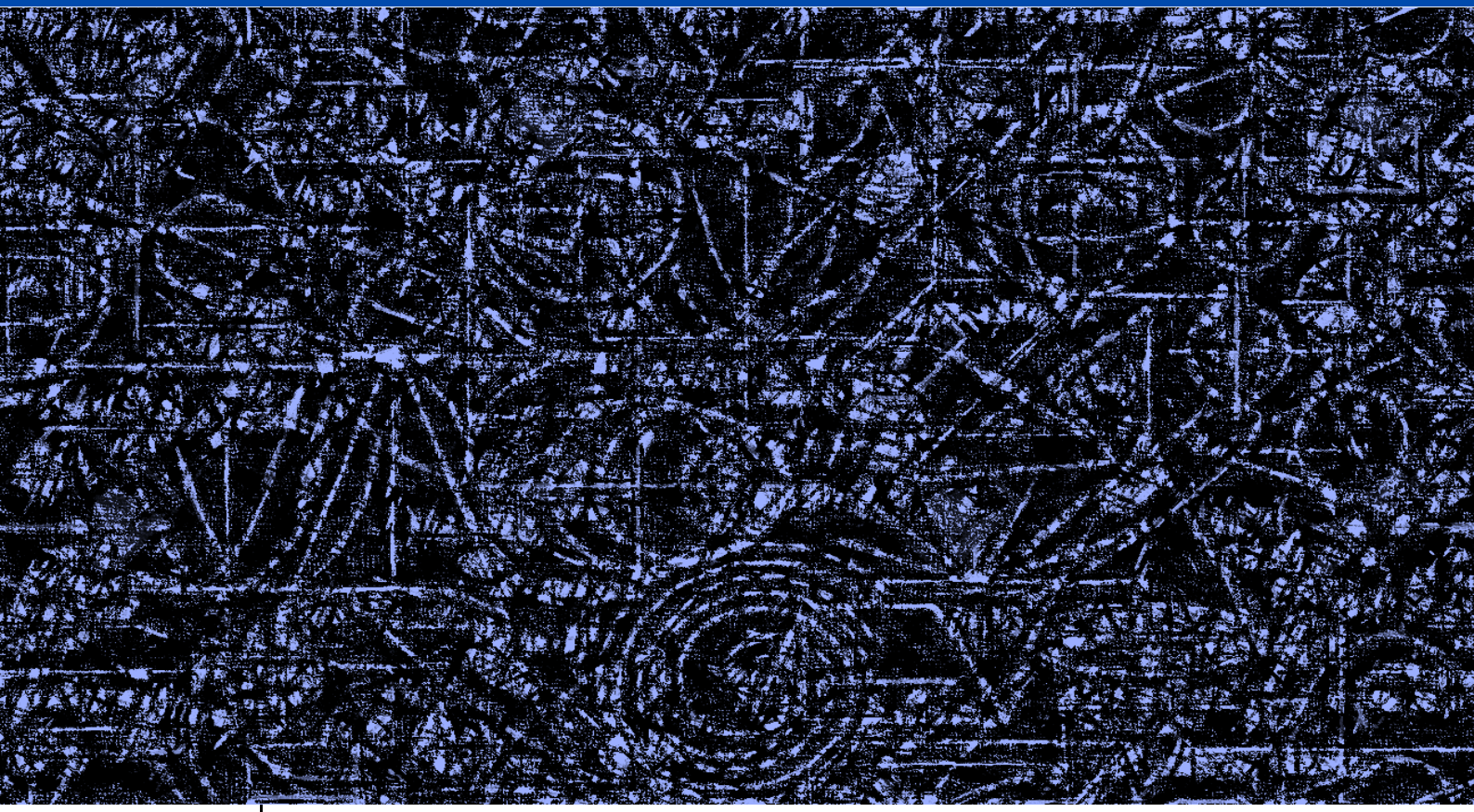
Arithmétique dans $\mathbb{Z}$: divisibilité et congruences

9



Introduction

L'arithmétique est une branche des mathématiques qui étudie les nombres entiers et rationnels. Mais les outils modernes permettent d'étendre le champ d'application de l'arithmétique.
Conformément aux objectifs fixés pour la licence 1, nous nous limitons uniquement aux entiers relatifs et aux polynômes (les polynômes sont étudiés dans les **chapitres 13**, **14** et **15**). Le lien avec les structures algébriques se fera dans le cours de licence 2 (**chapitre 1** du livre licence 2 – algèbre).

Prérequis

- Construction de $\mathbb{Z}$ (**chapitre 8**)

Objectifs du chapitre

Le théorème de la division euclidienne a déjà été abordé pour déterminer les sous-groupes additifs de $\mathbb{Z}$.

- Etudier la divisibilité des entiers relatifs
- Revoir le **théorème de la division euclidienne**
- Etudier les **systèmes de numération** (écriture d'un entier naturel dans une base donnée)
- Etudier la **congruence** des entiers relatifs
- Etudier les **critères de divisibilité** (par 2, 3, 4, 5, 7, 8, 9, 10 et 11)
- Introduire l'anneau $\mathbb{Z}/n\mathbb{Z}$

Le cours du chapitre 9

1 Multiples et diviseurs

A Définitions

Vous connaissez parfaitement ces notions. Redéfinissons-les.

Définition 1

Soient a et b deux entiers relatifs.
Dire que a **divise** b signifie qu'il existe un entier relatif k tel que $b = ak$.

Exemple

-6 divise 24 car $24 = (-6)\times(-4)$.

Remarques

Par exemple, $6 \mid 24$.

1. Pour signifier que a divise b, on écrit « $a \mid b$ » (attention à l'ordre).

2. On dit aussi que a est un **diviseur** de b, ou que b est un **multiple** de a ou encore que b est **divisible** par a.

Donc : $\forall a \in \mathbb{Z}, a \mid 0$.

3. Il est clair que 0 est multiple de tout entier relatif puisque pour tout entier relatif a : $0 = a \times 0$. Cette dernière égalité permet aussi de constater que 0 est divisible par 0.

Attention à ne pas confondre avec la division qui elle n'est pas permise avec l'entier 0.

4. Quel que soit l'entier relatif a, on a : $a = a \times 1 = (-a)\times(-1)$. Donc tout entier relatif est divisible par 1, par lui-même, par -1 et par son opposé.

Donc $a\mathbb{Z} = \{b \in \mathbb{Z}, \exists k \in \mathbb{Z}, b = ak\}$.

5. Pour tout $a \in \mathbb{Z}$, on notera $a\mathbb{Z}$ l'ensemble des multiples de a.

Définition 2

Soit a un entier relatif.
1) Dire que a est **pair** signifie que $2 \mid a$ 2) Dire que a est **impair** signifie que a n'est pas pair.

Autrement dit, a est pair quand il est divisible par 2.

B Premières conséquences

Théorème 1

$$\forall a \in \mathbb{Z}, 0 \mid a \Leftrightarrow a = 0.$$

Autrement dit, 0 ne divise aucun entier relatif non nul (il se divise seulement).

Preuve

($\Rightarrow$) Soit a un relatif tel que $0 \mid a$.
Par définition, il existe un entier relatif k tel que $a = 0 \times k$.
Il vient donc que $a = 0$.
($\Leftarrow$) Evident. □

Théorème 2

$$\forall (a,b) \in \mathbb{Z}\times\mathbb{Z}, a \mid b \Leftrightarrow a \mid -b \Leftrightarrow -a \mid b \Leftrightarrow -a \mid -b.$$

Le **théorème 2** est pratique. Quand un entier dispose d'un diviseur, alors l'opposé de ce diviseur est aussi un diviseur de cet entier. De même, lorsqu'un entier dispose d'un multiple, l'opposé de ce multiple et encore un multiple de l'entier.

Preuve

Considérons a et b des entiers relatifs.
On dispose des équivalences suivantes :

$$a \mid b \Leftrightarrow \exists k \in \mathbb{Z}, b = ak \Leftrightarrow \exists k \in \mathbb{Z}, b = -a\times(-k) \Leftrightarrow \exists k \in \mathbb{Z}, -b = a\times(-k) \Leftrightarrow \exists k \in \mathbb{Z}, -b = -a \times k.$$

On a ainsi les équivalences souhaitées. □

Théorème 3

La relation « $\mid$ » est une relation d'ordre dans $\mathbb{N}$.

On rappelle qu'une relation d'ordre est à la fois réflexive, antisymétrique et transitive.

Preuve

1) Pour tout entier naturel a, $a \mid a$, donc la relation « divise » est réflexive.

2) Soient a et b deux entiers naturels tels que $a \mid b$ et $b \mid a$.

Traitons un cas gênant.
Si $a = 0$, alors $b = 0$ (**théorème 1**). On suppose désormais que a n'est pas nul.

Il existe alors un couple $(k,l) \in \mathbb{N}^2$ tel que $a = bk$ et $b = al$.

Utilisation de la régularité de la multiplication.

