \pmod{p}$.

Corollaire *Soit un entier naturel p premier, pour tout entier naturel a,* $a^p \equiv a \pmod{p}$.

Démonstration

Si a est premier avec p, c'est le théorème précédent.

Sinon p divise a donc $a^p \equiv a \equiv 0 \pmod{p}$.

Théorème de Wilson *Soit un entier naturel p supérieur ou égal à 2,*
p est premier si et seulement si $(p-1)! + 1 \equiv 0 \pmod{p}$.

Démonstration

Ce résultat est trivial pour $p = 2$ et $p = 3$.

- Soit p un nombre premier strictement supérieur à 3.
  Pour tout entier naturel a premier avec p, il existe un entier b tel que $ab \equiv 1 \pmod{p}$. (cf Partie **C-I**-3)
  Considérons l'ensemble $[\![1, p-1]\!]$, pour tout $a \in [\![1, p-1]\!]$, il existe $b \in [\![1, p-1]\!]$ tel que $ab \equiv 1 \pmod{p}$.
  On note $b = a^{-1}$.
  De plus, $a = a^{-1} \Leftrightarrow (a = 1$ ou $a = p-1)$.
  En effet, $a = a^{-1} \Leftrightarrow a^2 \equiv 1 \pmod{p} \Leftrightarrow p \mid (a-1)(a+1) \Leftrightarrow (a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p})$.
  Si $a \in [\![2, p-2]\!]$ alors $a^{-1} \in [\![2, p-2]\!]$ et $a \neq a^{-1}$; ainsi en regroupant chaque élément de $[\![2, p-2]\!]$ avec son inverse, $2 \times \ldots \times k \times \ldots \times (p-2) \equiv 1 \pmod{p}$,
  donc $1 \times 2 \times \ldots \times k \times \ldots \times (p-2) \times (p-1) \equiv 1 \times (p-1) \pmod{p}$, ainsi $(p-1)! \equiv -1 \pmod{p}$.
- Soit p un entier naturel strictement supérieur à 3 tel que $(p-1)! + 1 \equiv 0 \pmod{p}$.
  Tout entier naturel n de l'ensemble $[\![2, p-1]\!]$ divise $(p-1)!$; si de plus n divise p alors n divise 1, ce qui est absurde.
  Par conséquent p est premier.

V- ÉTUDE DE QUELQUES FONCTIONS ARITHMÉTIQUES

Dans tout ce paragraphe les entiers considérés sont des entiers naturels

1- Nombre de diviseurs d'un entier naturel *n* non nul

Notation *Soit un entier naturel n non nul, on note* $\mathrm{d}(n)$ *le nombre de diviseurs de n.*

Remarque $\mathrm{d}(1)=1$

Propriété *Soit un entier naturel n strictement supérieur à* 1, *on note* $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$ *sa décomposition en produit de facteurs premiers. On a* $\mathrm{d}(n)=\prod_{i=1}^{n}(1+\alpha_i)$.

Démonstration

Soit un entier naturel *m*,

$m|n$ si et seulement si il existe des entiers naturels $\beta_1, \beta_2,\dots,\beta_r$ avec pour tout *i* élément de $[\![1,r]\!]$, $0\le\beta_i\le\alpha_i$ tels que $m=p_1^{\beta_1}p_2^{\beta_2}\dots p_r^{\beta_r}$.

Chaque β_i peut prendre $1+\alpha_i$ valeurs, d'où $\mathrm{d}(n)=\prod_{i=1}^{n}(1+\alpha_i)$.

Remarques

- $\mathrm{d}(n)$ impair $\Leftrightarrow$ *n* est le carré d'un entier.
- $\mathrm{d}(n)=2 \Leftrightarrow$ *n* est premier.

Exemple

$\mathrm{d}(150)=\mathrm{d}(2^1\times3^1\times5^2)=(1+1)\times(1+1)\times(2+1)=12$.

2- Somme des diviseurs d'un entier naturel *n* non nul

Notation *Soit un entier naturel n non nul, on note* $\mathrm{s}(n)$ *la somme des diviseurs de n.*

Propriété *Soit un entier naturel n ,*

n premier $\Leftrightarrow \mathrm{s}(n)=n+1$

Propriété *Soit un entier naturel p premier et un entier naturel* α *non nul. On a* $\mathrm{s}(p^\alpha)=1+p+\dots+p^\alpha$.

Propriété *Soit des entiers naturel m et n premiers entre eux. On a* $\mathrm{s}(mn)=\mathrm{s}(m)\mathrm{s}(n)$.

Démonstration

Elle repose sur le fait que tout diviseur *d* de *mn* s'écrit de façon unique sous la forme $d=d_1d_2$ avec $d_1|m$ et $d_2|n$.

En effet, notons $m=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$ et $n=q_1^{\beta_1}q_2^{\beta_2}\dots q_s^{\beta_s}$ les décompositions en produits de facteurs premiers de *m* et *n* avec $p_i\neq q_j$ pour tout *i* élément de $[\![1,r]\!]$ et tout *j* élément de $[\![1,s]\!]$.

L'unicité en produit de facteurs premiers de *mn*, nous assure que la décomposition en produit de facteurs premiers de *mn* est $mn=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}q_1^{\beta_1}q_2^{\beta_2}\dots q_s^{\beta_s}$.

Ainsi tout diviseur de *mn* s'écrit de façon unique $d=(p_1^{\alpha'_1}p_2^{\alpha'_2}\dots p_r^{\alpha'_r})(q_1^{\beta'_1}q_2^{\beta'_2}\dots q_s^{\beta'_s})$ avec $0\le\alpha'_i\le\alpha_i$ pour tout *i* élément de $[\![1,r]\!]$ et $0\le\beta'_j\le\beta_j$ pour tout *j* élément de $[\![1,s]\!]$.

D'une part, $\mathrm{s}(m)=\sum_{a|m}a$ et $s(n)=\sum_{b|n}b$, donc $\mathrm{s}(m)\mathrm{s}(n)=\left(\sum_{a|m}a\right)\left(\sum_{b|n}b\right)=\sum_{\substack{a|m\\b|n}}ab$.

D'autre part, $\mathrm{s}(mn)=\sum_{c|(mn)}c$.

➢ Quels que soient les entiers naturels *a* et *b* tels que $a|m$ et $b|n$, comme *m* et *n* sont premiers entre eux $(ab)|(mn)$.

➢ Soit c un diviseur de mn, comme m et n sont premiers entre eux, c s'écrit de façon unique sous la forme $c = ab$, avec $a|m$ et $b|n$.
D'où l'égalité $s(mn) = s(m)s(n)$.

Théorème *Soit un entier naturel n strictement supérieur à* 1, *on note* $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ *sa décomposition en produit de facteurs premiers, on a* $s(n) = (1 + p_1 + \dots + p_1^{\alpha_1})(1 + p_2 + \dots + p_2^{\alpha_2}) \dots (1 + p_r + \dots + p_r^{\alpha_r})$.
Exemple $s(150) = s(2^1 \times 3^1 \times 5^2) = (1+2)\times(1+3)\times(1+5+5^2) = 3\times 4\times 31 = 372$

3- Indicateur d'Euler

Notation *Soit un entier naturel n supérieur ou égal à 2, on note* $\varphi(n)$ *(resp.* E_n*) le nombre (resp. l'ensemble) des entiers naturels strictement inférieurs à n et premiers avec n. On appelle indicateur d'Euler la fonction* $\varphi : \mathbb{N} - \{0,1\} \mapsto \mathbb{N}$ *ainsi définie.*

Exemple
$\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(6) = 2$.

Propriété *Soit un entier naturel n supérieur ou égal à* 2, $\varphi(n)$ *est le nombre d'éléments inversibles de* $\mathbb{Z}/n\mathbb{Z}$

Démonstration
Ceci résulte immédiatement du résultat suivant que nous avons démontré :

pour tout élément k de $[\![1, n-1]\!]$, $\dot{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow PGCD(k,n) = 1$.

Conséquence *Soit un entier naturel n supérieur ou égal à* 2,
n est premier $\Leftrightarrow \varphi(n) = n - 1$.

Conséquence *Soit un entier naturel p premier et un entier naturel* α *supérieur ou égal à 1, on a*
$\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Théorème *Soit des entiers naturels m et n supérieurs ou égaux à 2 et premiers entre eux, on a*
$\varphi(mn) = \varphi(m)\varphi(n)$

Démonstration
Soit F la fonction définie comme suit:

$$F : [\![0, mn-1]\!] \to [\![0, m-1]\!] \times [\![0, n-1]\!], \quad x \mapsto (f(x), g(x)) \quad \text{avec} \quad \begin{cases} f(x) \equiv x \pmod m \\ g(x) \equiv x \pmod n \end{cases}$$

Nous allons démontrer que :

- F est bijective.
  Comme $[\![0, mn-1]\!]$ et $[\![0, m-1]\!] \times [\![0, n-1]\!]$ ont le même nombre d'éléments, il suffit de démontrer que F est injective.
  Soit des éléments x et y de $[\![0, mn-1]\!]$ tels que $F(x) = F(y)$, on a alors $x \equiv y \pmod m$ et $x \equiv y \pmod n$.
  Ainsi $x - y$ est divisible par m et n. Comme m et n sont premiers entre eux, $x - y$ est divisible par mn, donc il existe un entier relatif k tel que $x - y = kmn$. Mais on sait que $0 \le x < mn$ et $0 \le y < mn$, donc $-mn < x - y < mn$, en conséquence $k = 0$ et finalement $x = y$.
- La restriction de F à E_{mn} est une bijection de E_{mn} sur $\mathrm{E}_m \times \mathrm{E}_n$.
  Il nous suffit de démontrer que :
  (i) $\forall x \in \mathrm{E}_{mn}$, $F(x) \in \mathrm{E}_m \times \mathrm{E}_n$ (c'est-à-dire $F(\mathrm{E}_{mn}) \subset \mathrm{E}_m \times \mathrm{E}_n$).
  (ii) $\forall (a,b) \in \mathrm{E}_m \times \mathrm{E}_n$, il existe $x \in \mathrm{E}_{mn}$ tel que $F(x) = (a,b)$ (c'est-à-dire $\mathrm{E}_m \times \mathrm{E}_n \subset F(\mathrm{E}_{mn})$).

(i) $x \in E_{mn} \Leftrightarrow PGCD(x,mn)=1$

$\Rightarrow PGCD(x,m)=1$ et $PGCD(x,n)=1$

$\Rightarrow f(x) \in E_m$ et $g(x) \in E_n$

(ii) Soit $(a,b) \in E_m \times E_n$, il existe $x \in [\![0, mn-1]\!]$ tel que $F(x)=(a,b)$, c'est-à-dire $f(x)=a$ et $g(x)=b$.

$f(x) \in E_m \Leftrightarrow PGCD(x,m)=1$

$g(x) \in E_n \Leftrightarrow PGCD(x,n)=1$

Or $PGCD(m,n)=1$, donc $PGCD(x,mn)=1$, d'où $x \in E_{mn}$.

Remarque Nous avons démontré que :

Soit des entiers naturels m et n premiers entre eux,

$PGCD(x,mn)=1 \Leftrightarrow (PGCD(x,m)=1$ et $PGCD(x,n)=1)$

En conclusion *La fonction* F *est une bijection de* E_{mn} *dans* $E_m \times E_n$ *et donc* $\text{card}(E_{mn}) = \text{card}(E_m) \times \text{card}(E_n)$, *c'est-à-dire* $\varphi(mn) = \varphi(m)\varphi(n)$.

Pour démontrer que l'application $F : [\![0, mn-1]\!] \to [\![0, m-1]\!] \times [\![0, n-1]\!]$ est surjective nous aurions pu utiliser le théorème qui suit.

Théorème (Restes chinois) *Soit des entiers naturels m et n premiers entre eux et des entiers naturels a et b, le système* $\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$ *d'inconnue x admet une infinité de solutions dans* $\mathbb{Z}$.

Démonstration

Comme m et n sont premiers entre eux, d'après le théorème de Bézout, il existe des entiers relatifs u et v tels que $um+vn=1$.

On vérifie que $x_0 = avn+bum$ est une solution.

En effet $x_0 \equiv avn \pmod m$

$x_0 \equiv a(1-um) \pmod m$

$x_0 \equiv a \pmod m$

De même $x_0 \equiv b \pmod n$.

Les solutions du système $\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$ sont $x = x_0 + kmn$ avec k élément de $\mathbb{Z}$.

Bien évidemment on peut choisir x_0 élément de $[\![0, mn]\!]$.

Corollaire *Soit des entiers naturels p et q premiers et distincts, on a* $\varphi(pq) = (p-1)(q-1)$.

Corollaire *Soit un entier naturel n strictement supérieur à* 1, *on note* $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ *sa décomposition en produit de facteurs premiers, on a* $\varphi(n) = \prod_{i=1}^{r}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n\prod_{i=1}^{r}(1-\frac{1}{p_i})$.

Propriété (Généralisation du petit théorème de Fermat) *Soit un entier naturel n supérieur ou égal à* 2 *et un entier relatif a premier avec n, on a* $a^{\varphi(n)} \equiv 1 \pmod n$.

Démonstration

Puisque a est premier avec n, $\dot{a}$ est un élément inversible de $\mathbb{Z}/n\mathbb{Z}$. On appelle U_n l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. On a $\text{card}(U_n) = \varphi(n)$.

Soit E_n l'ensemble des puissances de $\dot{a}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Nous allons démontrer que $\text{card}(E_n)$ divise $\varphi(n)$.

- $\text{card}(E_n)$ est fini donc il existe deux entiers naturels i et j distincts tels que $(\dot{a})^i = (\dot{a})^j$.

  On suppose $i > j$ et on pose $k = i-j$, donc $0 < k \leq \varphi(n)$.

Comme $\dot{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, $(\dot{a})^i = (\dot{a})^j \Rightarrow (\dot{a})^k = \dot{1}$.