Il vient alors que $a = alk$, soit $lk = 1$, soit encore $l = k = 1$.
Finalement, $a = b$ et la relation « divise » est antisymétrique.
3) Soient a, b et c des entiers naturels tels que $a \mid b$ et $b \mid c$.
Il existe alors un couple $(k, l) \in \mathbb{N}^2$ tel que $b = ak$ et $c = bl$.
Il vient alors que $c = akl$, soit, puisque $kl \in \mathbb{N}$, $a \mid c$ et ainsi la relation « divise » est transitive. □

Remarques
1. On vient de voir que le couple $(\mathbb{N}, |)$ est un ensemble ordonné. Mais la relation « divise » n'est pas totale, car par exemple on n'a ni $2 \mid 3$, ni $3 \mid 2$.

Les vérifications sont immédiates.

Par ailleurs, par cette relation, 0 est le plus grand élément et 1 le plus petit élément de $\mathbb{N}$.
2. Attention, le couple $(\mathbb{Z}, |)$ n'est pas un ensemble ordonné. En effet, la relation « divise » n'est pas antisymétrique (le lecteur cherchera pourquoi).
On peut seulement dire que la relation « divise » est un **préordre** sur $\mathbb{Z}$, c'est-à-dire une relation qui est réflexive et transitive.

Le **théorème 4** est plus parlant quand il est énoncé dans $\mathbb{N}$:
$\forall (a, b) \in \mathbb{N} \times \mathbb{N}^*, a \mid b \Rightarrow a \leqslant b$.
Il dit intuitivement que si a divise b, alors b est plus grand que a. Mais attention, b doit être non nul.

Théorème 4

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}^*, a \mid b \Rightarrow |a| \leqslant |b|.$$

Preuve
Supposons que $a \mid b$.
Il existe un entier relatif k tel que $b = ak$.
Donc, $|b| = |ak|$, soit $|b| = |a| \times |k|$.
Comme b n'est pas nul, il en est de même pour k et de sa valeur absolue.
Ainsi, de l'inégalité $1 \leqslant |k|$, on en déduit que $|a| \leqslant |k| \times |a|$, soit $|a| \leqslant |b|$. □

Remarques
1. La contraposée du **théorème 4** nous fournit un moyen simple pour montrer qu'un entier ne divise pas un autre.

La contraposée donne :
$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}^*, |b| < |a| \Rightarrow \neg(a \mid b)$.

Par exemple, il est clair que 734 n'est pas un multiple de 1470 car $734 < 1470$.
2. Dans les hypothèses du **théorème 4**, on impose que b ne soit pas nul. C'est normal car par exemple, $1 \mid 0$ mais on n'a pas $1 \leqslant 0$.
3. Attention à ne pas oublier les valeurs absolues ! En effet, $2 \mid -6$ et pourtant on n'a pas $2 \leqslant -6$ ...

C Propriétés de la divisibilité

Théorème 5

$$\forall (a, b, c) \in \mathbb{Z}^3, a \mid b \Rightarrow a \mid bc.$$

Autrement dit, quand a divise b, alors tout multiple de b est encore un multiple de a.

Preuve
Supposons que $a \mid b$.
Il existe alors un entier relatif k tel que $b = ak$.
La dernière égalité entraîne que $bc = akc$, c'est-à-dire, puisque $kc \in \mathbb{Z}$, $a \mid bc$. □

Remarque
Le lecteur est invité à expliquer pourquoi la réciproque du **théorème 5** est fausse.

Attention, le **théorème 6** ne fonctionne guère avec l'addition (trouver un contre-exemple est très facile).

Théorème 6

$$\forall (a, b, c, d) \in \mathbb{Z}^4, \begin{cases} a \mid b \\ c \mid d \end{cases} \Rightarrow ac \mid bd.$$

Preuve
Supposons que $a \mid b$ et $c \mid d$.
Il existe alors un couple $(k, l) \in \mathbb{Z}^2$ tel que $b = ak$ et $d = cl$.
Il vient alors que $bd = (ak)(cl) = (ac)(kl)$, c'est-à-dire, puisque $kl \in \mathbb{Z}$, $ac \mid bd$. □

Remarque

Le lecteur est invité à expliquer pourquoi la réciproque du **théorème 6** est fausse.

Théorème 7

$$\forall (a,b,c)\in\mathbb{Z}^3, \forall (u,v)\in\mathbb{Z}^2, \begin{cases} a \mid b \\ a \mid c \end{cases} \Rightarrow a \mid (bu+cv).$$

Autrement dit, si a divise b et c, alors il divise toute **combinaison linéaire** de b et de c.

Preuve

Supposons que $a \mid b$ et $a \mid c$.

Il existe alors un couple $(k,l)\in\mathbb{Z}^2$ tel que $b=ak$ et $c=al$.

Il vient que $bu=(ak)u$ et $cv=(al)v$, et donc $bu+cv=(ak)u+(al)v=a(ku+lv)$, soit, comme $ku+lv$ est un entier relatif, $a \mid (bu+cv)$. □

Remarque

En particulier, si a divise b et c, il divise aussi leur somme, et la différence $b-c$.

Prendre $u=v=1$ et ensuite $u=1$, $v=-1$.

Théorème 8

$$\forall (a,b)\in\mathbb{Z}^2, \forall n\in\mathbb{N}^*, a \mid b \Rightarrow a^n \mid b^n.$$

Le **théorème 8** dit en particulier que si a divise b alors a^2 divise b^2.

Preuve

Récurrence sur n.

L'implication est claire quand $n=1$.

Soit $n\in\mathbb{N}^*$ et supposons que $a \mid b \Rightarrow a^n \mid b^n$.

Dans ces conditions, il faut montrer l'implication : $a \mid b \Rightarrow a^{n+1} \mid b^{n+1}$.

Supposons alors que $a \mid b$.

Alors, d'après l'hypothèse de récurrence, $a^n \mid b^n$, soit, en utilisant le **théorème 6**, $a^{n+1} \mid b^{n+1}$. □

2 Division euclidienne

A Théorème de la division euclidienne

Le **théorème de la division euclidienne** est le théorème le plus important de ce chapitre. Il est important car il donne l'existence de deux entiers naturels à partir de deux autres entiers naturels.

Comme on sait le faire depuis longtemps, effectuons la division euclidienne de 476 par 3.

476	3
17	158
26	
2	

Rappel du vocabulaire : 476 est le **dividende**, 3 le **diviseur**, 158 le **quotient** et 2 le **reste**. Les articles définis sont justifiés par le **théorème 8** ci-dessous.

Il vient alors que $476=3\times158+2$.

A partir des entiers 476 et 3, nous avons obtenus le couple d'entiers $(158,2)$. Bien entendu, on pourrait aussi écrire que $476=3\times157+5$, mais alors $5>3$.

On va montrer qu'il n'existe qu'un seul couple d'entiers naturels (q,r) tel que $476=3q+r$ et $0\leqslant r<3$.

Théorème 9 **Théorème de la division euclidienne (version 1)**

$$\forall (a,b)\in\mathbb{N}\times\mathbb{N}^*, \exists !(q,r)\in\mathbb{N}\times\mathbb{N}, \begin{cases} a=bq+r \\ 0\leqslant r<b \end{cases}.$$

Le **théorème 9** est très important.

Preuve

Existence

Posons $A=\{n\in\mathbb{N}, nb\leqslant a\}$ qui est donc une partie de $\mathbb{N}$.

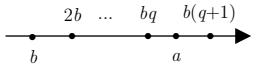
L'ensemble A n'est pas vide car il contient 0 (prendre $n=0$).

Montrons que l'ensemble A est en plus majoré.

Soit m un élément de A.

Comme $1\leqslant b$, il vient que $m\leqslant mb\leqslant a$ et donc m est majoré par a.

Une autre démonstration de l'existence est traitée dans l'**exercice 2**.



De ce qui précède, l'ensemble A admet un plus grand élément qu'on notera q et qui vérifie donc $bq \leqslant a$.

De plus, comme $q < q+1$, on a $q+1 \notin A$, c'est-à-dire $a < b(q+1)$ et ainsi :

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

Cette dernière relation entraîne que $0 \leqslant a - bq < b$. En posant $r = a - bq$ on a bien $a = bq + r$ et $0 \leqslant r < b$.

Unicité

Supposons qu'il existe deux couples d'entiers naturels (q, r) et (q', r') tels que :

$$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases} \text{ et } \begin{cases} a = bq' + r' \\ 0 \leqslant r' < b \end{cases}.$$

Utilisation de la régularité de la multiplication car b est non nul.

Alors $b(q - q') = r' - r$ et $-b < r' - r < b$, c'est-à-dire $-1 < q - q' < 1$, soit (**exercice 4**), $q = q'$.

Il vient ensuite que $r = r'$. □

Théorème 10 **Théorème de la division euclidienne (version 2)**

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{N}^*, \exists\,!(q, r) \in \mathbb{Z}^2, \begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}.$$

Le **théorème 10** est la formulation classique du théorème de la division euclidienne.

Preuve

Existence

Posons $A = \{n \in \mathbb{Z}, nb \leqslant a\}$ qui est donc une partie de $\mathbb{Z}$.