On désigne par l le plus petit entier naturel non nul tel que $(\dot{a})^l = \dot{1}$. Ainsi $E_n = \{\dot{1}, \dot{a}, (\dot{a})^2, \ldots, (\dot{a})^{l-1}\}$.

On définit dans l'ensemble U_n la relation $\mathscr{R}$,

$\dot{x}\,\mathrm{R}\,\dot{y} \Leftrightarrow$ il existe j élément de $[\![\,0, l-1\,]\!]$ tel que $\dot{y} = (\dot{a})^j \dot{x}$.

On vérifie aisément que :

- la relation $\mathscr{R}$ est une relation d'équivalence dans U_n ;
- chaque classe d'équivalence selon $\mathscr{R}$ possède l éléments distincts.

Nous venons de démontrer un résultat plus général qui est : *l'ordre du sous-groupe E_n divise l'ordre du groupe U_n.*

- Si l'on désigne par c le nombre de classes d'équivalence ainsi obtenues, on a $\varphi(n) = cl$ (c'est-à-dire l est un diviseur de $\varphi(n)$).

Donc, $(\dot{a})^{\varphi(n)} = (\dot{a})^{cl} = ((\dot{a})^l)^c = (\dot{1})^c = \dot{1}$ et par conséquent $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Rappel (Petit théorème de Fermat) *Soit un entier naturel n premier et un entier relatif a, $a^n \equiv a \pmod{n}$. En particulier si n et a sont premiers entre eux, $a^{n-1} \equiv 1 \pmod{n}$.*

Fermat (Pierre de) (Beaumont-de-Lomagne, 1601 - Castres, 1665), mathématicien français.

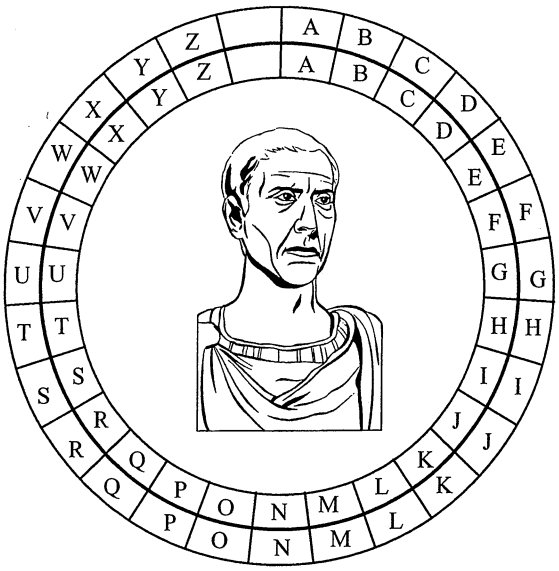
VI- PROBLÈMES DE CODAGE

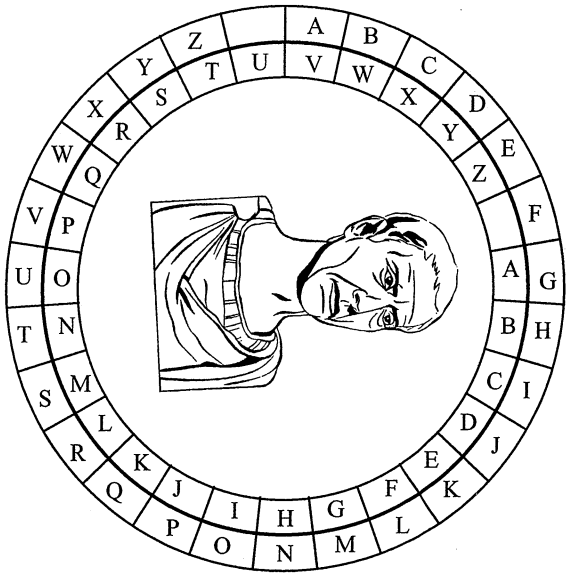
1- Exemple historique : " Le codage de César "

Pour écrire un message (à cette époque) on utilisait uniquement les 26 lettres de l'alphabet plus l'espace (bien évidemment). Un codage consistait en une bijection de cet ensemble de 27 éléments dans lui-même.

Considérons deux roues concentriques. La couronne extérieure est " fixe " et comporte les lettres de l'alphabet et l'espace, avant codage et après décodage.

On fait " tourner " le disque intérieur. Le codage s'effectue en remplaçant la lettre extérieure par la lettre correspondante de la roue intérieure.





Voici le codage de « VIVE L ARITHMETIQUE ».

V	I	V	E		L		A	R	I	T	H	M	E	T	I	Q	U	E
P	C	P	Z	U	F	U	V	L	C	N	B	G	Z	N	C	K	O	Z

Après codage on obtient « PCPZUFUVLCNBGZNCKOZ ».

Le décodage s'effectue par l'intermédiaire de l'opération réciproque.

Remarques

Selon la rotation que l'on fait subir à la roue intérieure on peut obtenir 27 codages différents, en comptant l'identité.

Ces codages sont assez puérils dans le sens où la fréquence des lettres permet d'effectuer facilement le décodage.

2- Liminaire aux codages actuels

Un message est constitué des caractères habituels de l'édition.

Étape 1 : numérisation ou chiffrement

On numérise ce message par des entiers naturels de même longueur l, quitte à rajouter des 0 " au début " , caractère par caractère.

On obtient ainsi un entier naturel α.

Étape 2 : codage

On découpe l'entier naturel obtenu en tranches de n chiffres. Les diverses tranches sont remplacées par des nouveaux entiers naturels de p chiffres, qui, concaténés, nous donnent un entier naturel α'. C'est le message codé.

Étape 3 : décodage

On revient de α' à α.

Étape 4 : dénumérisation ou déchiffrement

On passe de α au message en clair.

Remarques

Le chiffrement et le déchiffrement sont des procédés standards du domaine public.

Le codage (en général) et le décodage ne sont pas dans le domaine public.

Il se peut (eh oui !) que le codage soit dans le domaine public, sans que l'on puisse pour autant trouver aisément le décodage, c'est le principe du codage RSA que nous allons expliquer par la suite.

3- Un principe de codage

Chaque symbole est " chiffré " par un entier naturel de l'intervalle $[\![0,255]\!]$.

Parmi ces symboles figurent des caractères imprimables (" a ", " b ", " * ", " @ ", etc) et des caractères non imprimables mais qui font partie intégrante du texte (" retour ligne ", " fin de paragraphe ", " écrire en gras " et des ordres envoyés aux périphériques comme l'imprimante, l'écran, etc...).

Ainsi par exemple, le code 007 correspond à " BEL " qui est le début du mot anglais " BELL " qui signifie " CLOCHE " ou " SONNERIE " et qui envoie le célèbre " BIP " que vous entendez de temps en temps, surtout lorsque vous faites quelque chose de répréhensible ou de contre-indiqué avec votre clavier ou votre souris.

Mersenne (Marin) (près d'Oizé, Maine, 1588 - Paris, 1648), prêtre, philosophe et savant français; ami de Descartes.

Tableau de correspondance

Code	Car	Code	Car	Code	Car	Code	Car	Code	Car	Code	Car	Code	Car	Code	Car
000		032		064	@	096	`	128	•	160		192	À	224	à
001	´	033	!	065	A	097	a	129		161	¡	193	Á	225	á
002	•	034	"	066	B	098	b	130	,	162	¢	194	Â	226	â
003	˜	035	#	067	C	099	c	131	*f*	163	£	195	Ã	227	ã
004	¯	036	$	068	D	100	d	132	„	164	¤	196	Ä	228	ä
005	˘	037	%	069	E	101	e	133	…	165	¥	197	Å	229	å
006	·	038	&	070	F	102	f	134	†	166	¦	198	Æ	230	æ
007	¨	039	'	071	G	103	g	135	‡	167	§	199	Ç	231	ç
008	°	040	(	072	H	104	h	136	ˆ	168	¨	200	È	232	è
009		041	)	073	I	105	i	137	‰	169	©	201	É	233	é
010	°	042	*	074	J	106	j	138	Š	170	ª	202	Ê	234	ê
011	°	043	+	075	K	107	k	139	‹	171	«	203	Ë	235	ë
012		044	,	076	L	108	l	140	Œ	172	¬	204	Ì	236	ì
013	°	045	-	077	M	109	m	141		173	-	205	Í	237	í
014		046	.	078	N	110	n	142		174	®	206	Î	238	î
015	•	047	/	079	O	111	o	143		175	¯	207	Ï	239	ï
016	•	048	0	080	P	112	p	144		176	°	208	Đ	240	ð
017	•	049	1	081	Q	113	q	145	‘	177	±	209	Ñ	241	ñ
018	•	050	2	082	R	114	r	146	’	178	²	210	Ò	242	ò
019	•	051	3	083	S	115	s	147	“	179	³	211	Ó	243	ó
020	•	052	4	084	T	116	t	148	”	180	´	212	Ô	244	ô
021	•	053	5	085	U	117	u	149	•	181	µ	213	Õ	245	õ
022	•	054	6	086	V	118	v	150	–	182	¶	214	Ö	246	ö
023	•	055	7	087	W	119	w	151	—	183	·	215	×	247	÷
024	•	056	8	088	X	120	x	152	˜	184	¸	216	Ø	248	ø
025	•	057	9	089	Y	121	y	153	™	185	¹	217	Ù	249	ù
026	•	058	:	090	Z	122	z	154	š	186	º	218	Ú	250	ú
027	•	059	;	091	[	123	{	155	›	187	»	219	Û	251	û
028	•	060	<	092	\	124	|	156	œ	188	¼	220	Ü	252	ü
029	•	061	=	093	]	125	}	157		189	½	221	Ý	253	ý
030	-	062	>	094	^	126	~	158		190	¾	222	Þ	254	þ
031		063	?	095	_	127		159	Ÿ	191	¿	223	ß	255	ÿ

Vous remarquerez que $16^2 = 256$, ce qui correspond au calcul en hexadécimal. A la fin des modes d'emploi des imprimantes vous trouverez ces codes sous forme d'un tableau à double entrée de 16 sur 16.

Nous présentons dans les pages qui suivent différents systèmes de codages.

1^er^ exemple (" Translation ")

Étape 1 : numérisation ou chiffrement

Tout d'abord nous allons numériser «Vive l'Arithmétique!» .

V	i	v	e		l	'	A	r	i	t	h	m	é	t	i	q	u	e	!
086	105	118	101	032	108	039	065	114	105	116	104	109	233	116	105	113	117	101	033

$\alpha = 086105118101032108039065114105116104109233116105113117101033$

Étape 2 : codage Le message à envoyer est découpé en tranches de 3 chiffres.

$\alpha = 086\ 105\ 118\ 101\ 032\ 108\ 039\ 065\ 114\ 105\ 116\ 104\ 109\ 233\ 116\ 105\ 113\ 117\ 101\ 033$

Étant donné un élément a de $[\![0,255]\!]$, considérons l'application f définie comme suit :

$f : [\![0,255]\!] \to [\![0,255]\!]$ où $\psi(t)$ est le reste de la division euclidienne de t par 256

$x \mapsto \psi(x+a)$

Prenons par exemple $a = 21$.

En découpant en tranches de 3 chiffres on obtient :

V	i	V	e		l	'	A	r	i	t	h	m	é	t	i	q	u	e	!
086	105	118	101	032	108	039	065	114	105	116	104	109	233	116	105	113	117	101	033
107	126	139	122	053	129	060	086	135	126	137	125	130	254	137	126	134	138	122	054

Le message codé est alors :

$\alpha' = 107126139122053129060086135126137125130254137126134138122054$

Il n'y a pas de problème de décodage car l'opération de décodage est donnée par $f^{-1} : x \mapsto \psi(x-a)$.

2^ème^ exemple (" Translation ")

Étape 1 : numérisation ou chiffrement

Tout d'abord nous allons numériser «Vive l'Arithmétique!».

V	i	v	e		l	'	A	r	i	T	h	m	é	t	i	q	u	e	!
086	105	118	101	032	108	039	065	114	105	116	104	109	233	116	105	113	117	101	033

$\alpha = 086105118101032108039065114105116104109233116105113117101033$

Étape 2 : codage Le message en clair est découpé en tranches de 6 chiffres traitées par groupes de 3 chiffres.

$\alpha = 086105\ 118101\ 032108\ 039065\ 114105\ 116104\ 109233\ 116105\ 113117\ 101033$

Étant donné des éléments a et b de $[\![0,255]\!]$, considérons l'application f définie comme suit :

$f : [\![0,255]\!]\times[\![0,255]\!] \to [\![0,255]\!]\times[\![0,255]\!]$ où $\psi(t)$ est le reste de la division euclidienne de t par 256.

$(x, y) \mapsto (\psi(x+a), \psi(y+b))$

Prenons par exemple $a = 21$ et $b = 153$.

En découpant en tranches de 6 chiffres traitées par groupes de 3 chiffres on obtient :

V	i	v	e		l	'	A	r	i	t	h	m	é	t	i	q	u	e	!
086	**105**	118	**101**	032	**108**	039	**065**	114	**105**	116	**104**	109	**233**	116	**105**	113	**117**	101	**033**
107	**002**	139	**254**	053	**005**	060	**218**	135	**002**	137	**001**	130	**130**	137	**002**	134	**014**	122	**186**

Le message codé est alors :

$\alpha' = 107002139254053005060218135002137001130130137002134014122186$

Il n'y a pas de problème de décodage car l'opération de décodage est donnée par $f^{-1} : (x, y) \mapsto (\psi(x-a), \psi(y-b))$.

3ème exemple (" Application affine ")

Étape 1 : numérisation ou chiffrement

Tout d'abord nous allons numériser «Vive l'Arithmétique!».

V	i	v	e		L	'	A	r	i	t	h	m	é	t	i	q	u	e	!
086	105	118	101	032	108	039	065	114	105	116	104	109	233	116	105	113	117	101	033

$\alpha = 086105118101032108039065114105116104109233116105113117101033$

Étape 2 : codage Le message à envoyer est découpé en tranches de 3 chiffres.