- Traitons le cas où $a \geqslant 0$.

L'ensemble A n'est pas vide car il contient 0 (prendre $n = 0$).

Montrons que l'ensemble A est majoré.

Soit m un élément de A.

Si $m \geqslant 0$, alors, comme $1 \leqslant b$, il vient que $m \leqslant mb \leqslant a$ et donc m est majoré par a.

Si $m < 0$, alors bien sûr $m < a$.

- Traitons le cas où $a < 0$.

De l'inégalité $1 \leqslant b$, on obtient $a \geqslant ab$ et donc $a \in A$ et ainsi A n'est pas vide.

Montrons que l'ensemble A est majoré.

Soit m un élément de A.

Si $m \geqslant 0$, alors comme $a < -a$ et $1 \leqslant b$, on a $m \leqslant mb \leqslant a < -a$.

Si $m < 0$, alors bien sûr $m \leqslant -a$ (puisque $-a > 0$).

Dans les deux cas, A est majorée par $-a$.

Finalement A est une partie non vide de $\mathbb{Z}$ et majorée : elle admet donc un plus grand élément q.

La preuve se termine comme pour le théorème précédent.

Attention, la démonstration proposée ici est différente du **théorème 9** !

Unicité

Comme dans le **théorème 9**. □

Remarques

1. Le procédé qui à tout couple $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ associe l'unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leqslant r < b$, est appelé la **division euclidienne de *a* par *b***.

2. Le lecteur prouvera facilement qu'il y a équivalence entre :

- a est un diviseur de b ;
- le reste de la division euclidienne de a par b est nul.

Exemple

Effectuons la division euclidienne -32 par 5.

On comme par effectuer la division euclidienne de 32 par 5.

On a : $32 = 5 \times 6 + 2$.

On déduit donc que $-32 = 5 \times (-6) + (-2)$. Or $-2 < 0$. Le couple $(-6, -2)$ en convient pas.

On remarque que $5 \times (-7) \leqslant -32 < 5 \times (-6)$.

Ainsi, $-32 = 5 \times (-6) - 5 + (5 - 2) = 5 \times (-7) + 3$, avec $0 \leqslant 3 < 5$.

Pour une méthode générale, voir l'**exercice 2**.

Théorème 11 **Théorème de la division euclidienne (version 3)**

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}^*, \exists\,!(q, r) \in \mathbb{Z}^2, \begin{cases} a = bq + r \\ 0 \leqslant r < |b| \end{cases}.$$

Le **théorème 11** est la formulation la plus étendue du **théorème de la division euclidienne**.

Preuve

Existence

Quand $b>0$, on sait faire.

Quand $b<0$, on effectue la division euclidienne de a par $-b$.

L'inégalité $r<-b$ devient $r<|b|$.

Il existe alors un unique couple $(q,r)\in\mathbb{Z}^2$ tel que $a=b(-q)+r$ et $0\leqslant r<|b|$.

Unicité

Comme dans le **théorème 9** mais en distinguant deux cas suivant le signe de b. □

Remarques

1. De ce qui précède, il est très simple d'obtenir la division euclidienne de a par -b quand on a celle de a par b.
En effet, par exemple, $32=5\times6+2$. On en déduit la division euclidienne de 32 par -5 : $32=(-5)\times(-6)+2$.
De même, il est très simple d'obtenir la division euclidienne de -a par -b quand on a celle de -a par b.
En effet, par exemple, $-32=5\times(-7)+3$. On en déduit la division euclidienne de -32 par -5 :

$$-32=(-5)\times7+3.$$

Cherchez cette condition large sur le reste (discussion en vidéo).

2. Dans le **théorème 11**, on peut être encore plus large sur la condition du reste, mais attention, on perd l'unicité.

B Systèmes de numération

Le système de numération que nous utilisons couramment est un système dont la base est 10.

Dans ce système de numération, l'écriture 473 signifie que $473=4\times10^2+7\times10+3$.

Mais le théorème suivant que nous allons démontrer, permet de définir d'autres systèmes de numération.

Théorème 12 **Théorème des systèmes de numération**

$$\forall a\in\mathbb{N}^*,\forall b\in\mathbb{N}\setminus\{0,1\},\exists n\in\mathbb{N},\exists!(a_0,...,a_n)\in\mathbb{N}^{n+1},\begin{cases}a=a_0+a_1b+a_2b^2+...+a_nb^n\\0\leqslant a_0,...,a_n<b\\a_n\neq0\end{cases}.$$

Pour des raisons pragmatiques, nous avons nommé ce théorème ainsi.
La formulation du **théorème 14** est très lourde mais à au moins l'avantage d'être exprimée sans aucun mot de français.

Preuve

La démonstration est très lourde et peut être omise en première lecture.

Existence

On fait ici une récurrence sur N.

Pour $N\geqslant1$ (avec b fixé dans $\mathbb{N}\setminus\{0,1\}$), nous allons noter $P(N)$ la propriété :

$$\forall a\leqslant N,\exists n\in\mathbb{N},\exists(a_0,...,a_n)\in\mathbb{N}^{n+1},\begin{cases}a=a_0+a_1b+a_2b^2+...+a_nb^n\\0\leqslant a_0,...,a_n<b\\a_n\neq0\end{cases}.$$

Dans la foulée, nous avons $P(1)$ qui est vraie et donc P est initialisée.

La propriété est évidente quand $N<b$, effet, il suffit de choisir $n=0$ et $a=a_0$.

Soit $N\geqslant b-1$ et supposons que $P(N)$ est vraie.

Par le **théorème de la division euclidienne** appliqué au couple $(N+1,b)$, on a l'existence d'un couple (q,r) tel que $N+1=bq+r$ et $0\leqslant r<b$.

Comme $N\geqslant b-1$, on a $N+1\geqslant b$ et donc $q>0$ (puisque si $q=0$, on aurait $N+1<b$, ce qui est contradictoire).

Puis, comme $2\leqslant b$, on a $q<2q\leqslant bq\leqslant N+1$ et donc $q\leqslant N$.

L'hypothèse de récurrence appliquée à q donne alors l'existence d'un entier naturel m et $m+1$ entiers naturels de sorte que :

$$\begin{cases}q=c_0+c_1b+c_2b^2...+c_mb^m\\0\leqslant c_0,...,c_m<b\\c_m\neq0\end{cases}.$$

Ainsi, $N+1=b(c_0+c_1b+c_2b^2...+c_mb^m)+r=r+bc_0+c_1b^2+...+c_mb^{m+1}$.

Unicité

Soient $a\in\mathbb{N}^*$ et $b\in\mathbb{N}\setminus\{0,1\}$.

Supposons qu'il existe un couple $(n,m)\in\mathbb{N}^2$, $(a_0,...,a_n)\in\mathbb{N}^{n+1}$ et $(c_0,...,c_m)\in\mathbb{N}^{m+1}$ tels que :

$$\begin{cases}a=a_0+a_1b+a_2b^2+...+a_nb^n=c_0+c_1b+c_2b^2+...+c_mb^m\\0\leqslant a_0,...,a_n,c_0,...,c_m<b\\a_nc_m\neq0\end{cases}.$$

Le cours du chapitre 9

Le but est de prouver que $m = n$.

Supposons par l'absurde que $m < n$ par exemple.

Utilisation du **théorème 7** du **chapitre 5** et des inégalités :
$0 \leqslant c_0, ..., c_m \leqslant b-1$.

On a d'une part $a_0 + a_1 b + a_2 b^2 + ... + a_n b^n \geqslant b^n$ et d'autre part $c_0 + c_1 b + c_2 b^2 + ... + c_m b^m \leqslant (b-1)(1 + b + ... + b^m)$

$$= b^{m+1} - 1$$
$$\leqslant b^n - 1$$

La suite $(a^n)_{n\in\mathbb{N}}$ à valeur dans $\mathbb{N}$ avec $a \geqslant 1$ est strictement croissante comme le lecteur pourra le vérifier en remarquant que :
$a^{n+1} - a^n = a^n(a-1)$.

Il vient alors que $a \leqslant b^n - 1 < b^n \leqslant a$, ce qui est absurde.

De même, on parviendrait avec la même contradiction en supposant cette fois-ci que $n < m$.

Ainsi, on a $n = m$.

On dispose à présent des égalités :

$$a = a_0 + a_1 b + a_2 b^2 + ... + a_n b^n = c_0 + c_1 b + c_2 b^2 + ... + c_n b^n \quad (*).$$

Il reste plus qu'à montrer que :

$$\forall i \in \{0, ..., n\}, a_i = c_i.$$

Effectuons une récurrence sur n.

L'initialisation est évidente (on obtient $a = a_0 = c_0$).

Soit $n \in \mathbb{N}^*$ et supposons que pour tous les entiers $a_0, ..., a_{n-1}, c_0, ..., c_{n-1}$ compris entre 0 et $b-1$ on a l'implication :

$$a_0 + a_1 b + a_2 b^2 + ... + a_{n-1} b^{n-1} = c_0 + c_1 b + c_2 b^2 + ... + c_{n-1} b^{n-1} \Rightarrow \forall i \in \{0, ..., n-1\}, a_i = c_i.$$

La deuxième égalité $(*)$ entraîne que :

$$a_0 - c_0 = c_1 b + c_2 b^2 + ... + c_n b^n - a_1 b - a_2 b^2 - ... - a_n b^n = b(c_1 + c_2 b + ... + c_n b^{n-1} - a_1 - ... - a_n b^{n-1}).$$

Donc b divise $a_0 - c_0$. Mais comme $0 \leqslant a_0 < b$ et $0 \leqslant c_0 < b$, on a $-b < a_0 - c_0 < b$, soit :

$$a_1 + a_2 b + ... + a_n b^{n-1} = c_1 + c_2 b + ... + c_n b^{n-1}.$$

L'hypothèse de récurrence s'applique et donc :

$$\forall i \in \{1, ..., n\}, a_i = c_i.$$

Enfin, avec $a_0 = c_0$, il vient que :

$$\forall i \in \{0, ..., n\}, a_i = c_i. \qquad \square$$

Comme vous le constatez, il était plus simple d'utiliser le théorème suivant :
$$\begin{cases} P(0) \\ \forall n \in \mathbb{N}^*, P(n-1) \Rightarrow P(n) \end{cases} \Rightarrow \forall n \in \mathbb{N}, P(n).$$

Remarques

Dans ces remarques, on reprend les hypothèses du **théorème 14**.

1. L'entier naturel a se note $\overline{a_n ... a_1 a_0}^b$ et c'est l'écriture de a en base b. Quand la base est 10, on omettra la barre.

Attention, ici le mot *chiffre* est utilisé pour désigner un objet abstrait et non un symbole.

2. Les entiers naturels $a_0, ..., a_n$ sont des **chiffres** du système de numération de base b.

3. Dans un système de numération de base b, il y a b chiffres (tous strictement inférieurs à b) distincts deux à deux.

4. Quand la base du système de numération dépassera 10, nous conviendrons de noter le « chiffre » 10 par **A**, 11 par **B**, 12 par **C**, 13 par **D**, 14 par **E** et 15 par **F**.

En informatique, les ordinateurs fonctionnent en utilisant le **système binaire**, c'est-à-dire le système de numération de base 2, dans lequel l'écriture d'un nombre n'utilise que deux chiffres (0 et 1) rendant compte ainsi du fait que certains éléments ne peuvent prendre que deux états.

Mais l'inconvénient du système binaire est que les écritures des nombres deviennent rapidement de longues suites de 0 et de 1.

C'est pourquoi on utilise aussi le **système hexadécimale** (base 16), le passage d'un système à l'autre étant facile.

Exemples

1. Ecrivons le nombre $\overline{1433}^8$ en base 10.

$\overline{1433}^8 = 1 \times 8^3 + 4 \times 8^2 + 3 \times 8 + 3 = 512 + 256 + 24 + 3 = 795$.

2. Ecrivons le nombre $\overline{10100011}^2$ en base 10.

$\overline{10100011}^2 = 2^7 + 2^5 + 2 + 1 = 128 + 32 + 3 = 163$.

3. Ecrivons le nombre 1729 en base 5.

Nous avons : $1729 = 5 \times 345 + 4$, $345 = 5 \times 69 + 0$, $69 = 5 \times 13 + 4$, $13 = 5 \times 2 + 3$ et $2 = 5 \times 0 + 2$.

Les restes, représentés en bleus, sont écrits « à l'envers ».

Ainsi, $1729 = \overline{23404}^5$.

4. Ecrivons le nombre 122 en base 2.

On a : $122 = 2 \times 61 + 0$, $61 = 2 \times 30 + 1$, $30 = 2 \times 15 + 0$, $15 = 2 \times 7 + 1$, $7 = 2 \times 3 + 1$, $3 = 2 \times 1 + 1$, $1 = 2 \times 0 + 1$.

Ainsi, $122 = \overline{1111010}^2$.

Nous allons maintenant expliquer les coulisses de cette méthode.

Le cours du chapitre 9

Soient a un entier naturel non nul et b un entier naturel non nul et différent de 1.

D'après le **théorème 14**, il existe un entier naturel n et un $n+1$-uplet $(a_0,...,a_n)\in\mathbb{N}^{n+1}$ tels que :

$$\begin{cases} a = a_0 + a_1 b + a_2 b^2 + ... + a_n b^n \\ 0 \leqslant a_0, ..., a_n < b \\ a_n \neq 0 \end{cases}.$$

Effectuons la division euclidienne de a par b.

On obtient successivement :

$$\left|\begin{array}{l} a = bq_0 + r_0 \\ q_0 = bq_1 + r_1 \\ q_1 = bq_2 + r_2 \\ \quad\vdots \\ q_{n-1} = bq_n + r_n \end{array}\right. \quad \text{où } n\in\mathbb{N}^*,\ 0\leqslant r_0,...,r_n<b \text{ et } q_0,...,q_n\in\mathbb{N}.$$

Par exemple, $q_0 = bq_1 + r_1 \geqslant bq_1 \geqslant q_1$.

On sait qu'il n'existe pas de suite strictement décroissante d'entiers naturels. Comme $q_0\geqslant q_1\geqslant ...\geqslant q_n$, il existe un entier naturel i (compris entre 0 et n) tel que $q_i = 0$.

Pour $n\in\mathbb{N}^*$, supposons que $q_n = 0$ et $q_{n-1}\neq 0$. Il vient alors que :

$$a = r_n b^n + ... + r_1 b + r_0 \text{ avec } r_n \neq 0.$$

Le **théorème 12** s'applique et l'écriture de a en base b donne alors : $a = \overline{r_n...r_1r_0}^{\,b}$.

3 Congruences

A Définition

La **définition 3** est très importante.

Définition 3

Soient a et b deux entiers relatifs et n un entier naturel.
Dire que a est **congru** à b **modulo** n signifie que n divise la différence $a-b$.

Remarques

On rencontre aussi les notations : $a\equiv b\ (n)$ et $a\equiv b\ (\text{mod } n)$.

1. Pour signifier que a est congru à b modulo n, on écrit $a\equiv b\ [n]$.
2. Compte tenu du **théorème 2**, dire que a est congru à b modulo n signifie également que n divise $b-a$.
3. La situation où $n=0$ est particulière. En effet :
$$\forall (a,b)\in\mathbb{Z}^2,\ a\equiv b\ [0] \Leftrightarrow 0\mid a-b \Leftrightarrow a-b=0 \Leftrightarrow a=b.$$
4. Il est clair que : $\forall (a,b)\in\mathbb{Z}^2,\ a\equiv b\ [1]$.
5. Par définition, il est immédiat que :
$$\forall (a,b)\in\mathbb{Z}^2,\ a\equiv b\ [n] \Leftrightarrow \exists k\in\mathbb{Z},\ a=b+kn.$$
6. Il est clair qu'un entier relatif a est divisible par n si et seulement si $a\equiv 0\ [n]$.

La vérification est immédiate.

Exemples

1. On a $57\equiv 43\ [2]$ car $2\mid 57-43$ c'est-à-dire $2\mid 14$.
2. On a aussi $57\equiv 43\ [7]$.

Il est important de préciser le modulo car par exemple $4\equiv 1\ [3]$ mais on n'a pas $4\equiv 1\ [5]$.

B Propriétés

Les propriétés de la congruence sont nombreuses et vous devez tous les connaître.

Le **théorème 13** est une caractérisation de la congruence. Mais attention, il faut supposer n non nul.

Théorème 13

Soient a et b deux entiers relatifs et n un entier naturel non nul.
L'entier a est congru à b modulo n si et seulement si a et b ont le même reste dans la division euclidienne par n.

Preuve

Commençons par effectuer la division euclidienne de a par n et de b par n.
Il existe deux couples (q,r) et (q',r') d'entiers relatifs tels que $a=nq+r$, $b=nq'+r'$, $0\leqslant r<n$ et $0\leqslant r'<n$.
Il vient alors que $a-b=n(q-q')+r-r'$.

($\Rightarrow$) Supposons que a est congru à b modulo n.
Alors n divise $a-b$ et il existe donc un entier relatif k tel que $a-b=nk$.
Il vient alors que $nk-n(q-q')=n(k-q+q')=r-r'$ et $-n<n(k-q+q')<n$.

Remarquez que l'entier n est non nul, ce qui permet de simplifier par n.

Ainsi, $-1<k-q+q'<1$ et alors $k=q-q'$, ce qui entraîne que $r=r'$.
($\Leftarrow$) Supposons que a et b ont le même reste dans la division euclidienne par n.
Alors $a-b=n(q-q')$ et donc, puisque $q-q'\in\mathbb{Z}$, n divise $a-b$, c'est-à-dire que a est congru à b modulo n. □

Exemple
$11=7\times1+4$ et $18=7\times2+4$. Donc $11\equiv18\ [7]$.

Le **théorème 14** est très important en pratique.