Étant donné des éléments a et b de $[\![0,255]\!]$, tels que a soit premier avec 256 (a impair), on considère l'application définie comme suit:

$f : [\![0,255]\!] \to [\![0,255]\!]$ où $\psi(t)$ est le reste de la division euclidienne de t par 256.

$x \mapsto \psi(ax+b)$

Prenons par exemple $a = 21$ et $b = 60$.

V	i	v	e		l	'	A	r	i	t	h	m	é	t	i	q	u	e	!
086	105	118	101	032	108	039	065	114	105	116	104	109	233	116	105	113	117	101	033
074	217	234	133	220	024	111	145	150	217	192	196	045	089	192	217	129	213	133	241

Le message codé est alors :

$\alpha' = 074217234133220024111145150217192196045089192217129213133241$

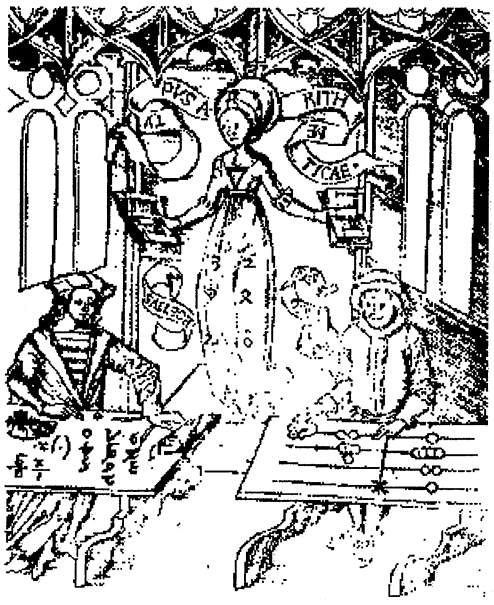
Le choix de a premier avec 256 nous assure de l'existence de a' élément de $[\![0,255]\!]$ tel que $\psi(aa') = 1$.

Pour $a = 21$ on a $a' = 61$ et $f^{-1}(x) = \psi(61x+180)$.

Note Pour ces codages et décodages :

- se référer aux programmes de la TI 92 PLUS de Texas Instruments© présentés en annexe.
- l'emploi d'un tableur comme EXCEL© peut s'avérer fort commode en utilisant les fonctions suivantes : " CODE " qui renvoie le code d'un caractère par exemple CODE(i) = 105 et la fonction " CAR " qui est la fonction réciproque de la précédente, par exemple CAR(116) = t.

  De plus on dispose dans ce tableur des fonctions habituelles de l'arithmétique comme par exemple la fonction " MOD " : MOD(a ; b) renvoie le reste de la division euclidienne de a par b.



4- Le codage RSA (Rivest, Shamir, Adleman)

a) Préliminaire

Soit des entiers naturels p et q distincts et premiers.

Notons $N = pq$, on a $\varphi(N) = (p-1)(q-1)$.

Soit un entier naturel k tel que $k \equiv 1 \pmod{\varphi(N)}$, il existe donc un entier naturel λ tel que $k = 1 + \lambda\varphi(N)$.

On a alors le résultat suivant, *pour tout entier naturel x,* $x^k \equiv x \pmod{N}$.

Démonstration

Nous avons plusieurs cas à envisager.

- x et pq sont premiers entre eux.

  $x^{\varphi(pq)} \equiv 1 \pmod{pq}$ (Généralisation du petit théorème de Fermat)

  $(x^{\varphi(pq)})^{\lambda} \equiv 1^{\lambda} \pmod{pq}$

  $x^{\lambda\varphi(pq)} \equiv 1 \pmod{pq}$

  $x^{\lambda\varphi(pq)+1} \equiv x \pmod{pq}$

  $x^k \equiv x \pmod{pq}$

- p divise x, et, q ne divise pas x.

  $x^{q-1} \equiv 1 \pmod{q}$ (Petit théorème de Fermat)

  En élevant chaque membre à la puissance $\lambda(p-1)$, on obtient,

  $x^{\lambda(p-1)(q-1)} \equiv 1 \pmod{q}$

  $x^{\lambda(p-1)(q-1)+1} \equiv x \pmod{q}$

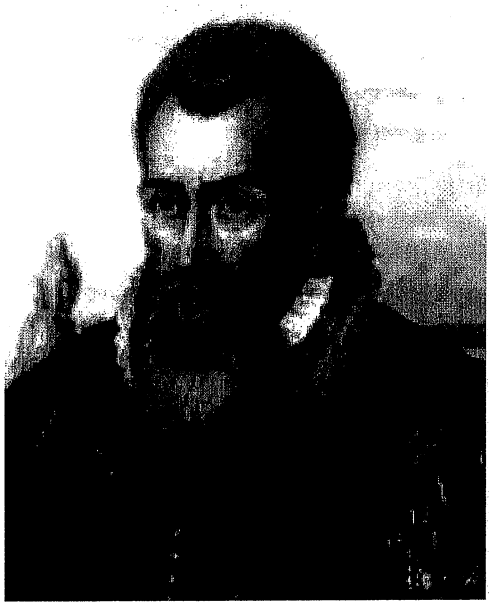
  $x^k \equiv x \pmod{q}$

  Ainsi p divise x et q divise $x^k - x$, comme p et q sont premiers entre eux, pq divise $x^k - x$, c'est à dire $x^k \equiv x \pmod{pq}$

- q divise x, et, p ne divise pas x.

  C'est la même chose que précédemment car p et q jouent des rôles symétriques.

- p et q divisent x. C'est trivial.



Neper ou Napier (John, baron de Merchiston) (Merchiston, 1550 - 1617), mathématicien écossais. Il inventa un instrument appelé bâtons de Neper qui est l'ancêtre de la règle à calcul.

b) Revenons au codage RSA proprement dit

Principe

On choisit un entier naturel N produit de deux nombres premiers distincts p et q.

On détermine deux entiers naturels e et d tels que $ed \equiv 1 \pmod{\varphi(N)}$.

Le résultat précédent conduit à,

(E) $x^{ed} = (x^e)^d = (x^d)^e \equiv x \pmod{N}$ pour tout entier naturel x.

Les nombres N et e sont publiés et utilisés pour l'écriture du message codé, par contre p et q ne sont pas connus du public.

Le processus commence par le découpage du message en clair préalablement numérisé, en blocs de même longueur. Chaque bloc du message non codé est ainsi un nombre x dont le nombre de chiffres est strictement inférieur au nombre de chiffres de N.

Le codage c du message clair représenté par x est obtenu à l'aide de la relation $c \equiv x^e \pmod{N}$ avec $0 \leq c < N$ (c est le reste de la division euclidienne de x^e par N).

Ainsi l'opération de décodage du message se fait grâce aux égalités ***(E)*** puisque $x \equiv c^d \pmod{N}$ avec $0 \leq x < N$ (x est le reste de la division euclidienne de c^d par N).

Mais si les nombres N et e sont publiés et permettent à tout un chacun de coder un message, le nombre d est fourni au seul détenteur de l'opération de décodage par le concepteur du processus qui est le seul à connaître p et q et donc $\varphi(N)$.

En résumé, l'opération de codage est une élévation à la puissance e dans $\mathbb{Z}/N\mathbb{Z}$, l'opération de décodage est une élévation à la puissance d dans $\mathbb{Z}/N\mathbb{Z}$ avec $ed \equiv 1 \pmod{\varphi(N)}$.

La sécurité du système réside dans la difficulté qu'il y a à obtenir le nombre d qui permet le déchiffrement, c'est à dire la difficulté à factoriser le nombre N.

Exemple

$N = 2173 = 41 \times 53$

$p = 41$ et $q = 53$

L'indicateur d'Euler de N est

$\varphi(2173) = (41-1)(53-1) = 2080$

En prenant $e = 1427$ et on obtient $d = 1083$.

Prenons un nombre à coder, par exemple

$\alpha = 15070356901453213$

Découpons cet entier en tranche de 3 chiffres à partir de la droite. Ce découpage nous assure que chacun des nombres obtenus est strictement inférieur à 2173.

x	c	Normalisation (*)
015	1565	1565
070	1580	1580
356	1297	1297
901	901	0901
453	907	0907
213	1273	1273

$\alpha' = 156515801297090109071273$

(*) Nous avons été obligés d'écrire des nombres de 4 chiffres (en " rajoutant " éventuellement des 0 " devant ") car $0 \leq c < 2173$ et les nombres obtenus peuvent avoir 4 chiffres, ce qui est le cas pour $x = 15$, on a $c = 1565$ (c'est ce que nous avons appelé normalisation dans le tableau ci-dessus).

Pour décoder, on découpe α' en tranches de 4 chiffres (nombre de chiffres de N) à partir de la droite.

C	x	Normalisation
1565	15	015
1580	70	070
1297	356	356
901	901	901
907	453	453
1273	213	213

Ainsi on retrouve

$\alpha = 15070356901453213$

Trouver un nombre premier très grand n'est pas très difficile. En revanche la grande difficulté (actuelle) est de factoriser un nombre N donné.

c) Pour conclure

Ce système de codage à " clefs publiques " pourrait si l'on n'est pas un minimum astucieux présenter un grave inconvénient : *"n'importe qui peut envoyer un message codé à n'importe qui "*. Par conséquent, il est indispensable d'authentifier l'auteur du message.

Alors voici comment on procède.

Une personne A dont la " fonction de codage est f " envoie un message à une personne B dont la " fonction de codage est g ".

Rappelons que f et g sont publics mais que le seul à connaître f^{-1} est A et que le seul à connaître g^{-1} est B.

La personne A envoie un message M à la personne B sous la forme $g(M)$.

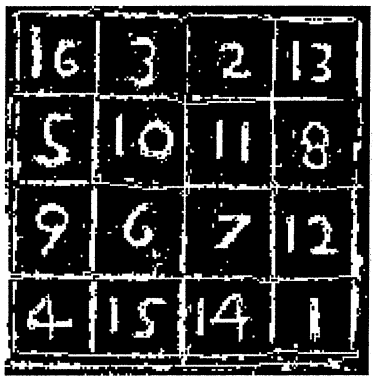
Ce message M contient, en plus du texte, la signature A **plus** (là c'est très important) $f^{-1}(A)$.

La personne B reçoit le message $g(M)$ et lit à la fin du message le nom de l'expéditeur A plus un autre message codé m qui est en fait $f^{-1}(A)$. La personne B fait $f(m)$.

Si $f(m) = A$ c'est que le vrai auteur du message est bien A puisque c'est la seule personne à connaître f^{-1}, sinon c'est un faux message.

Melancolia gravure sur cuivre (1514) d'Albrecht Dürer (Nuremberg 1471 - Nuremberg 1528, peintre et graveur allemand).

En haut à droite de la gravure on peut voir un carré magique de 4 sur 4 dont voici le détail. Vous remarquerez que la date à laquelle a été réalisé cette gravure figure dans le carré magique.



Partie D ALGORITHMES

1- Codage RSA à l'aide de la TI 92 PLUS

Extrait de *Hypothèses* n° 13 Avril 1998 " Arithmétique et codage " Henri LAMBERT.

Pour rendre ce paragraphe indépendant de ce qui précède nous rappelons très brièvement le principe du codage RSA.

La clef de codage est un nombre $n = p_1 p_2$, avec p_1 et p_2 des nombres premiers, et la clef de décodage sera $\varphi(n) = (p_1 - 1)(p_2 - 1)$. Ainsi pour la déterminer, il faudra connaître p_1 et p_2, ce qui n'est pas si simple lorsqu'on ne connaît que n et même si n n'a que quelques dizaines de chiffres. En effet, il faudrait aujourd'hui plusieurs millions d'années pour décomposer un nombre n (convenablement choisi) de 500 chiffres en facteurs premiers, même pour les ordinateurs les plus puissants.

On choisit deux nombres premiers assez grands, 113 et 239 par exemple, et $n = 113 \times 239 = 27007$.
L'indicateur d'Euler est $\varphi(n) = (p_1 - 1)(p_2 - 1) = 26656$.

- On choisit ensuite deux nombres a et b tels que $ab \equiv 1 \pmod{\varphi(n)}$, ici $a = 19$ et $b = 1403$.
- Si m appartient à l'intervalle $[\![0, n-1]\!]$, alors $f(m)$ sera le reste de la division de m^a (m^{19}) par $n = 27007$ et $f^{-1}(m)$ le reste de m^b dans la même division.

Pour mettre en place notre algorithme, utilisons les capacités de calcul de la TI-92 PLUS. Le nombre a ($a = 19$) étant petit, le calcul de $f(m)$ peut se faire sans programmation. Le nombre b (ici $b = 1403$) étant lui grand, il nous faudra toutefois écrire un programme de calcul de $m^b \pmod{n}$ m^b. L'algorithme utilisé, (fonction " puismod ") est semblable à celui de « l'exponentiation rapide ».

Remarque
Par rapport au paragraphe précédent,

Notation précédente	N	p_1	p_2	a	b
Notation TI92 PLUS	n	p	q	e	d

Programmes

```
cod(l,a,n)
Func
seq(mod(l[i]^a, n), i, 1, dim(l))
Endfunc
```

Codage d'une liste *l*
a = puissance, *n* = clef on élève chaque élément de *l* à la puissance *a*, et on le prend modulo *n*.

```
conv(ch)
Func
seq(ord(mid(ch, i, 1)), i, 1, dim(ch))
Endfunc
```

Conversion d'une chaîne *ch*
chaque caractère de *ch* est converti en son mode ASCII.

```
decod(l,b,n)
Func
seq(puismod(l[i], b, n), i, 1, dim(l))
Endfunc
```

Décodage de la liste *l*
b = puissance, *n* = clef, on élève chaque de *l*, à la puissance *n* qu'on prend modulo *b*.

```
deconv(l)
Func
Local ch,i
" "→ ch
For i,1,dim(l) ch&char(l[i]) → ch
Endfor
ch
Endfunc
```

Conversion inverse de la liste *l*
ch est initialisé à la chaîne vide.
Chaque élément de *l* est converti en lettre et rajouté à *ch*.
Retourne *ch*.

```
puismod(b,n,c)
Func
Local m, r, i, j, l
2 → m
1 → i
While m≠n
2*m → m
i+1 → i
EndWhile
i−1 → i
m/2 → m
1→r
For j,1,i+1
   If n≥m Then
   mod(b*r,c)→r
   n−m→n
   EndIf
m/2 → m
   If m≥1 Then
   mod(r^2,c)→r
   EndIf
Endfor
r
Endfunc
```

Calcul de b^n modulo *c*

Calcul du plus grand *i* tel que $2^i < n$

Calcul rapide de b^n modulo *c*.

2- Algorithme d'Euclide

- **Itératif**

La version la plus dépouillée de l'algorithme d'Euclide sous sa forme itérative est la suivante :

```
x :=a ; y :=b ;
TANT QUE x≠y FAIRE
    DEBUT
    SI x>y ALORS x :=x-y
    SINON y :=y-x
   FIN
resultat :=x
```

Si l'on dispose d'une fonction permettant de donner le reste d'une division euclidienne, son utilisation permet d'accélérer la convergence de l'algorithme. En voici une version écrite en langage MAPLE.

Cette procédure utilise la fonction **irem** permettant d'obtenir le reste de la division euclidienne de deux entiers :

```
➢ pgcd:=proc(a,b)
  local x,y,r;
  x:=a;y:=b;
  while y<>0 do
    r:=irem(x,y);
    x:=y;
    y:=r;
    od;
  x
  end:
```

- **Récursif**

C'est dans sa forme récursive que l'algorithme d'Euclide prend tout son sens. Le principe est le suivant, on veut calculer le *PGCD* de *a* et de *b*. (Écriture en MAPLE en utilisant la fonction **irem**).

- Si *b* est nul, le *PGCD* est *a*.
- Sinon, ce *PGCD* est aussi le *PGCD* de *b* et du reste de la division euclidienne de *a* par *b*.

```
➢ pgcd:=proc(a,b)
    if b=0 then a
    else pgcd(b,irem(a,b))
    fi
  end:
```

3- Algorithme de Bézout

L'algorithme d'Euclide permet d'obtenir le *PGCD* de deux entiers a et de b.
Il est possible sans trop de modifications de calculer en même temps les coefficients u et v de l'identité de Bézout : $au+bv=d$

Supposons que $a>b>0$ (ce qui ne nuit en rien à la généralité de nos propos), on calcule la suite des triplets $W_i=(u_i,v_i,d_i)$ définis par :

$W_0=(1,0,a)$

$W_1=(0,1,b)$

$W_{i+1}=W_{i-1}-q_{i+1}W_i$ où $q_{i+1}=\mathrm{E}(d_{i-1}/d_i)$ pour $i\geq 2$. ($\mathrm{E}(x)$ désigne la partie entière de x.)

L'algorithme s'arrête au premier entier j tel que $d_j=0$.

On a alors $d=d_{j-1}=au_{j-1}+bv_{j-1}$.

En effet, par construction, pour tout entier naturel i, $d_i=au_i+bv_i$, et donc en particulier $d_{j-1}\in(a\mathbb{Z}+b\mathbb{Z})$.

Il en résulte que d divise d_{j-1}, il reste à montrer que d_{j-1} divise à la fois a et b.

Par définition d_{j-1} divise à la fois d_{j-1} et d_{j-2}. La formule $d_{i-2}=d_i+q_i\,d_{i-1}$, appliquée successivement pour i allant de $j-1$ à 2, montre que d_{j-1} divise tous les d_i pour i allant de $j-1$ à 0, et donc $d_1=b$ et $d_0=a$.

Voici cet algorithme programmé sur une TI-92 dans lequel a et b sont des entiers relatifs quelconques.

```
gcdex(a,b)
Func
Local temp
{1,0,a}→a
{0,1,b}→b
While a[3]≠0
     a→temp
     b-a*int(b[3]/(a[3]))→a
     temp→b
EndWhile
EndFunc
```

L'appel de **gcdex(a,b)** retourne la liste $\{u,v,d\}$, où $d=PGCD(a,b)$ et $au+bv=d$.

Partie E – EXERCICES

Introduction

Nous proposons ici, quelques exercices permettant une meilleure compréhension des notions exposées dans le cours. Nous avons évité d'inclure des exercices d'applications immédiates et connus de tous les enseignants. Nous avons essayé de présenter des utilisations souvent originales des résultats établis précédemment et espérons que vous, lecteurs, prendrez autant de plaisir à les résoudre que nous en avons pris à les concevoir.

Les exercices sont classés en fonction du cours.

A la suite du numéro de chaque exercice nous avons indiqué la référence au cours. Par exemple **20. AV** signifie numéro d'exercice 20 correspondant au paragraphe **V** de la partie **A**. De plus à la fin du document sont répertoriés des exercices de synthèse numérotés **S**.

1. A-I FRACTION ÉGYPTIENNE

Les égyptiens prenaient soin pour effectuer leurs divers calculs de décomposer 1 sous la forme de la somme des inverses d'entiers naturels différents deux à deux. Nous nous proposons de vérifier que ceci est toujours possible.

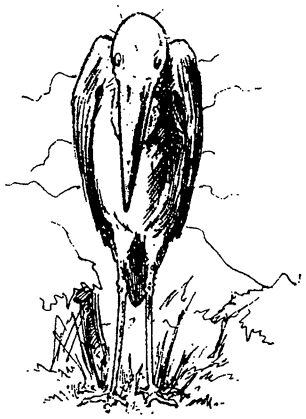
Par exemple : $1=\frac{1}{2}+\frac{1}{3}+\frac{1}{6}$, $1=\frac{1}{2}+\frac{1}{4}+\frac{1}{6}+\frac{1}{12}$.

Soit un entier naturel $n\geq 3$, *montrer qu'il existe* $a_1, a_2, \ldots, a_n$ *deux à deux distincts tels que* $1=\frac{1}{a_1}+\frac{1}{a_2}+\ldots+\frac{1}{a_n}$.

Indication

Raisonner par récurrence.

2. A-II



L'exercice qui suit peut être résolu à l'aide de raisonnements par récurrence au tout début de l'apprentissage de l'arithmétique. Il gagnera à être repris par la suite avec l'outil des congruences modulo un entier naturel judicieusement choisi.

Démontrer que pour tout entier naturel n non nul :

a) 1998^n-3^n *est divisible par* 7.

b) $3\times 5^{2n-1}+2^{3n-2}$ *est divisible par* 17.

c) $16\times 7^{2n}-28\times 3^{2n+3}$ *est divisible par* 5.

d) $2^{2n}(2^{2n+1}-1)-1$ *est divisible par* 9.

e) $18^{4n+1}-44^{4n-1}-3\times 96^{4n+2}$ *est divisible par* 13.

f) 4^n+6n-1 *est divisible par* 9.

Indication

d) On pourra écrire :. $2^{2n}(2^{2n+1}-1)-1=(4^n-1)(2\times 4^n+1)$

3. A-III

Déterminer tous les entiers naturels x et y tels que $(x-1)(y+5)=36$.

4. A-III

Déterminer tous les entiers naturels x et y tels que $xy = 3x + 2y + 54$.

Indication

On écrira cette équation sous la forme $(x-a)(y+b) = n$.

5. A-IV PREMIER PROBLÈME BASCO-CHINOIS

Les joyeux lurons de la Banda « Los Borachos » défilent tous les ans. Cette année le vieil Antoine étant perclus de rhumatismes, ils se mirent comme d'habitude en rang par 6, bien sur il manquait Antoine pour compléter le dernier rang. Ils essayèrent en rang par 5, puis par 4, puis 3 et même 2 et chaque fois il manquait Antoine pour compléter le dernier rang. Ils purent cependant défiler par rang de 7 sans que l'absence d'Antoine ne se fasse sentir ailleurs que dans les cœurs et les chœurs.
Sachant qu'ils étaient moins de 500, combien étaient-ils ?

Indication

Le nombre *n* de membres de la Banda est divisible par 6, par, 5, par 4, par 3 et par 2.

6. A-IV

Soit des entiers naturels a, b et c non nuls tels que $a^2 = b^2 + c^2$.

1- *Montrer que l'un de ces trois nombres au moins a, b ou c est divisible par* 2.

2- *Montrer que l'un de ces trois nombres au moins a, b ou c est divisible par* 3.

3- *Montrer que l'un de ces trois nombres au moins a, b ou c est divisible par* 4.

4- *Montrer que l'un de ces trois nombres au moins a, b ou c est divisible par* 5.

7. A-IV UN ASPECT GÉOMÉTRIQUE du *PGCD* et du *PPCM*

Nous nous proposons d'illustrer graphiquement la notion de plus grand commun diviseur et de plus petit commun multiple de nombres dont la décomposition en produit de facteurs premiers ne comprend que les deux mêmes facteurs premiers.

On considère les entiers naturels n de la forme $n = 2^x \times 3^y$ *avec x et y entiers naturels.*

Le plan P est muni d'un repère (O,I,J).

Au nombre $n = 2^x \times 3^y$ *on associe le point N de coordonnées* $(x;y)$ *appelé image de n.*

Dans tout ce qui suit, on appellera " points ", les points dont les coordonnées sont des entiers naturels et on désignera par A, B, C, ..., les points correspondant aux entiers naturels a, b, c, ...

On pose $a = 2^x \times 3^y$ *et* $b = 2^{x'} \times 3^{y'}$.

Dans tout ce qui suit pour représenter des points on prendra $a = 2^7 \times 3^3$ *et* $b = 2^5 \times 3^{11}$.

1- *Caractériser et représenter géométriquement :*

a) *les diviseurs de a ;*

b) *les multiples de a ;*

c) *les puissances de a ;*

d) *le point de la droite* (OA) *distinct de O, le plus près de O.*

2- *Caractériser et représenter géométriquement :*

a) $d = PGCD(a\,;\,b)$

b) $m = PPCM(a\,;\,b)$.

À quelle condition les points A, B, D et M sont-ils distincts ?

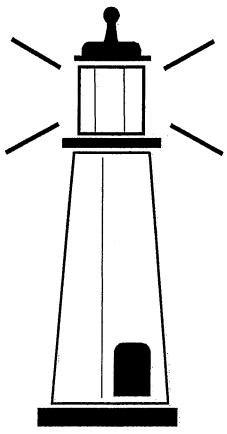
3- *Soit* $p = ab$.

a) *Démontrer que* $\overrightarrow{OP} = \overrightarrow{OA} + \overrightarrow{OB}$.

a) *Démontrer que* $\overrightarrow{OP} = \overrightarrow{OD} + \overrightarrow{OM}$.

a) *Quelle relation peut-on en déduire entre a, b, d et m ?*

8. A-IV LE PHARE



Un phare émet trois feux de couleurs différentes : un feu rouge toutes les 16 secondes, un feu vert toutes les 45 secondes et un feu blanc toutes les 2 minutes 20 secondes.

Ces trois feux sont émis simultanément à minuit. Indiquer les instants des émissions simultanées :

1- *des feux rouge et vert ;*

2-*des feux rouge et blanc ;*

3- *des feux vert et blanc ;*

4- *des trois feux.*

9. A-IV LES AIGUILLES[1]

Nous avons une montre traditionnelle :

1- *Combien de fois par 24 heures les aiguilles sont-elles superposées ?*

2- *En partant de minuit donner les heures de superposition des deux aiguilles.*

10. A-IV

Soit un entier naturel n. Le but de cet exercice est de chercher les entiers naturels a et b supérieurs à $2n$ *vérifiant* $(a-2n)(b-2n)=2n^2$. $\boxed{1}$

1- *Démontrer que tout diviseur commun à* $a-2n$ *et* $b-2n$ *divise a et b.*

2- *En montrant que l'équation* $\boxed{1}$ *peut s'écrire sous la forme* $a^2+b^2=(a+b-2n)^2$, *montrer que tout diviseur commun à a et b divise* $a-2n$ *et* $b-2n$.

3- *Démontrer que tout diviseur commun à a et b divise n.*

4- *On suppose* $n=30$, *trouver tous les entiers naturels a et b premiers entre eux vérifiant l'équation* $\boxed{1}$.

11. A-IV

Soit un entier naturel n et l'entier naturel $N=n^4+4$.

1- *Montrer que N est premier si et seulement si* $n=1$.

2- *Montrer que N est divisible par 5 si et seulement si n n'est pas un multiple de 5.*

12. A-IV

Déterminer tous les entiers naturels a et b admettant 7560 *pour plus petit commun multiple et* 36 *pour plus grand commun diviseur.*

13. A-IV

Déterminer tous les entiers naturels a et b admettant 2590 *pour plus petit commun multiple et dont le produit est* 12950.

14. A-IV

Déterminer tous les entiers naturels a et b admettant 13 *pour plus grand commun diviseur et dont la somme est* 182.

---

[1] Il serait vain de retranscrire cet exercice avec une montre digitale, un cadran solaire ou un clepsydre.

15. A-IV

Soit deux entiers naturels a et b.

1- *On considère les entiers naturels* $A = 5a + 4b$ *et* $B = 11a + 9b$.

Démontrer que $PGCD(a,b) = PGCD(A,B)$

2- *On considère les entiers naturels* $A = pa + qb$ *et* $B = ra + sb$ *avec* $ps - qr = 1$.

Démontrer que $PGCD(a,b) = PGCD(A,B)$

16. A-IV

Soit un entier naturel n.

On considère les entiers naturels $a = 2n^2$ *et* $b = n(2n+1)$.

On pose $d = PGCD(a,b)$ *et* $m = PPCM(a,b)$.

Démontrer que $b - a = d$ *et* $b^2 - a^2 = m - d^2$.

17. A-IV

Déterminer les entiers naturels a et b tels que : $PPCM(a,b) - PGCD(a,b) = 77$.

18. A-IV

Déterminer les entiers naturels a et b tels que : $PPCM(a,b) + 11PGCD(a,b) = 203$.