Théorème 14

Soient a et r deux entiers relatifs et n un entier naturel non nul.
L'entier a est congru à r modulo n avec $0\leqslant r<n$ si et seulement si r est le reste de la division euclidienne de a par n.

Preuve
($\Rightarrow$) Supposons que a est congru à r modulo n avec $0\leqslant r<n$.
Effectuons la division euclidienne de a par n.
Il existe un unique couple $(q,r')\in\mathbb{Z}^2$ tel que $a=qn+r'$ et $0\leqslant r'<n$.
Par unicité du reste, on a $r=r'$.
($\Leftarrow$) Supposons que r est le reste de la division euclidienne de a par n.
On sait déjà d'après le **théorème de la division euclidienne** que $0\leqslant r<n$.
De plus, la division euclidienne de a par n fournit l'existence d'un entier relatif q tel que $a=qn+r$.

L'égalité $a-r=qn$ entraîne que l'entier n divise $a-r$.

Il vient alors que $a-r=qn$ et donc par définition de la congruence, $a\equiv r\ [n]$. □

Remarques
1. Attention ! Il est important dans le **théorème 14** d'avoir la condition $0\leqslant r<n$.
En effet, par exemple $11\equiv18\ [7]$, mais 18 n'est pas le reste de la division euclidienne de 11 par 7...
2. Quand a est congru à r modulo n avec $0\leqslant r<n$, le reste de la division euclidienne de r par n vaut de nouveau r puisque $r=0\times n+r$.

Ce qui est quand même rassurant compte tenu du **théorème 13** !

Théorème 15

$$\forall(a,b)\in\mathbb{Z}^2,\forall(n,m)\in\mathbb{N}^2,n\mid m\Rightarrow(a\equiv b\ [m]\Rightarrow a\equiv b\ [n]).$$

Attention à la position de la parenthèse et à l'ordre des lettres n et m. On rappelle que quand P, Q et R désignent des assertions, il y a une différence entre les implications :
$P\Rightarrow(Q\Rightarrow R)$ et $(P\Rightarrow Q)\Rightarrow R$.

Preuve
Supposons que $n\mid m$ et que $a\equiv b\ [m]$.
Comme $m\mid a-b$, il vient que (la relation « divise » est transitive) $n\mid a-b$. □

Exemple
Comme $14\equiv2\ [6]$, il vient que $14\equiv2\ [3]$.

Le **théorème 16** est fondamentale pour la suite du cours.

Théorème 16

La relation « $\equiv$ » est une relation d'équivalence sur $\mathbb{Z}$.

Preuve
Ici, a, b et c désignent des entiers relatifs et n un entier naturel.
Réflexivité
Puisque $n\mid a-a$, on a $a\equiv a\ [n]$.
Symétrie
Utilisation du **théorème 2**.
On dispose les implications suivantes : $a\equiv b\ [n]\Rightarrow n\mid a-b\Rightarrow n\mid b-a\Rightarrow b\equiv a\ [n]$.
Transitivité
Utilisation du **théorème 7**.
On dispose les implications suivantes : $\begin{cases}a\equiv b\ [n]\\ b\equiv c\ [n]\end{cases}\Rightarrow\begin{cases}n\mid a-b\\ n\mid b-c\end{cases}\Rightarrow n\mid a-c\Rightarrow a\equiv c\ [n]$. □

Remarque

Admettons que $a \equiv b\ [n]$.

La symétrie de la congruence permet de dire aussi que b est congru à a modulo n et donc que a et b sont congru modulo n sans tenir compte du sens.

Le **théorème 17** est très important.

On peut donc ajouter membre à membre des entiers relatifs dans les congruences.

Théorème 17 **Compatibilité de la congruence avec l'addition**

$$\forall (a,b,c,d) \in \mathbb{Z}^4, \forall n \in \mathbb{N}, \begin{cases} a \equiv b\ [n] \\ c \equiv d\ [n] \end{cases} \Rightarrow a+c \equiv b+d\ [n].$$

Preuve

Supposons que $a \equiv b\ [n]$ et $c \equiv d\ [n]$.

Il existe alors deux entiers relatifs k et l tels que $a = b+nk$ et $c = d+nl$.

Donc $a+c = (b+d)+n(k+l)$, d'où, $(a+c)-(b+d) = n(k+l)$.

La dernière égalité entraîne que, puisque $k+l \in \mathbb{Z}$, $n \mid (a+c)-(b+d)$, c'est-à-dire $a+c \equiv b+d\ [n]$. □

Exemples

1. Comme $5 \equiv 1\ [2]$ et $11 \equiv -3\ [2]$, il vient que $16 \equiv -2\ [2]$.

2. Un exercice pour vous : a et b désignent des entiers relatifs tels que $a \equiv 2\ [5]$ et $b \equiv 3\ [5]$.

Montrer que $a^2+b^3 \equiv 1\ [5]$.

Remarque

La réciproque du **théorème 17** est évidemment fausse et le lecteur est invité à trouver un contre-exemple.

Le **théorème 18** est très important.

On peut donc multiplier membre à membre des entiers relatifs dans les congruences.

Théorème 18 **Compatibilité de la congruence avec la multiplication**

$$\forall (a,b,c,d) \in \mathbb{Z}^4, \forall n \in \mathbb{N}, \begin{cases} a \equiv b\ [n] \\ c \equiv d\ [n] \end{cases} \Rightarrow ac \equiv bd\ [n].$$

Preuve

Supposons que $a \equiv b\ [n]$ et $c \equiv d\ [n]$.

Il existe alors deux entiers relatifs k et l tels que $a-b = nk$ et $c-d = nl$.

Comme $ac-bd = ac-bd+bc-bc = c(a-b)+b(c-d)$, on a $ac-bd = cnk+bnl = n(ck+bl)$.

Ce genre d'égalité très astucieuse est à connaître. Elle est parfois utilisée dans des démonstrations comme ici.
Il est possible de passer outre cette astuce en remarquant que :
$ac-bd = (b+nk)(d+nl)-bd$.

Comme $ck+bl \in \mathbb{Z}$, $n \mid ac-bd$ et donc $ac \equiv bd\ [n]$. □

Exemple

Comme $5 \equiv -3\ [2]$ et $11 \equiv -3\ [2]$, il vient que $55 \equiv 9\ [2]$.

Remarque

La réciproque du **théorème 18** est évidemment fausse et le lecteur est invité à trouver un contre-exemple.

Le **théorème 19** est très important.

En particulier, si on a $a \equiv b\ [n]$, alors $a^2 \equiv b^2\ [n]$.

Théorème 19

$$\forall (a,b) \in \mathbb{Z}^2, \forall k \in \mathbb{N}, a \equiv b\ [n] \Rightarrow a^k \equiv b^k\ [n].$$

Preuve

Récurrence sur k.

L'implication est clairement vérifiée quand $k = 1$.

Soit $k \in \mathbb{N}$ et supposons que $a \equiv b\ [n] \Rightarrow a^k \equiv b^k\ [n]$.

On va montrer dans ces conditions l'implication : $a \equiv b\ [n] \Rightarrow a^{k+1} \equiv b^{k+1}\ [n]$.

Supposons alors que $a \equiv b\ [n]$.

Par hypothèse de récurrence, on a $a^k \equiv b^k\ [n]$.

Puis, en utilisant le **théorème 18**, il vient que $a^k \times a \equiv b^k \times b\ [n]$, c'est-à-dire $a^{k+1} \equiv b^{k+1}\ [n]$. □

Remarque

La réciproque du **théorème 19** est fausse et le lecteur est invité à trouver un contre-exemple.

Exemples

1. Montrons que $1809^{235}-1$ est divisible par 8.

En utilisant le critère de divisibilité par 8, il est clair que $1809 \equiv 1\,[8]$, donc (**théorème 19**) $1809^{235} \equiv 1\,[8]$.

Sans utiliser de critère de divisibilité, on pouvait aussi remarquer que : $1809 = 8\times 226 + 1$.

2. Déterminons le reste de la division euclidienne de 1773^{704} par 7.

Evidemment, un calcul à la main est inenvisageable !

On effectue d'abord la division euclidienne de 1773 par 7 : $1773 = 7\times 753 + 2$.

Donc (**théorème 14**), $1773 \equiv 2\,[7]$.

Via le **théorème 19**, on en déduit que $1773^{704} \equiv 2^{704}\,[7]$.

Il faut s'occuper maintenant de l'entier 2^{704}.

On a : $2^0 \equiv 1\,[7]$, $2^1 \equiv 2\,[7]$, $2^2 \equiv 4\,[7]$ et $2^3 \equiv 1\,[7]$.

Donc, $2^{704} = (2^3)^{234}\times 4$ et alors $2^{704} \equiv 4\,[7]$.

Ainsi, $1773^{704} \equiv 2^{704}\,[7]$ et $2^{704} \equiv 4\,[7]$, d'où (transitivité de la relation de congruence) $1773^{704} \equiv 4\,[7]$.

Utilisation du **théorème 14**.

Le reste de la division euclidienne de 1773 par 7 est donc 4.