19. A-IV

Soit un entier naturel p, montrer que

$\sqrt{p}$ *est un nombre rationnel si et seulement si p est le carré d'un entier.*

***Dans les exercices de 20 à 41, sauf mention explicite contraire, on acceptera comme écriture d'un entier naturel en base b, une écriture commençant par* 0.**

20. A-V

À tout nombre N qui s'écrit $\overline{xyz}$ *en base dix, on associe le nombre* $r(N)$ *qui s'écrit* $\overline{zyx}$ *en base dix.*

Soit $N = \overline{xyz}$ *avec* $x > y > z$.

On appelle P le nombre $N - r(N)$ *et on calcule le nombre* $Q = P + r(P)$.

1- *Démontrer que Q est indépendant de N.*

2- *Reprendre le problème en base b.*

21. A-V

À tout nombre N qui s'écrit $\overline{xyz}$ *en base dix, on associe les nombres :*

- $r(N)$ *qui s'écrit* $\overline{zyx}$ *en base dix. (Certains chiffres x, y ou z peuvent être égaux à 0) ;*
- $\rho(N)$ *qui s'écrit* $\overline{x'y'z'}$ *en base dix, obtenu en rangeant les chiffres x, y et z par ordre décroissant (exemple* $p(131)=311$*).*

On considère la suite $(N_n)_{n\in\mathbb{N}}$ *définie par*

$$\begin{cases} N_0 = \overline{xyz} \\ N_{n+1} = \rho(N_n) - r(\rho(N_n)) \end{cases}$$

où x, y et z désignent des chiffres qui ne sont pas tous égaux.

1- *Écrire les cinq premiers termes de la suite* $(N_n)_{n\in\mathbb{N}}$ *de premier terme* 527.

2- *Montrer que* N_1 *est divisible par* 99 *et n'a pas tous ses chiffres égaux.*

3- *Montrer que la suite* $(N_n)_{n\in\mathbb{N}}$ *est constante à partir d'un certain rang et que cette constante est indépendante du choix de* N_0.

22. A-V

Soit N un entier s'écrivant $\overline{xy7}$ *en base dix et* $\overline{y00x}$ *en base huit. Déterminer N.*

23. A-V C'EST UNE AFFAIRE DE CHROMOSOMES

On considère les entiers naturels A et B qui s'écrivent dans le système décimal : $A = \overline{xyxyxyxyx5}$ *et* $B = \overline{xyxyxy}$, *x et y étant des chiffres et x étant non nul.*

1- a) *A quelle condition le nombre A est-il divisible par* 25 *?*

b) *Déterminer les différentes valeurs de A, sachant que A est divisible par* 225 *?*

2- *A quelle condition le nombre B est-il divisible par* 225 *?*

24. A-V

Soit N le nombre qui s'écrit en base dix $\overline{2xyyx2}$.

Déterminer tous les nombres N divisibles par 21.

25. A-V

Quels sont les nombres de trois chiffres qui s'écrivent $\overline{xyz}$ *en base sept et* $\overline{zyx}$ *en base onze.*

26. A-V

Quels sont les nombres de trois chiffres qui s'écrivent $\overline{xyz}$ *en base sept et* $\overline{zyx}$ *en base neuf.*

27. A-V

Dans quelle base 13^4 *s'écrit-il* $\overline{14641}$ *?*

Indication

Développer $(b+1)^4$.

28. A-V

Déterminer tous les nombres qui s'écrivent en base dix avec deux chiffres et qui sont divisibles par le produit de leurs chiffres.

Indication

On n'échappera pas à un nombre **limité** d'essais successifs..

29. A-V

1- *Dans un système de base b* $(b \geq 2)$*, démontrer que les nombres*

$N = (b-1)^2$ *et* $P = 2(b-1)$

s'écrivent $\overline{xy}$ *et* $\overline{yx}$.

2- *Dans un système de base b* $(b \geq 3)$*, démontrer que les nombres*

$Q = (b-1)^3$ *et* $R = (b+2)(b-1)^2$

s'écrivent avec les mêmes chiffres.

3- *On suppose que des entiers naturels p et q sont tels que* $p+q = b+1$ *et sont différents de 0, 1 et b.*

Démontrer que dans le système de numération de base b, les deux nombres

$S = p(b-1)$ *et* $T = q(x-1)$

s'écrivent avec les mêmes chiffres.

Indication

L'écriture d'un nombre en base *b* est unique.

30. A-V

1- *Soit N le nombre qui s'écrit en base dix* $N = \overline{xxyy}$ *Existe-t-il des chiffres x et y tels que ce nombre soit un carré ?*

2- *Pour quelles bases de numération b existe-t-il des chiffres x, y et z tels que* $\overline{xxyy} = (\overline{zz})^2$ *?*

31. A-V

Dans le système de numération de base b, les chiffres x et y sont consécutifs. Peut-on déterminer x, y et b de telle sorte que $\overline{xxxx} = (\overline{yy})^2$ *?*

Indication

On utilisera l'identité $b^3 + b^2 + b + 1 = (b^2 + 1)(b + 1)$.

On remarquera que $PGCD(b^2 + 1\ ,\ x + 1)$ divise 2 et on distinguera deux cas : b pair et b impair.

32. A-V

Existe-t-il une base b dans laquelle $\overline{41} \times \overline{14} = \overline{1224}$ *?*

33. A-V

Existe-t-il une base b dans laquelle $\overline{52} \times \overline{25} = \overline{1693}$ *?*

34. A-V

1- *Déterminer la base b dans laquelle on a* $\overline{46} + \overline{53} = \overline{132}$.

2- *Déterminer la base b dans laquelle on a* $\overline{35} + \overline{13} = \overline{51}$.

35. A-V

Soit N le nombre qui s'écrit en base dix : $\overline{13x7y}$.

Déterminer les chiffres x et y de façon que N soit divisible :

1- *par* 4 ;

2- *par* 9 ;

3- *par* 36.

36. A-V

Soit N le nombre qui s'écrit en base dix $\overline{abc}$.

Déterminer N sachant que N est divisible par 45 *et que* $2a + 3b + c = 14$.

37. A-V

Soit N un nombre qui s'écrit en base dix $\overline{axa}$ *avec a non nul.*

Déterminer N sachant que N est divisible par 11 *et que N est un carré parfait.*

38. A-V DIVISIBILITÉ PAR $\overline{11}$

1- *Soit N le nombre qui s'écrit en base dix avec n chiffres sous la forme* $\overline{10...01}$.
Montrer que N est divisible par 11 *si et seulement si n est pair.*
2- *Soit N le nombre qui s'écrit en base deux avec n chiffres sous la forme* $\overline{10...01}$.
Montrer que N est divisible par le nombre écrit $\overline{11}$ *en base deux si et seulement si n est pair.*
3- *Ce résultat peut-il être généralisé à une base quelconque ?*

39. A-V

Un nombre s'écrit 341 en base dix. Dans quelle base s'écrit-il $\overline{2331}$ *?*

40. A-V

Le but de cet exercice est de compter le nombre de parties d'un ensemble à *n* éléments (*n* entier naturel non nul).
Soit un ensemble $E = \{e_1, e_2, ..., e_n\}$.
À toute partie P de E on associe le nombre N_P *écrit en binaire de la manière suivante :*

$$N_P = \overline{a_1 a_2 ... a_n} \text{ où } a_i = \begin{cases} 1 & si \quad e_i \in P \\ 0 & si \quad e_i \notin P \end{cases}$$

1- *Montrer que l'application* $\varphi : \mathcal{P}(E) \to [\![0, 2^{n-1}]\!]$ *définie par* $\varphi(P) = N_P$ *est une bijection.*
2- *En déduire le nombre de parties de l'ensemble E.*

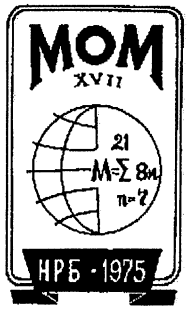
41. A-V

Nous allons considérer le nombre N qui s'écrit $\overline{ab...ab}$ *en base dix.*
1- *Montrer que* $\overline{ababab}$ *est divisible par* 7.
2- *Lorsque* $a \neq 0$ *et* $a \neq b$ *déterminer en fonction du nombre de chiffres de N, combien de ces entiers sont divisibles par* 7.

42. B-V

La somme des produits 2 à 2 de 3 entiers consécutifs n'est divisible ni par 3, ni par 5, ni par 7.

43. B-V OLYMPIADES U. R. S. S. 1964



1- *Déterminer tous les entiers naturels n tels que* $2^n - 1$ *soit divisible par* 7.
2- *Démontrer que, pour tout entier naturel n, le nombre* $2^n + 1$ *n'est jamais divisible par* 7.

44. B-V

1- *Montrer que le carré d'un nombre entier impair est congru à* 1 *modulo* 8.
2- *Soit un entier naturel n premier avec* 6 *alors* $n^2 - 1$ *est divisible par* 24.

45. B-V

1- *Quel est, en base dix, le chiffre des unités du nombre* 1998^{1998} *?*

2- *Quels sont, en base dix, les deux derniers chiffres du nombre* 1998^{1998} *?*

Indication

1- Quel est le reste de la division par 5 du nombre $A = 1998^{1998}$? (On pourra utiliser le petit théorème de Fermat).

2- Même démarche en utilisant le reste de la division par 25 et la généralisation du petit théorème de Fermat et on remarquera que $100 = 4 \times 25$.

46. B-V

1- *Démontrer que pour tout entier naturel n, l'entier naturel* $n^7 - n$ *est divisible par* 42.

2- *Déterminer le plus grand entier naturel qui, pour tout entier naturel n divise* $n^5 - n$.

3- *Déterminer le plus grand entier naturel qui, pour tout entier naturel n divise* $n^3 - n$.

47. B-V

Étant donné des entiers naturels x, y et z, démontrer que,

3 *divise* $(x+y+z)$ *si et seulement si* 3 *divise* $(x^3+y^3+z^3)$.

48. B-V

Étant donné des entiers naturels x, y et z, démontrer que,

si $(x^3+y^3+z^3)$ *est divisible par* 9 *alors l'un au moins des entiers x, y ou z est divisible par* 3.

49. B-VI BEÑAT ET PANCHOA

Beñat et Panchoa ont chacun un champ rectangulaire à cotés entiers (en mètres), dont les surfaces ne diffèrent que de 1 *mètre carré.*

Sachant que celui de Beñat a une longueur de 253 *mètres de long, celui de Panchoa a une longueur de* 256 *mètres et que les cotés ont moins de* 300 *m, quel est celui qui a le plus grand champ ?*

Quelles sont les dimensions de leurs champs sachant que :

1- *celui de Beñat est le plus grand ?*

2- *celui de Beñat est le plus petit ?*

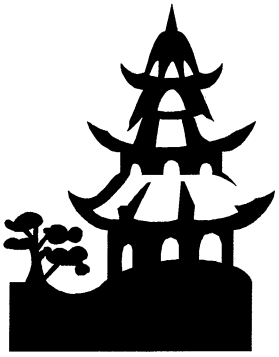
Indication

Utiliser l'identité de Bézout.

50. B-V DEUXIÈME PROBLÈME BASCO-CHINOIS

Les joyeux lurons de la Banda « Los Borachos » défilent tous les ans. Cette année le vieil Antoine étant perclus de rhumatismes, ils se mirent comme d'habitude en rang par 6, bien sûr il manquait Antoine pour compléter le dernier rang. Ils essayèrent en rang par 5, puis par 4, et chaque fois le copain Beñat d'Antoine était seul au dernier rang. Ils purent cependant défiler par rang de 7 sans que l'absence d'Antoine ne se fasse sentir ailleurs que dans les cœurs et les chœurs.
Sachant qu'ils étaient moins de 500, combien étaient-ils ?

Indication
On pourra montrer que le nombre n de membres de la Banda peut s'écrire sous la forme $n = 2 + 20q$ et $n = 1 + 7q'$, puis on utilisera le théorème de Bézout.



51. B-VI (Restes chinois)

1- a) *Déterminer un entier relatif x vérifiant le système :* $\begin{cases} x \equiv 3 \pmod{15} \\ x \equiv 7 \pmod{14} \end{cases}$

b) *Trouver tous les entiers relatifs vérifiant ces mêmes conditions.*

2- *Étant donné des entiers relatifs* a_1 *et* a_2*, et des entiers naturels* b_1 *et* b_2 *premiers entre eux, déterminer tous entiers relatifs x vérifiant le système :* $\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \end{cases}$.

Indication
2- Il existe des entiers relatifs u_1 et u_2 vérifiant $u_1 b_1 + u_2 b_2 = 1$ et $x = u_1 b_1 a_2 + u_2 b_2 a_1$ est une solution.

52. B-VI (Restes chinois)

1- a) *Déterminer tous les entiers relatifs vérifiant le système :* $\begin{cases} x \equiv 4 \pmod{30} \\ x \equiv 7 \pmod{21} \end{cases}$.

b) *Déterminer tous les entiers relatifs vérifiant le système :* $\begin{cases} x \equiv 2 \pmod{30} \\ x \equiv 6 \pmod{21} \end{cases}$.

2- *Étant donné des entiers relatifs* a_1 *et* a_2*, et des entiers naturels* b_1 *et* b_2*.*
Soit d le PGCD de b_1 *et* b_2*.*

a) *Montrer que le système* $\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \end{cases}$ *n'a pas de solution si* a_1 *n'est pas congru à* $a_2 \pmod{d}$

b) *Montrer que si* $a_1 \equiv a_2 \pmod{d}$ *le système* $\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \end{cases}$ *admet des solutions, et les trouver toutes les autres.*

Indication
2- Il existe des entiers relatifs u_1 et u_2 tels que $u_1 b_1 + u_2 b_2 = d$. On pose $b_1 = db_1'$ et $b_2 = db_2'$ alors $x = u_1 b_1' a_2 + u_2 b_2' a_1$ est une solution.

53. B-VI (Restes chinois)

Étant donné des entiers relatifs a_1, a_2 *et* a_3, *et des entiers naturels* b_1, b_2 *et* b_3.