3 Critères de divisibilité

Vous connaissez pas mal de critère de divisibilité (par 2, 3, 5, 9 et 10). Dans ce paragraphe, nous allons utiliser les congruences pour les démontrer.

Rappelons le **théorème des systèmes de numération** appliquer à la base 10 :

$$\forall a\in\mathbb{N}^*, \exists n\in\mathbb{N}, \exists !(a_0,...,a_n)\in\mathbb{N}^{n+1}, \begin{cases} a = a_0 + a_1\times 10 + a_2\times 10^2 + ... + a_n\times 10^n \\ 0\leqslant a_0,...,a_n < n \\ a_n \neq 0 \end{cases}.$$

Pour toute la suite, on notera $N = \sum_{k=0}^{n} a_k 10^k$. L'entier N s'écrit alors $\overline{a_n...a_1a_0}$ où nous avons omis la base 10 car il n'y aura pas d'ambiguïté.

A Critère de divisibilité par 2

Théorème 20 **Critère de divisibilité par 2**

L'entier N est divisible par 2 si et seulement si $a_0 \in \{0,2,4,6,8\}$.

Autrement dit, N est divisible par 2 si et seulement si son chiffre des unités est 0, 2, 4, 6 ou 8.

Preuve

Il suffit d'écrire que $N = \sum_{k=0}^{n} a_k 10^k = a_0 + \sum_{k=1}^{n} a_k 10^k = a_0 + 10\sum_{k=1}^{n} a_k 10^{k-1}$.

$(\Rightarrow)$ Supposons que N est divisible par 2.

Alors, comme $2 \mid 10\sum_{k=1}^{n} a_k 10^{k-1}$, il vient que (**théorème 7**) $2 \mid N - 10\sum_{k=1}^{n} a_k 10^{k-1}$, c'est-à-dire $2 \mid a_0$.

Comme $0\leqslant a_0 < 10$, la condition $2 \mid a_0$ revient à dire que $a_0 \in \{0,2,4,6,8\}$.

$(\Leftarrow)$ Réciproquement, supposons que $a_0 \in \{0,2,4,6,8\}$.

Alors, $2 \mid a_0$ et comme $2 \mid 10\sum_{k=1}^{n} a_k 10^{k-1}$, il vient que $2 \mid a_0 + 10\sum_{k=1}^{n} a_k 10^{k-1}$, c'est-à-dire $2 \mid N$. □

B Critère de divisibilité par 3

Théorème 21 **Critère de divisibilité par 3**

L'entier N est divisible par 3 si et seulement si $3 \mid \sum_{k=0}^{n} a_k$.

Autrement dit, N est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

Preuve

Comme $10 \equiv 1\,[3]$, on a (**théorème 19**) pour tout entier naturel k, $10^k \equiv 1\,[3]$.

Il vient alors que $N \equiv \sum_{k=0}^{n} a_k \ [3]$.

$(\Rightarrow)$ Supposons que N est divisible par 3.

Utilisation du **théorème 7**.

Alors comme $3 \mid N - \sum_{k=0}^{n} a_k$, on a $3 \mid N - N + \sum_{k=0}^{n} a_k$, c'est-à-dire $3 \mid \sum_{k=0}^{n} a_k$.

$(\Leftarrow)$ Supposons que $3 \mid \sum_{k=0}^{n} a_k$.

Alors il est clair que $\sum_{k=0}^{n} a_k \equiv 0 \ [3]$, d'où $N \equiv 0 \ [3]$.

Ainsi N est bien divisible par 3. □

Exemple

Le nombre 4789 est-il divisible par 3 ?

On a : $4+7+8+9 = 28$ et $3 \times 9 < 28 < 3 \times 10$.

Réponse : non.

C Critère de divisibilité par 4

Théorème 22 — Critère de divisibilité par 4

L'entier N est divisible par 4 si et seulement si $4 \mid \overline{a_1 a_0}$.

Autrement dit N est divisible par 4 si et seulement si le nombre formé par les deux derniers chiffres (ce qui explique la présence de la barre) est divisible par 4.

Preuve

Comme $4 \mid 100$, on a pour tout entier $k \geqslant 2$, $4 \mid 10^k$, donc pour tout $k \geqslant 2$, $10^k \equiv 0 \ [4]$.

Il vient alors que $\sum_{k=2}^{n} a_k 10^k \equiv 0 \ [4]$, d'où $N \equiv a_0 + a_1 \times 10 \ [4]$.

$(\Rightarrow)$ Supposons que N est divisible par 4.

Utilisation du **théorème 7**.

Alors comme $4 \mid N - (a_0 + a_1 \times 10)$, on a $4 \mid N - N + (a_0 + a_1 \times 10)$, soit $4 \mid a_0 + a_1 \times 10$.

$(\Leftarrow)$ Supposons que $4 \mid \overline{a_1 a_0}$.

Alors $4 \mid a_0 + a_1 \times 10$ et $4 \mid N - (a_0 + a_1 \times 10)$, on obtient $4 \mid N$. □

Exemple

Le nombre 4788 est-il divisible par 4 ?

Oui car $88 = 4 \times 22$.

D Critère de divisibilité par 5

Théorème 23 — Critère de divisibilité par 5

L'entier N est divisible par 5 si et seulement si $a_0 \in \{0, 5\}$.

Autrement dit N est divisible par 5 si et seulement si son chiffre des unités est 0 ou 5.

Preuve

Comme $5 \mid 10$, on a pour tout entier $k \geqslant 1$, $5 \mid 10^k$, donc pour tout $k \geqslant 1$, $10^k \equiv 0 \ [5]$.

Il vient alors que $\sum_{k=1}^{n} a_k 10^k \equiv 0 \ [5]$, d'où $N \equiv a_0 \ [5]$.

$(\Rightarrow)$ Supposons que N est divisible par 5.

Utilisation du **théorème 7**.

Alors comme $5 \mid N - a_0$, on a $5 \mid N - N + a_0$, c'est-à-dire $5 \mid a_0$.

De plus, $0 \leqslant a_0 < 10$, donc $a_0 = 0$ ou $a_0 = 5$.

$(\Leftarrow)$ Supposons que $a_0 \in \{0, 5\}$.

Quand $a_0 = 0$, on a $N \equiv 0 \ [5]$ et donc N est divisible par 5.

Quand $a_0 = 5$, on a encore $N \equiv 0 \ [5]$ (puisque $5 \equiv 0 \ [5]$) et donc N est divisible par 5.

Dans tous les cas N est bien divisible par 5. □

Exemple

Le nombre $789\,632\,445$ est-il divisible par 5 ?

Oui, son chiffre des unités est 5.

E Critère de divisibilité par 8

Un critère de divisibilité par 7 sera fourni dans le chapitre suivant en utilisant le **théorème de Gauss**.

Théorème 24 Critère de divisibilité par 8

L'entier N est divisible par 8 si et seulement si $8 \mid \overline{a_2a_1a_0}$.

Autrement dit N est divisible par 8 si et seulement si le nombre formé par les trois derniers chiffres (ce qui explique la présence de la barre) est divisible par 8.

Preuve

En effet, $1000 = 8\times125$.

Comme $8 \mid 1000$, on a pour tout entier $k \geqslant 3$, $8 \mid 10^k$, donc pour tout $k \geqslant 3$, $10^k \equiv 0\ [8]$.

Il vient alors que $\sum_{k=3}^{n} a_k 10^k \equiv 0\ [8]$, d'où $N \equiv a_0 + a_1\times10 + a_2\times10^2\ [8]$.

$(\Rightarrow)$ Supposons que N est divisible par 8.

Utilisation du **théorème 7**.

Alors comme $8 \mid N - (a_0 + a_1\times10 + a_2\times10^2)$, on a $8 \mid N - N + (a_0 + a_1\times10 + a_2\times10^2)$, soit $8 \mid a_0 + a_1\times10 + a_2\times10^2$.

$(\Leftarrow)$ Supposons que $8 \mid \overline{a_2a_1a_0}$.

Alors $8 \mid a_0 + a_1\times10 + a_2\times10^2$ et $8 \mid N - (a_0 + a_1\times10 + a_2\times10^2)$, on obtient $8 \mid N$. □

Exemple

Le nombre $456\,123\,886$ est-il divisible par 8 ?

Non car $886 = 8\times110 + 6$.

F Critère de divisibilité par 9

Théorème 25 Critère de divisibilité par 9

L'entier N est divisible par 9 si et seulement si $9 \mid \sum_{k=0}^{n} a_k$.

Autrement dit, N est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

Preuve

Il suffit de remplacer 3 par 9 dans la démonstration du **théorème 21**. □

Exemple

Le nombre $456\,123\,886$ est-il divisible par 9 ?

On a : $4+5+6+1+2+3+8+8+6 = 43$ et $9\times4 < 43 < 9\times5$.

Réponse : non.

G Critère de divisibilité par 10

Théorème 26 Critère de divisibilité par 10

L'entier N est divisible par 10 si et seulement si $a_0 = 0$.