Résoudre le système $\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \\ x \equiv a_3 \pmod{b_3} \end{cases}$.

Indication

On commence par résoudre le système $\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \end{cases}$.

En reprenant les notations de l'indication de l'exercice 4, les solutions, lorsqu'il y en a sont celles du système $\begin{cases} x \equiv a' \pmod{b'} \\ x \equiv a_3 \pmod{b_3} \end{cases}$ avec $\begin{cases} b' = PPCM(b_1, b_2) \\ a' = u_1 b_1' a_1 + u_2 b_2' a_1 \end{cases}$

54. B-VI APPLICATION LES « BANDAS CHINOISES »

L'orchestre de la république populaire de Chine a entre 50 *et* 100 *musiciens. Lorsqu'il défile par rangées de* 6 *la dernière rangée n'a que* 5 *musiciens, lorsqu'il défile par rangées de* 5 *la dernière rangée n'a que* 1 *musiciens, lorsqu'il défile par rangées de* 4 *la dernière rangée n'a que* 1 *musicien.*

Quel est le nombre de musiciens ?

55. B-VI

Soit des entiers a et b premiers entre eux,

1- *Démontrer que les entiers* $a^2 + b^2 - ab$ *et* $a + b$ *ne peuvent avoir d'autres diviseurs communs que les diviseurs de* 3.

2- *Plus généralement, démontrer que, étant donné un entier naturel n, les entiers* $a^2 + b^2 - nab$ *et* $a + b$ *ne peuvent avoir d'autres diviseurs communs que les diviseurs de* $n + 2$.

56. B-VI

Déterminer pour quels entiers relatifs n le nombre $\frac{n+17}{n-4}$ *est :*

1- *un entier relatif ;*

2- *le carré d'un nombre rationnel.*

Indications

1- Remarquer que $\frac{n+17}{n-4} = \frac{(n-4)+21}{n-4} = 1 + \frac{21}{n-4}$

2- Poser $\frac{n+17}{n-4} = \left(\frac{p}{q}\right)^2$ avec p et q entiers naturels premiers entre eux. Montrer alors que $n = 4 + \frac{21q^2}{p^2 - q^2}$ et remarquer que q^2 et $p^2 - q^2$ sont premiers entre eux.

57. B-VI

Soit un entier relatif n.

1- *Pour quelles valeurs de n le nombre* $\frac{n+8}{2n-5}$ *est-il un entier relatif ?*

2- *En supposant que la fraction* $\frac{n+8}{2n-5}$ *ne soit pas irréductible, quels peuvent être les diviseurs communs de* $n+8$ *et* $2n-5$ *?*

3- *Pour quelles valeurs de n cette fraction est-elle réductible ?*

58. C-IV Utilisation du petit théorème de Fermat

Soit un entier naturel premier p et un entier naturel x non nul premier avec p.

Le but de cet exercice est de démontrer qu'il existe un entier naturel n supérieur ou égal à 1 tel que :

pour $k \geq 1$, $\quad x^k \equiv 1 \pmod{p} \Leftrightarrow k$ est un multiple de n.

1° *Démontrer que l'ensemble des entiers k supérieurs ou égaux à 1 tels que* $x^k \equiv 1 \pmod{p}$ *est non vide.*

2° *Soit n le plus petit élément de cet ensemble et k un entier supérieur ou égal à 1 tel que* $x^k \equiv 1 \pmod{p}$.

Montrer que k est un multiple de n.

Indication

2° On pourra effectuer la division euclidienne de k par n et démontrer que le reste de cette division est non nul.

Remarques :

1° D'après le petit théorème de Fermat n divise $p-1$.

2° L'entier n est appelé ordre de l'entier naturel x modulo p.

59. C-IV Utilisation du petit théorème de Fermat

Soit un entier naturel x non nul et un entier naturel p premier qui divise $(x+1)^5 - x^5$.

1° *Démontrer que l'entier naturel p est différent de 2.*

2° *On pose* $y = (x+1)x^{p-2}$.

Montrer que $y^5 \equiv 1 \pmod{p}$ *et que* $y \not\equiv 1 \pmod{p}$.

En utilisant l'exercice précédent, prouver que p est de la forme $5k+1$ *où k est un entier naturel non nul.*

2° *.Soit un entier naturel n non nul, on considère, dans cette question, l'entier* $x = n!$.

Démontrer qu'il existe un entier naturel premier supérieur à n de la forme $5k+1$ *où k est un entier naturel.*

En déduire qu'il existe une infinité de nombres premiers de la forme $5k+1$.

60. C-IV Utilisation du petit théorème de Fermat

Soit un entier naturel p premier différent de 2. Démontrer que si il existe un entier naturel x strictement supérieur à 1 tel que p divise x^4+1 *alors* $p \equiv 1 \pmod 8$.

Indication

- Remarquer que p est nécessairement impair.
- Examiner alors les divers cas $p \equiv 3 \pmod 8$, $p \equiv 5 \pmod 8$, $p \equiv 7 \pmod 8$ pour les écarter à l'aide du petit théorème de Fermat.

61. C-IV Utilisation du petit théorème de Fermat (Généralisation de l'exercice précédent)

Soit un entier naturel p premier différent de 2. Démontrer que si il existe un entier naturel x strictement supérieur à 1 tel que p divise $x^{2^n}+1$ *alors* $p \equiv 1 \pmod{2^{n+1}}$.

Pour ce faire :

1° *Démontrer que* $x^{2^{n+1}} \equiv 1 \pmod p$.

2° *Déduire de l'exercice* **65** *que l'ordre de x (i. e. le plus petit élément naturel r non nul tel que* $x^r \equiv 1 \pmod p$*) est un diviseur de* 2^{n+1}.

3° *On note* $r = 2^k$ *avec* $0 \le k \le n+1$.

Montrer que k ne pas être inférieur ou égal à n.

En déduire que $r = 2^{n+1}$ *et que* $p = q2^{n+1}+1$ *(on pourra utiliser à nouveau le résultat de l'exercice* ***65****).*

62. C-V CARRÉS et RECTANGLES

Soit n carrés identiques. On se propose de déterminer le nombre R_n de rectangles (sans trou) différents que l'on peut former en les accolant tous.

Par exemple, avec 6 carrés on peut former 2 rectangles, un rectangle de 1 sur 6 et un rectangle de 2 sur 3.

1- *Calculer* R_{72}, R_{121}, R_{200}, R_{317} *et* R_{323}.

2- *Déterminer* R_n. *On distinguera 2 cas selon que n est un carré ou non.*

3- *Déterminer le plus petit nombre n de carrés tel qu'il y ait exactement 11 rectangles possibles.*

Indications

2- Considérer la fonction d qui à tout entier naturel non nul associe son nombre de diviseurs.

3- Comme précédemment on distinguera 2 cas.

63. C-V TRIPLETS PYTHAGORICIENS

Étant donné un entier naturel n non nul, nous nous proposons de déterminer les entiers naturels x et y tels que $x^2 - y^2 = n$ et de plus nous donnerons des interprétations arithmétiques et géométriques des résultats obtenus.

1- *Résoudre :*

- $x^2 - y^2 = 15$;
- $x^2 - y^2 = 13$;
- $x^2 - y^2 = 12$;
- $x^2 - y^2 = 22$;
- $x^2 - y^2 = 225$.

2-a) *Déterminer des conditions nécessaires et suffisantes pour que ce problème admette au moins une solution.*

b) *Démontrer que ce problème admet une solution unique lorsque n est premier et différent de 2.*

c) *Déterminer en fonction de n le nombre de solutions.*

3- Application arithmétique : ***un critère pour reconnaître qu'un nombre est premier.***

Démontrer que, étant donné un entier naturel n impair,

n est premier si et seulement si pour tout λ *élément de* $[\![0, \frac{n-1}{2} [\![$, $\lambda^2 + n$ *n'est pas le carré d'un entier.*

4- Application géométrique : ***étant donné un entier naturel b strictement supérieur à 2, peut-on trouver un triangle rectangle à côtés entiers dont un côté de l'angle droit mesure b ?***

Démontrer que, étant donné un entier naturel b strictement supérieur à 2, on peut trouver des entiers naturels a et c non uls tels que $a^2 = b^2 + c^2$, *c'est à dire tels que* $a^2 - c^2 = b^2$.

Remarque : *le nombre de solutions d'un tel problème est fini et le triplet* (a, b, c) *est appelé triplet pythagoricien.*

Indication

2- c On sera amené à distinguer pluseurs cas selon que n est un carré ou non.

64. C-V AUTRES FONCTIONS ARITHMÉTIQUES

En prolongement du paragraphe consacré à l'étude de quelques fonctions arithmétiques nous nous proposons de déterminer la somme $s_2(n)$ des carrés des diviseurs d'un entier naturel n non nul, la somme $s_3(n)$ des cubes des diviseurs d'un entier naturel n non nul, et de généraliser ce résultat.

1- *Calculer* $s_2(720)$, *puis* $s_2(n)$.

2- *Calculer* $s_3(720)$, *puis* $s_3(n)$.

3- *Calculer* $s_k(720)$, *puis* $s_k(n)$.

65. C-V

Nous proposons de déterminer un entier naturel n connaissant certaines caractéristiques de ses diviseurs.

On considère un nombre a dont la décomposition en produit de facteurs premiers est $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$.

On sait que le nombre $d(n)$ *de ses diviseurs est* $d(n) = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_r + 1)$.

1- *Déterminer n sachant que* $n = 5^{\alpha} \times 6^{\beta}$ *et que* $d(n) = 12$.

2- *On considère le nombre* $n = 490\ldots0$. *Combien doit-on mettre de zéros afin que* $d(n) = 27$.

3- *Trouver le plus petit nombre n tel que* $d(n) = 12$.

66. C-V

Déterminer l' entier naturel n vérifiant les conditions suivantes :

- *il admet deux diviseurs premiers distincts ;*
- *le nombre de ses diviseurs est* 6 ;
- *la somme de ses diviseurs est* 28.

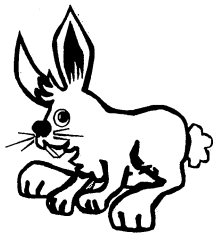
67. C-V

Déterminer les entiers naturels n vérifiant les conditions suivantes :

- *ses seuls diviseurs premiers sont* 2 *et* 5 *;*
- *le nombre de diviseurs de* n^2 *est le triple du nombre de diviseurs de n.*

68. D LA SUITE de FIBONACCI ou Pan Pan le lapin

L'origine de ce problème est le suivant : on enferme un couple de lapins adultes dans un endroit clos. Un couple de lapins adultes donne naissance au bout d'un mois à un nouveau couple de jeunes lapins. Un jeune lapin devient adulte en un mois et perpétue alors le processus de reproduction initié par ses parents, eux-mêmes ne restant pas inactifs.



Combien aura-t-on de couples de lapins à la fin de la première année ?

Mois	Nombre de couples de lapins adultes	Nombre de couples de lapins jeunes
0	1	0
1	1	1
2	2	1
3	3	2
4	5	3
5	8	5
6	13	8

En désignant par u_n avec $n \in \mathbb{N}$ le nombre de couples de lapins jeunes au cours du n-ième mois nous sommes amenés à étudier la suite suivante appelée suite de Fibonacci :

$$\begin{cases} u_0 = 0 \\ u_1 = 1 \\ \forall n \in \mathbb{N} - \{0\,;1\},\ u_n = u_{n-2} + u_{n-1} \end{cases}$$

1- *On considère deux termes consécutifs de cette suite (par exemple* 2584 *et* 4181*) en utilisant l'algorithme d'Euclide permettant de calculer le PGCD de deux nombres, montrer que ces deux nombres sont premiers entre eux.*

2- *Combien a-t-on effectué de divisions pour obtenir le résultat précédent (la condition d'arrêt est que le reste soit nul) ?*

3- *Soit des entiers naturels a et b non nuls.*
On recherche $PGCD(a,b)$ *par l'algorithme d'Euclide en commençant par la division de a par b et on note* $r_1, r_2, \ldots, r_n$ *les restes successifs avec* $r_n = 0$ *et* $r_{n-1} \neq 0$. *On convient d'écrire* $b = r_0$.
On suppose que b ne divise pas a, montrer alors que $r_k \geq r_{k+1} + r_{k+2}$ *pour* $k \in [\![0, n-2]\!]$ *; en déduire que* $b \geq u_n$ *où* u_n *est le* $(n+1)$*-ième terme de la suite de Fibonacci.*

4- *En déduire que lorsque* $0 < b < u_n$ *(où* u_n *est le* $(n+1)$*-ième terme de la suite de Fibonacci) il faut* ***au plus*** *n divisions pour trouver* $PGCD(a,b)$ *et ce, quelle que soit la valeur de a.*
Remarque : *lorsque* $b = u_n$ *et* $a = u_{n+1}$ *il faut* $n+1$ *divisions pour obtenir* $PGCD(a\,;b)$ *(voir question* ***2****).*

69. S NOMBRES DE MERSENNE ET DE FERMAT

Peut-on trouver une expression donnant tous les nombres premiers ou tout au moins une infinité de nombres premiers ?

Nous allons considérer les nombres de la forme a^n+1 et a^n-1 et établir des conditions nécessaires sur a et n afin que de tels nombres soient premiers. Ceci nous conduira aux nombres de Fermat et Mersenne.

Soit des entiers naturels a et n, $a \geq 2$ et n non nul.

1- a) *Démontrer que a^n-1 premier $\Rightarrow a=2$.*

b) *Donner une valeur de n telle que 2^n-1 ne soit pas premier.*

c) *Démontrer que 2^n-1 premier $\Rightarrow n$ premier.*

On appelle nombres de Mersenne les nombres M_n tels que $M_n=2^n-1$ avec n premier.

Calculer M_2, M_3, M_5, M_7 et M_{11}.

Tous les nombres de Mersenne sont-ils premiers ?

2- a) *Démontrer que a^n+1 premier $\Rightarrow n=2^k$.*

b) *Démontrer que a^n+1 premier $\Rightarrow a$ pair.*

Lorsque $a=2$ de tels nombres sont appelés nombres de Fermat, on les note $F_n=2^{2^n}+1$.