Autrement dit, N est divisible par 10 si et seulement si son chiffre des unités est 0.

Preuve

En fait, il suffit de combiner les critères de divisibilité par 2 et par 5, mais la justification de ce procédé est plus délicate.

Il suffit d'écrire que $N = \sum_{k=0}^{n} a_k 10^k = a_0 + \sum_{k=1}^{n} a_k 10^k = a_0 + 10\sum_{k=1}^{n} a_k 10^{k-1}$.

$(\Rightarrow)$ Supposons que N est divisible par 10.

Alors, comme $10 \mid 10\sum_{k=1}^{n} a_k 10^{k-1}$, il vient que (**théorème 7**) $10 \mid N - 10\sum_{k=1}^{n} a_k 10^{k-1}$, c'est-à-dire $10 \mid a_0$.

Utilisation du **théorème 4**.

Cette condition impose que $a_0 = 0$ puisque $0 \leqslant a_0 < 10$.

$(\Leftarrow)$ Réciproquement, supposons que $a_0 = 0$.

Alors $N = 10\sum_{k=1}^{n} a_k 10^{k-1}$, donc N est divisible par 10. □

Le cours du chapitre 9

H Critère de divisibilité par 11

Théorème 27 **Critère de divisibilité par 11**

L'entier N est divisible par 11 si et seulement si $11 \mid \sum_{k=0}^{n} (-1)^k a_k$.

Preuve

Comme $10 \equiv -1\ [11]$, on a pour tout entier naturel k, $10^k \equiv (-1)^k\ [11]$.

Il vient alors que $N \equiv \sum_{k=0}^{n} (-1)^k a^k\ [11]$.

$(\Rightarrow)$ Supposons que N est divisible par 11.

Utilisation du **théorème 7**.

Alors comme $11 \mid N - \sum_{k=0}^{n} (-1)^k a^k$, on a $11 \mid N - N + \sum_{k=0}^{n} (-1)^k a^k$, soit $11 \mid \sum_{k=0}^{n} (-1)^k a^k$.

$(\Leftarrow)$ Réciproquement, supposons que $11 \mid \sum_{k=0}^{n} (-1)^k a^k$.

Alors il est clair que $\sum_{k=0}^{n} (-1)^k a^k \equiv 0\ [11]$ et donc $N \equiv 0\ [11]$.

Ainsi, N est bien divisible par 11. □

Exemple

L'entier 793 236 111 est-il divisible par 11 ?

On a d'une part $7+3+3+1+1=15$ et d'autre part : $-(9+2+6+1)=-18$.

Donc $15-18=-3$.

Réponse : non.

4 L'anneau Z/nZ

A Définition

Nous avons vu que la relation de congruence est une relation d'équivalence sur $\mathbb{Z}$. Quel est donc l'ensemble-quotient ?

En théorie, cet ensemble-quotient devrait se noter $\mathbb{Z}/\equiv$, mais elle sera notée $\mathbb{Z}/n\mathbb{Z}$.

L'explication de cette notation tient son origine des idéaux (programme de licence 2).

Pour tout a de $\mathbb{Z}$, on notera $\overline{a}$ la classe d'équivalence de a modulo la relation de congruence.

Ainsi, $\overline{a} = \{b \in \mathbb{Z}, a \equiv b\ [n]\} = \{b \in \mathbb{Z}, \exists k \in \mathbb{Z}, b = a + kn\} = \{a + kn, k \in \mathbb{Z}\}$.

Que peut-on dire de $\mathbb{Z}/0\mathbb{Z}$ et de $\mathbb{Z}/1\mathbb{Z}$?

La deuxième égalité mérite une explication. En effet, quel que soit l'entier relatif a, on a $\overline{a} = \mathbb{Z}$ (on travaille modulo 1). Donc l'ensemble des classes est un singleton et c'est $\overline{0}$ qu'on a choisi (n'importe quelle classe d'équivalence aurait pu convenir).

Il est clair que $\mathbb{Z}/0\mathbb{Z} = \{\{a\}, a \in \mathbb{Z}\}$ et que $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$.

B Propriété fondamentale

Il est évident que $\mathbb{Z}/n\mathbb{Z} = \{\overline{a}, a \in \mathbb{Z}\}$, mais l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est-il vraiment infini ?

Théorème 28

Soit n un entier naturel non nul.

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n et $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.

Preuve

Dans le **chapitre 1** du livre des probabilités, nous démontrerons qu'entre deux entiers a et b (avec $a \leqslant b$), il y a $b-a+1$ entiers.

On admet qu'il y a n entiers compris entre 0 et $n-1$.

Soit a un entier relatif.

La division euclidienne de a par n fournit deux entiers relatifs q et r tels que $a = nq + r$ et $0 \leqslant r < n$.

On a donc $a \equiv r\ [n]$ d'où $\overline{a} = \overline{r}$ (**théorème 12-2** du **chapitre 2**).

La condition $0 \leqslant r < n$ étant équivalente à $r \in \{0, ..., n-1\}$, un élément de $\mathbb{Z}/n\mathbb{Z}$ s'écrit alors de la forme $\overline{r}$ avec $r \in \{0, ..., n-1\}$ d'où $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, ..., \overline{n-1}\}$ (l'inclusion $\{\overline{0}, ..., \overline{n-1}\} \subset \mathbb{Z}/n\mathbb{Z}$ étant triviale).

A ce stade, on sait que l'ensemble-quotient $\mathbb{Z}/n\mathbb{Z}$ est fini. Il reste à montrer qu'il est de cardinal n.

Montrons maintenant que les éléments $\overline{0}, \overline{1}, ..., \overline{n-1}$ sont deux à deux distincts.

Le cours du chapitre 9

Soient r et s deux éléments de $\{0,...,n-1\}$ tels que $\overline{r}=\overline{s}$.

Alors $r\equiv s\ [n]$ et donc par définition, il existe un entier relatif k tel que $r-s=kn$.

De plus, comme $-n<r-s<n$, il vient que $-1<k<1$ et donc $k=0$.

On a montré (par contraposition) que : $\forall (r,s)\in\{0,...,n-1\}^2, r\neq s\Rightarrow \overline{r}\neq\overline{s}$.

Par suite, $r=s$.

Ainsi, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est bien fini et de cardinal n. □

Exemple

$\mathbb{Z}/3\mathbb{Z}=\{\overline{0},\overline{1},\overline{2}\}$.

Quitte à avoir des entiers négatifs, il est parfois utile de répartir des éléments « autour de 0 ».

Mais il est intéressant aussi d'écrire $\mathbb{Z}/3\mathbb{Z}=\{\overline{-1},\overline{0},\overline{1}\}$ puisque $-1\equiv 2\ [3]$.

C Addition dans Z/nZ

Dorénavant, n ne sera jamais nul.

Dans ce paragraphe, n désigne un entier naturel non nul.

Définissons une loi interne dans $\mathbb{Z}/n\mathbb{Z}$ par :

$$\forall (a,b)\in\mathbb{Z}^2, \overline{a}+\overline{b}=\overline{a+b}.$$

Vérifions que la somme $\overline{a}+\overline{b}$ ne dépend pas du choix des représentants des classes $\overline{a}$ et $\overline{b}$.

Soient c et d sont deux entiers relatifs tels que $\overline{a}=\overline{c}$ et $\overline{b}=\overline{d}$.

Alors $a\equiv c\ [n]$ et $b\equiv d\ [n]$.

D'après la compatibilité de la congruence avec l'addition (**théorème 17**), on a $a+b\equiv c+d\ [n]$. Cette dernière relation entraîne que $\overline{a+b}=\overline{c+d}$ ... ouf.

Exemple

Dans $\mathbb{Z}/3\mathbb{Z}$, $\overline{2}+\overline{1}=\overline{0}$.

Le **théorème 29** est très important.

Théorème 29

Soit n un entier naturel non nul.

Le couple $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe commutatif.

Preuve

- Loi + est évidemment interne dans $\mathbb{Z}/n\mathbb{Z}$.

Utilisation de l'associativité de l'addition dans $\mathbb{Z}$.

- On a : $\forall (a,b,c)\in\mathbb{Z}^3, \overline{a}+(\overline{b}+\overline{c})=\overline{a}+\overline{b+c}=\overline{a+(b+c)}=\overline{(a+b)+c}=\overline{a+b}+\overline{c}=(\overline{a}+\overline{b})+\overline{c}$.

La loi + est donc associative dans $\mathbb{Z}/n\mathbb{Z}$.

Utilisation de la commutativité de l'addition dans $\mathbb{Z}$.

- On a : $\forall (a,b)\in\mathbb{Z}^2, \overline{a}+\overline{b}=\overline{a+b}=\overline{b+a}=\overline{b}+\overline{a}$.

La loi + est donc commutative dans $\mathbb{Z}/n\mathbb{Z}$.

L'entier 0 est neutre pour l'addition dans $\mathbb{Z}$.

- On a : $\forall a\in\mathbb{Z}, \overline{a}+\overline{0}=\overline{a+0}=\overline{a}$.