Calculer F_0, F_1, F_2 et F_3.

c) *Démontrer que quels que soit les entiers naturels m et n, $m \neq n$, F_m et F_n sont premiers entre eux.*

Remarque : *Fermat pensait que de tels nombres étaient tous premiers, Euler a démontré que*
$F_5=4294967297=641\times 6700417$

A titre curiosité, $F_6=18446744073709551617=274177\times 67280421310721$

Les seuls nombres de Fermat premiers connus sont F_0, F_1, F_2, F_3 et F_4.

Le nombre de Fermat le plus grand dont un diviseur est connu est F_{23471}, il a comme diviseur $5\times 2^{23473}+1$.

Indications

1- a) Factoriser a^n-1.

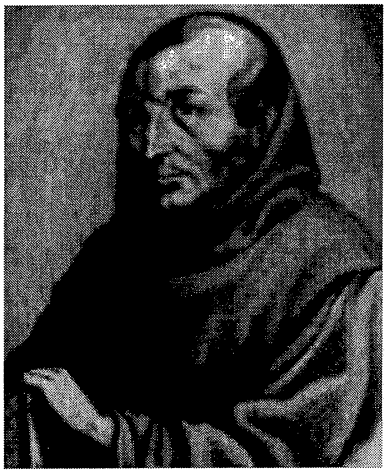
c) Poser $n=pq$ et factoriser $2^{pq}-1$.

2- c) Supposons, $n<m$,

(p divise F_n et divise F_m) $\Rightarrow 0 \equiv (-1)^{2^{m-n}}+1 \pmod p$

$\Rightarrow 0 \equiv 2 \pmod p$

$\Rightarrow p=2$ (Absurde)



Marin Mersenne, né à La Soulière (Maine) en 1588 et mort à Paris en 1648. Théologien, mathématicien et philosophe qui était très ami de Descartes. Il était en relation constante avec Fermat.

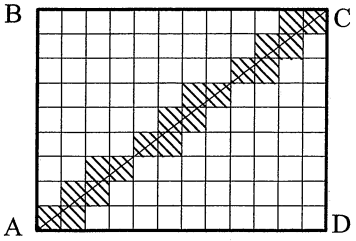
70. S Diagonale dans un rectangle

On considère un rectangle ABCD dont les longueurs des côtés sont m et n, m et n étant des entiers naturels non nuls. On découpe ce rectangle en carrés de côtés 1 (voir dessin).
Combien la diagonale $[A,C]$ traverse-elle de carrés ?

Exemple:

Exemple:

Ce rectangle est de dimension 9 sur 12.
La diagonale $[A,C]$ traverse tous les carrés hachurés soit 18 carrés.

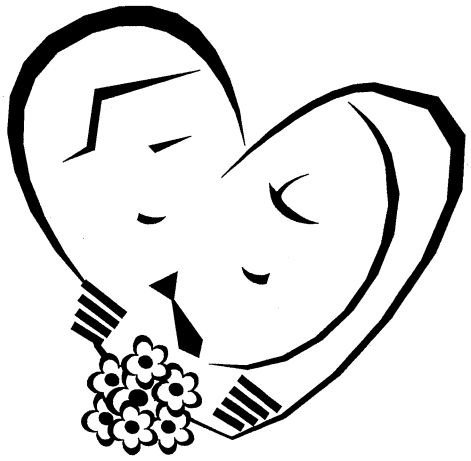


$18 = 9 + 12 - \boldsymbol{pgcd}(9,12)$

Indication

La diagonale $[A,C]$ traverse $(m+n-PGCD(m,n))$ carrés

71. S NOMBRES AMIABLES



1- *On appelle diviseur strict d'un entier naturel n tout entier naturel diviseur de n autre que n. Déterminer les entiers naturels diviseurs stricts de* 220.

2- *On appelle nombres amiables deux entiers naturels tels que chacun d'eux soit égal à la somme des diviseurs stricts de l'autre. Vérifier que* 220 *et* 284 *sont amiables.*

3- a) *On appelle nombre parfait tout nombre qui est amiable avec lui-même.*

Le nombre 28 *est-il parfait ?*

Déterminer un entier naturel p premier tel que le nombre $2^4 p$ soit parfait.

b) *Plus généralement, soit des entiers naturels n et p, p premier, exprimer une condition nécessaire sur p, en fonction de n, afin que $2^n p$ soit parfait ? Donner la liste des nombres parfaits de cette forme pour $n \leq 20$.*

Nous venons d'établir le résultat suivant :

Étant donné un nombre de Mersenne M_n (voir exercice " Nombres de Fermat et de Mersenne "),

Si M_n est premier alors $2^{n-1} M_n$ est parfait.

On ne sait pas s'il existe des nombres parfaits impairs.

4- Montrer qu'un carré n'est jamais un nombre parfait.

72. S POLYGONES

Soit des entiers naturels n et p tels que $1 \leq p < n$.

Soit P un polygone de n sommets $A_0, A_1, \ldots, A_{n-1}$. *On joint de p en p dans un sens de rotation fixé, les sommets du polygone P en partant de* A_0.

1- *Démontrer que la ligne polygonale obtenue se ferme en* A_0. *On note* P_p *le polygone ainsi obtenu.*

2- *Démontrer que le nombre m de sommets du polygone* P_p *vérifie* $m = \frac{1}{p} PPCM(n\ ;\ p) = \frac{n}{PGCD(n\ ;\ p)}$.

3- *En déduire que les sommets de P sont des sommets de* P_p *si et seulement si n et p sont premiers entre eux.*

4- *Lorsque p varie de 1 à n, combien fabrique-t-on ainsi de polygones* P_p *dont les sommets sont ceux de P ?*

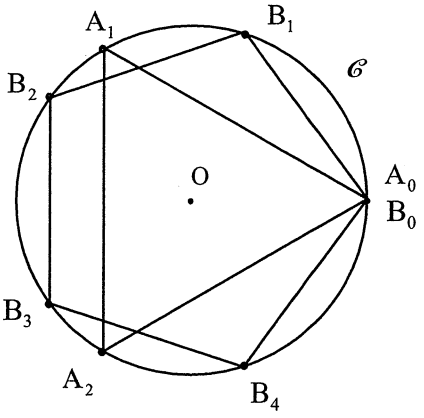
Indications

1- On justifiera que mp est un multiple de n. Il pourra être commode d'utiliser les congruences modulo n.

2- La réponse est $\varphi(n)$ avec φ indicateur d'Euler.

73. S TRIANGLE ÉQUILATÉRAL et PENTAGONE

Gauss a démontré que les seuls polygones réguliers constructibles à la règle et au compas sont des polygones de n côtés avec : $n = 2^p$ ou $n = 2^p \times F_{p_1} \times \ldots \times F_{p_q}$ avec F_{p_i} nombres de Fermat premiers et 2 à 2 distincts. Nous nous proposons d'illustrer ceci à travers un exemple.



1- *Soit la figure ci-contre,* $A_0A_1A_2$ *est un triangle équilatéral inscrit dans le cercle* $\mathcal{C}$ *de centre O,* $B_0B_1B_2B_3B_4$ *(avec* $A_0 = B_0$*) est un pentagone régulier convexe inscrit dans le cercle* $\mathcal{C}$ *de centre O.*

Montrer qu'il existe (i, j) *élément de* $[\![0\,;2]\!] \times [\![0\,;4]\!]$ *tel que* $[A_i, B_j]$ *soit le côté d'un polygone régulier convexe de 15 côtés inscrit dans le cercle* $\mathcal{C}$.

2- *Soit un cercle* $\mathcal{C}$ *de centre O et A un point de cercle. Pour tout entier 1 strictement supérieur à 1, on considère le polygone* P_l, *à l sommets, inscrit dans le cercle* $\mathcal{C}$, *A étant l'un de ses sommets.*

Soit des entiers naturels m et n strictement supérieurs à 1, on considère les polygones P_m *et* P_n *dont on note respectivement les sommets* $A_0, A_1, \ldots, A_{m-1}$ *et* $B_0, B_1, \ldots, B_{n-1}$ *avec* $A_0 = B_0 = A$.

Montrer qu'il existe (i, j) *élément de* $[\![0\,;m-1]\!] \times [\![0\,;n-1]\!]$ *tel que* $[A_i, B_j]$ *soit le côté d'un polygone régulier convexe de k côtés inscrit dans le cercle* $\mathcal{C}$, *où* $k = PPCM(m\,;n)$.

Indication

On pourra utiliser avec profit le théorème de Bézout.

74. S RATIONNELS ET IRRATIONNELS

Soit le polynôme $P(x)=x^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\ldots+a_1x+a_0$ *dont les coefficients sont des entiers relatifs.*

1- *Montrer que les racines réelles de P(x) sont soit des entiers, soit des irrationnels.*

2- *En déduire que* $\sqrt{2}$, $\sqrt{3}$ *et* $\sqrt{2}+\sqrt{3}$ *sont des nombres irrationnels.*

Indication

2- Déterminer des polynômes admettant respectivement comme racines, $\sqrt{2}$, $\sqrt{3}$ *et* $\sqrt{2}+\sqrt{3}$

75. S

1- *Soit le polynôme* $P(x)=a_nx^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\ldots+a_1x+a_0$ *avec* $a_n\neq 0$ *et* $a_0\neq 0$ *dont les coefficients sont des entiers relatifs.*

Montrer que si $\frac{p}{q}$ *(p et q premiers entre eux) est une racine de P, alors p divise* a_0 *et q divise* a_n.

2- ***Applications.***

a) *Montrer que le polynôme* $P(x)=5x^4+15x^2-30x-3$ *n'a pas de racine rationnelle.*

b) *Trouver les racines rationnelles du polynôme* $P(x)=5x^4+3x^3-25x^2+20x-3$.

76. S DIVERS (entraînement olympiades)

Étant donné des entiers naturels *m* et *n* non nuls, on considère le nombre $a=36^n-5^m$.
On cherche à déterminer *m* et *n* afin que $|a|$ soit minimum.

1- *Montrer que le chiffre des unités de* $|a|$ *ne peut être que* 1 *ou* 9.

2-a) *Montrer que* $|a|=9$ *est impossible*

b) *Montrer que* $|a|=1$ *est impossible.*

3-a) *Déduire de la question précédente que* $|a|\geq 11$.

b) *En déduire le minimum de* $|a|$.

Indications

2-a) Utiliser des congruences modulo 3.

2-b) Utiliser des congruences modulo 4 et modulo 5.

77. S

Démontrer que pour tout entier naturel n, le nombre $n(n+1)(n+2)(n+3)$ *est divisible par* 24.

78. S

Soit un entier naturel n et l'entier naturel $N = n^4 + n^2 + 1$.

1- *Démontrer que N est premier si et seulement si* $n = 1$.

2- *On suppose que* $n \neq 1$, *montrer que N n'est pas une puissance d'un nombre premier.*

Indications

$n^4 + n^2 + 1 = (n^2 - n + 1)(n^2 + n + 1)$.

On remarquera que tout diviseur commun à $n^2 - n + 1$ et $n^2 + n + 1$ est un nombre impair qui divise $2n$.

79. S

Déterminer les entiers relatifs n tels que l'entier naturel $N = n^2 - 3n + 6$ *soit divisible par* 5.

80. S

Soit un entier naturel n strictement supérieur à 1 *et deux entiers naturels m et n tels que* $m > n$.

On note q et r le quotient et le reste de la division euclidienne de m par n et on considère les entiers naturels $M = a^m - 1$, $N = a^n - 1$ *et* $R = a^r - 1$.

1- *Montrer que* $PGCD(M, N) = PGCD(N, R)$.

2- *En déduire* $PGCD(M, N)$.

3- ***Application numérique :*** *calculer* $PGCD(M, N)$ *avec* $M = 99\ldots9$ *(M s'écrit avec* 4680 *chiffres) et* $N = 99\ldots9$ *(M s'écrit avec* 2520 *chiffres).*

81. S

Soit des entiers relatifs a et b.

On considère les entiers naturels $A = 11a + 2b$ *et* $B = 18a + 5b$.

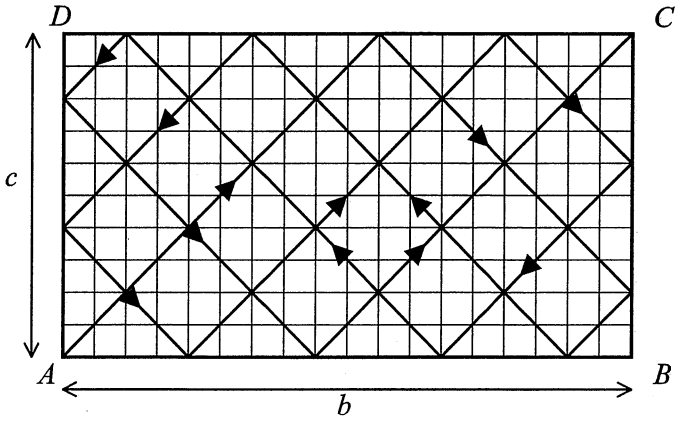
1- *Montrer que* 19 *divise A si et seulement si* 19 *divise B.*

2- *On suppose a et b premiers entre eux, montrer que le plus grand commun diviseur de A et B est 1 ou 19.*

3-a) *Donner deux entiers naturels a et b premiers entre eux tels que* $PGCD(A, B) = 1$

b) *Donner deux entiers naturels a et b premiers entre eux tels que* $PGCD(A, B) = 19$

82. S



Le rectangle ci-contre est formé d'un nombre entier de petits carrés.

Considérons le chemin partant du coin A et traversant les carrés selon leurs diagonales en ligne droite. Lorsque le chemin arrive sur un bord il tourne à angle droit vers l'intérieur du rectangle et continue ainsi jusqu'à ce qu'il arrive dans un autre coin du rectangle.

Appelons b le nombre de carrés bordant un coté et c le nombre de ceux bordant l'autre coté.

Deux questions se posent :

(i) *arrive-t-on à un sommet du rectangle, quel que soit le rectangle du départ ?*

(ii) *quel est le nombre de carrés traversés lorsque pour la première fois on arrive à un sommet ?*

1° a) *On considère* $b=2$ *et* $c=3$. *Vérifier que le chemin construit aboutit bien dans un coin du rectangle et compter le nombre m de carrés traversés.*

b) *Reprendre la question précédente pour* $b=4$ *et* $c=6$, *puis avec* $b=6$ *et* $c=8$.

c) *Que représente le nombre m pour les couples* (b,c) *précédents ?*

2° *Soit l un entier naturel, on note M le point atteint après avoir traversé, selon le tracé donné, l carrés.*

a) *Montrer que M appartient à* $[A,D]\cup[B,C]$ *si et seulement si b divise l.*

b) *Montrer que M est l'un des sommets du rectangle si et seulement si M est un multiple commun à b et c.*

c) *Répondre aux questions* ***(i)*** *et* ***(ii)*** *posées.*

3° a) *En gardant les notations précédentes montrer que M appartient à* $[A,D]$ *si et seulement si* $2b$ *divise l.*

b) *Préciser dans les cas suivants le nombre m de cases traversées et le premier sommet atteint :*

- $b=6$ *et* $c=8$;
- $b=28$ *et* $c=35$;
- $b=15$ *et* $c=21$.

83. S

Une récurrence pas très « classique ».

Une tablette de chocolat est formée de ab petits carrés , a et b sont des entiers naturels non nuls.

On casse la tablette en deux en coupant le long d'une ligne droite de séparation des carrés, puis on recommence l'opération jusqu'à ce que tous les carrés soit séparés.

On se propose de calculer en fonction de a et b le nombre d'opérations nécessaires.

1- *Calculer pour les couples suivants* (a,b) *le nombre d'opérations nécessaire en fonction de a et b et de la manière de procéder :* $(a,b)=(2,3)$, $(a,b)=(1,5)$, $(a,b)=(4,3)$, $(a,b)=(2,6)$ *?*

Sur ces exemples peut-on dire que le nombre cherché dépend de la manière de procéder ?

Peut-on dire qu'il dépend exclusivement du couple (a,b) *?*

Faites une conjecture sur le nombre d'opérations.

2- *Choisissez une hypothèse de récurrence permettant de prouver cette conjecture .*

84. S

Soit n carrés identiques. Combien de rectangles différents (sans trous) utilisant tous les carrés peut-on former en les accolant ?

1) Déterminer ce nombre pour $n \in \{200, 72, 323, 317\}$

2) Déterminer le plus petit nombre n de carrés tel qu'il y ait exactement 11 rectangles possibles.

85. S

Existe-t-il des nombres dont le produit de leur somme par leur produit égale 29400 *?*

86. S

Démontrer que tout entier naturel divise une puissance de 10 *ou une différence non nulle de deux puissances de* 10.

87. S

Soit b une base de numération. Pour quelles valeurs de b existe-t-il trois entiers α, β *et* γ *tels que* $1 \le \alpha < b$, $1 \le \beta < b$ *et* $1 \le \gamma < b$, *vérifiant dans cette base b* $\overline{\alpha\alpha\beta\beta} = \overline{\gamma\gamma} \times \overline{\gamma\gamma}$ *?*

1. *Montrer que pour* $b = 2$ *ou* $b = 3$ *cela n'est pas possible.*

2. *Soit une valeur de b pour laquelle la propriété est vraie. Montrer alors que* $b+1$ *divise* $\alpha + \beta$ *, en déduire la valeur de* $\alpha + \beta$ *en fonction de b et calculer* γ^2 *en fonction de* α *et b.*

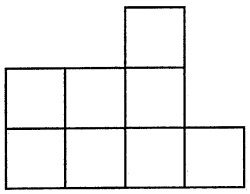
Comparer γ, $\sqrt{b}$ *et* $b-2$ *puis en déduire que* $b \ge 5$.

3. *Pour* $b \ge 5$ *montrer que l'on a toujours une solution avec* $\beta = 4$.

88. S

Avec n cubes on forme un mur de la façon suivante : le mur n'a pas de trous, ni de surplomb, il est situé dans le même plan vertical et chaque cube des rangées supérieures est exactement posé sur un seul cube de la rangée en dessous comme dans l'exemple ci-contre avec 8 *cubes.*

Combien de murs différents de ce type pouvons nous faire avec n cubes ?



1- *Calculer ce nombre pour* $n = 3$ *et* $n = 4$.

2- *À chaque mur on associe le nombre écrit en base deux de la manière suivante. Pour chaque cube de la rangée inférieure, en allant de gauche à droite, on écrit un « 1 » suivi d'autant de « 0 » que de cubes au dessus de lui. Pour l'exemple au dessus cela donne* $\overline{10101001}$.

3- *En déduire la solution du problème posé.*

89. S

Un problème inspiré par une colle posée par une charmante collègue, issue de je ne sais où (la colle et non pas la collègue) : déterminer le chiffre des unités de l'entier le plus proche de $\frac{10^{1992}}{10^{97}+7}$.

1- *Soit* $a=10^{97}$, $b=7$ *et* n *un entier . Montrer que* $n a^k b^p \equiv -n a^{k-1} b^{p+1} \ [a+b]$

En déduire le reste de la division euclidienne de 10^{1992} *par* $10^{97}+7$.

Donner une expression à l'aide d'une somme du quotient de la division euclidienne de 10^{1992} *par* $10^{97}+7$ *et répondre à la question posée.*

2- *Par une méthode analogue déterminer le chiffre des unités du nombre entier le plus proche de* $\frac{10^{1998}}{10^{54}-7}$.

90. S Algorithme pour déterminer des nombres premiers

Construction d'un tableau infini

Ligne	1er terme	Raison	1er terme	2ème terme	3ème terme	4ème terme	5ème terme	etc
1	1×2	$1+2$	2	5	8	11	14	...
2	2×3	$2+3$	6	11	16	21	26	...
3	3×4	$3+4$	12	19	26	33	39	...
n	$n(n+1)$	$2n+1$	n^2+1	n^2+2n+2	n^2+4n+3	n^2+6n+4	n^2+8n+5	

Soit τ *l'ensemble des nombres figurant dans ce tableau.*

Montrer que pour tout entier naturel n non nul, les propositions suivantes sont équivalentes :

i) $4n+1$ *est un nombre premier.*

ii) $n \notin \tau$.

Indication

Raisonner par contraposées.

91. S

1- *Soit un entier naturel n, on considère le nombre* 7^{n^2}.

On note u_n *le chiffre des unités de ce nombre écrit en base dix.*

Démontrer que la suite $(u_n)_{n\in\mathbb{N}}$ *est périodique.*

2- ***Généralisation*** *:soit un polynôme P à coefficients dans* $\mathbb{N}$ *et un entier naturel n, on considère le nombre* $7^{P(n)}$.

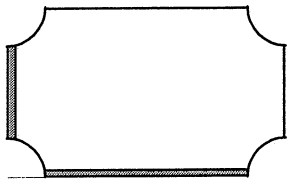
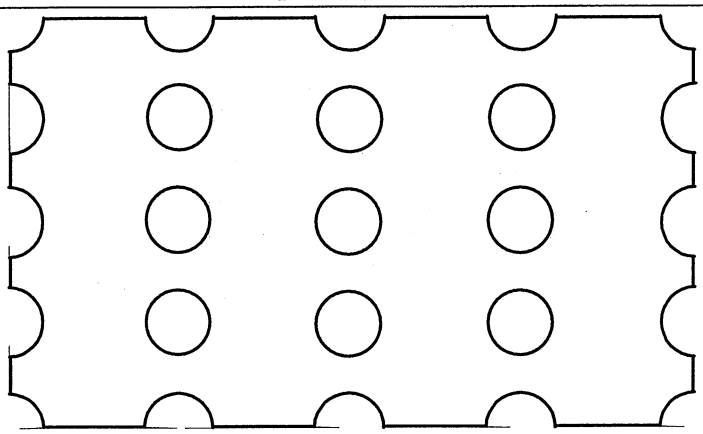
On note v_n *le chiffre des unités de ce nombre écrit en base dix.*

Que peut-on dire de la suite $(v_n)_{n\in\mathbb{N}}$ *?*

92. S Tiré d'un Kangourou

On plie soigneusement en 2 une feuille de papier rectangulaire, n fois de suite, en pliant à chaque fois suivant un pli perpendiculaire au précédent. Après cela on déchire les 4 coins du rectangle de papier obtenu, puis on déplie la feuille.

Combien de vrais trous voit-on alors à l'intérieur de la feuille ?

On plie et on déchire	*Après dépliage*
	

93. S Les cartes qu'on jette

On prend dans la main n cartes numérotées de 1 à n. Les cartes sont rangées dans cet ordre et la carte du dessus est numérotée 1.

On prend la carte du dessus on la met sous le paquet, on jette maintenant celle qui est dessus, et on continue ainsi jusqu'à ce qu'il nous reste une seule carte en main.

Quel est son numéro ?

Exemple prenons 6 cartes :

Au départ : [1] [2] [3] [4] [5] [6]

La carte [1] passe dessous : [2] [3] [4] [5] [6] [1]

On jette la carte [2] : [3] [4] [5] [6] [1]

La carte [3] passe dessous : [4] [5] [6] [1] [3]

On jette la carte [4] : [5] [6] [1] [3]

La carte [5] passe dessous : [6] [1] [3] [5]

On jette la carte [6] : [1] [3] [5]

La carte [1] passe dessous : [3] [5] [1]

On jette la carte [3] : [5] [1]

La carte [5] passe dessous : [1] [5]

On jette la carte [1] : [5]

C'est la carte [5] qui nous reste dans la main.

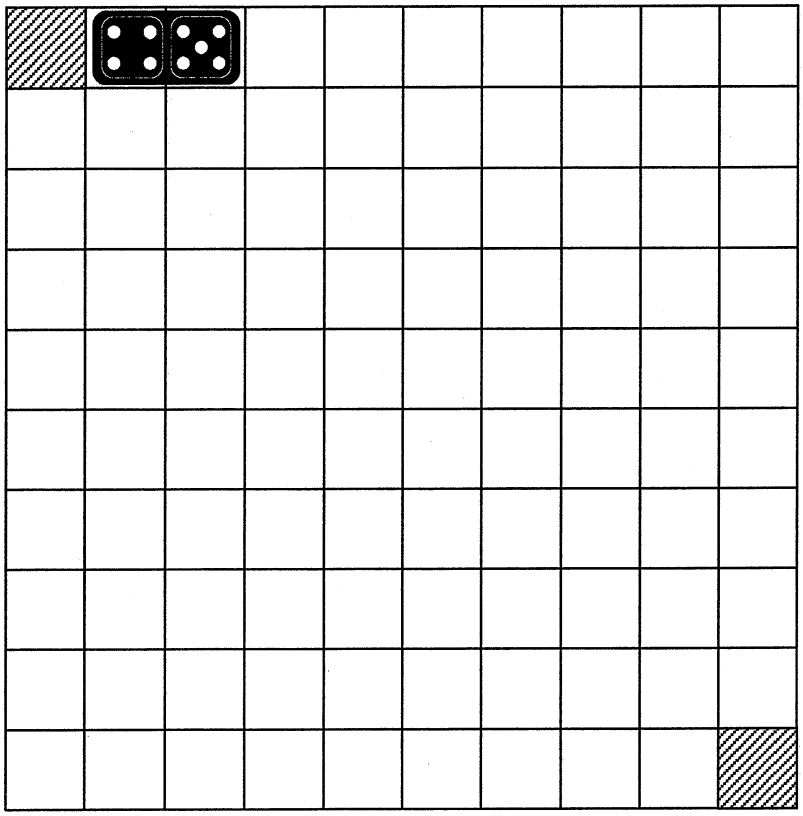
1- *Que se passe-t-il avec un jeu de 32 cartes ?*

2- *Que se passe-t-il avec un jeu de 52 cartes ?*

94. S Le damier.

On considère un damier

On supprime les deux cases hachurées.
On dispose de 98 *dominos permettant de couvrir deux cases exactement.*



Peut-on paver tout le damier ?

Indications
Colorier le damier

IREM d'Aquitaine

Groupe de Géométrie et d'Arithmétique

Titre : Initiation à l'Arithmétique

Auteurs

BOUSCASSE Jean-Marie, CHAUMET Marie-Claude, DAMEY Pierre, GOUTEYRON Antoine, GOUTEYRON Claire, POMÈS Roland, PINET Bernard, PUYOU Jacques, ROBERT Yves.

Public concerné :

- ☞ enseignants des lycées ;
- ☞ formateurs IUFM ;
- ☞ préparataires aux CAPES internes et externes de mathématiques.

Résumé

Cet ouvrage est consacré à l'arithmétique élémentaire. Sa rédaction a été motivée par la nouvelle introduction de cette partie des mathématiques dans l'enseignement dispensé au lycée. Il présente les notions générales de l'arithmétique dans $\mathbb{N}$, avec les seuls outils de la classe de terminale scientifique, puis dans $\mathbb{Z}$, en dépassant un peu le cadre des programmes du second cycle pour établir une liaison avec l'enseignement post-baccalauréat. Il développe des exemples d'utilisation de ces notions : étude de l'ensemble $\mathbb{Z}/n\mathbb{Z}$, étude de quelques fonctions arithmétiques, problèmes de codage...

Il est complété par un recueil d'exercices pour la plupart originaux.

Mots clefs

Arithmétique - Algorithme - Codages - Congruences - Décomposition en produit de facteurs premiers - Diviseurs - Division euclidienne - Entiers naturels - Entiers relatifs - Nombres premiers - PGCD - PPCM - Bézout - Euclide - Fermat - Gauss.

Publication

IREM d'Aquitaine
40 rue Lamartine
33400 TALENCE

I.S.B.N. : 2-85633-028-9
ISBN : 978-2-85633-028-9
EAN : 9782856330289