La loi + admet donc $\overline{0}$ comme élément neutre.

Tout entier relatif a admet $-a$ comme opposé.

- On a : $\forall a\in\mathbb{Z}, \overline{a}+\overline{-a}=\overline{a+(-a)}=\overline{0}$.

Tout élément de $\mathbb{Z}/n\mathbb{Z}$ admet donc un opposé.

Le couple $(\mathbb{Z}/n\mathbb{Z},+)$ est par conséquent un groupe commutatif. □

D Multiplication dans Z/nZ

Dans ce paragraphe, n désigne un entier naturel non nul.

Définissons une loi interne dans $\mathbb{Z}/n\mathbb{Z}$ par :

$$\forall (a,b)\in\mathbb{Z}^2, \overline{a}\times\overline{b}=\overline{a\times b}.$$

Là encore, vérifions que le produit $\overline{a}\times\overline{b}$ ne dépend pas du choix des représentants des classes $\overline{a}$ et $\overline{b}$.

Soient c et d sont deux entiers relatifs tels que $\overline{a}=\overline{c}$ et $\overline{b}=\overline{d}$.

Alors $a\equiv c\ [n]$ et $b\equiv d\ [n]$.

D'après la compatibilité de la congruence avec la multiplication (**théorème 18**), on a $ab\equiv cd\ [n]$. Cette dernière relation entraîne que $\overline{ab}=\overline{cd}$.

Exemple

Dans $\mathbb{Z}/5\mathbb{Z}$, $\overline{4}\times\overline{3}=\overline{2}$.

Le cours du chapitre 9

Le **théorème 30** est très important.

Théorème 30

Soit n un entier naturel non nul.
Le triplet $(\mathbb{Z}/n\mathbb{Z}\,,+,\times)$ est un anneau commutatif.

Preuve

On sait déjà que le couple $(\mathbb{Z}/n\mathbb{Z}\,,+)$ est un groupe commutatif.

- La loi $\times$ est évidemment interne dans $\mathbb{Z}/n\mathbb{Z}$.

Utilisation de l'associativité de la multiplication dans $\mathbb{Z}$.

- $\forall (a,b,c)\in\mathbb{Z}^3, \overline{a}\times(\overline{b}\times\overline{c})=\overline{a}\times\overline{b\times c}=\overline{a\times(b\times c)}=\overline{(a\times b)\times c}=\overline{a\times b}\times\overline{c}=(\overline{a}\times\overline{b})\times\overline{c}$.

La loi $\times$ est donc associative dans $\mathbb{Z}/n\mathbb{Z}$.

Utilisation de la commutativité de la multiplication dans $\mathbb{Z}$.

- $\forall (a,b)\in\mathbb{Z}^2, \overline{a}\times\overline{b}=\overline{a\times b}=\overline{b\times a}=\overline{b}\times\overline{a}$.

La loi $\times$ est donc commutative dans $\mathbb{Z}/n\mathbb{Z}$.

L'entier 1 est neutre pour la multiplication dans $\mathbb{Z}$.

- $\forall a\in\mathbb{Z}, \overline{a}\times\overline{1}=\overline{a\times 1}=\overline{a}$.

La loi $\times$ admet $\overline{1}$ comme élément neutre.

Utilisation de la distributivité de la multiplication sur l'addition dans $\mathbb{Z}$.

- $\forall (a,b,c)\in\mathbb{Z}^3, \overline{a}\times(\overline{b}+\overline{c})=\overline{a}\times\overline{b+c}=\overline{a\times(b+c)}=\overline{a\times b+a\times c}=\overline{a\times b}+\overline{a\times c}=\overline{a}\times\overline{b}+\overline{a}\times\overline{c}$.

La loi $\times$ est distributive sur la loi $+$.
Le triplet $(\mathbb{Z}/n\mathbb{Z}\,,+,\times)$ est finalement un anneau commutatif. □

Remarque

L'anneau $\mathbb{Z}/n\mathbb{Z}$ (avec $n\geqslant 1$) est-il intègre ?

Dans $\mathbb{Z}/4\mathbb{Z}$, on a $\overline{2}\times\overline{2}=\overline{0}$. L'anneau $(\mathbb{Z}/4\mathbb{Z}\,,+,\times)$ n'est donc pas intègre.

Si vous cherchez des diviseurs de zéro dans $\mathbb{Z}/5\mathbb{Z}$, vous n'en trouverez pas ! L'explication sera fournie dans un autre chapitre d'arithmétique.

Il s'agit du **chapitre 13**.

Les exercices du chapitre 9

1 **Démonstrations supplémentaires de cours** 🖫

Montrer que : $\forall (a,b)\in\mathbb{Z}^2, \begin{cases} a \mid b \\ b \mid a \end{cases} \Rightarrow |a|=|b|$.

2 **Démonstrations supplémentaires de cours** 🖫

Montrer que : $\forall a\in\mathbb{Z}, -1<a<1 \Rightarrow a=0$.

3 **Démonstrations supplémentaires de cours** 🖫

Soit a un entier relatif.

1) A l'aide de la division euclidienne, montrer que a est impair si et seulement s'il existe un entier relatif k tel que $a=2k+1$.

Parité de la somme de deux entiers relatifs

2) Montrer que :

a) La somme de deux nombres entiers pairs est paire.

b) La somme de deux nombres entiers impairs est paire.

c) La somme d'un nombre entier pair et d'un nombre entier impair est impaire.

Parité du produit de deux entiers relatifs

3) Montrer que :

a) Le produit de deux nombres entiers pairs est pair.

b) Le produit de deux nombres entiers impairs est impair.

c) Le produit d'un nombre entier pair et d'un nombre entier impair est pair.

4 **Démonstrations supplémentaires de cours** 🖫

Soit n un entier relatif pair.

Montrer que quel que l'entier naturel p non nul, n^p est un entier pair.

5 **Démonstrations supplémentaires de cours** 🖫

Soit n un entier relatif impair.

Montrer que quel que l'entier naturel p, n^p est un entier impair.

6 **Divisibilité** 🖫

Montrer que : $\forall (a,b)\in\mathbb{Z}^2, \forall n\in\mathbb{Z}^*, a\mid b \Leftrightarrow an\mid bn$.

7 **Démonstrations supplémentaires de cours** 🖫

Soit n un entier relatif.

1) Montrer que si n^2 est pair, alors n est pair.

2) Montrer que si n^2 est impair, alors n est impair.

8 **Divisibilité**

Déterminer l'ensemble des entiers naturels n tels que $n+1$ divise n^2+n+1.

9 **Divisibilité**

Montrer que : $\forall n\in\mathbb{N}^*, n^2\mid (n+1)^n-1$.

10 **Multiple**

Soit n un entier naturel impair.

Montrer que la somme de n nombres consécutifs est un multiple de n.

11 **Division euclidienne**

Soient x et y deux entiers naturels tels que :

$$x=27y+257\,.$$

Effectuer la division euclidienne de x par 27.

12 ★ **Une inégalité**

Montrer que : $\forall n\in\mathbb{N}^*, 4^n(n\,!)^3<(n+1)^{3n}$.

13 ★ **Equation diophantienne**

Résoudre dans $\mathbb{N}^3$ l'équation d'inconnue (x,y,z) :

$$10x+15y+6z=133\,.$$

14 **Division euclidienne**

Soit n un entier naturel non nul.

Effectuer la division euclidienne de 2^n-1 par 2^{n-1}.

15 **Division euclidienne**

Soit n un entier naturel.

Effectuer la division euclidienne de n^4+1 par n^2+1.

16 **Division euclidienne**

En divisant un nombre entier par 4, il reste 3 et en le divisant par 8, il reste 5.

Déterminer ce nombre.

17 **Division euclidienne**

1) Déterminer le reste de la division euclidienne de 1991^{1991} par 5.

2) Quel est le chiffre des unités dans l'écriture décimale de 1991^{1991} ?

18 **Division euclidienne**

Déterminer selon les valeurs de l'entier naturel n, les restes de la division euclidienne de n^4-2n^2-8 par 3.

19 **Equation et congruences**

Résoudre dans $\mathbb{Z}$ l'équation d'inconnue x :

$$x^2\equiv -1\ [5]\,.$$

20 **Ecriture décimale**

Démontrer que si un entier naturel a pour chiffre des unités 5 dans son écriture décimale, alors son carré se termine par 25.

21 **Ecriture d'un entier naturel en une base**

1) Un nombre s'écrit 10010011 en base 2. L'écrire en base 10.

2) Un nombre s'écrit 46326 en base 7. L'écrire en base 10.

3) Un nombre s'écrit 2**AE**50**B** en base 16. L'écrire en base 10.

22 **Ecriture d'un entier naturel en une base**

1) Ecrire le nombre $\overline{A012E}^{16}$ en base 2.

2) Ecrire le nombre $\overline{1234}^{5}$ en base 3.

23 **Divisibilité**

Démontrer que : $\forall (n,m)\in\mathbb{N}^2, 3\mid nm(n+m)(n-m)$.

24 **Division euclidienne**

Déterminer tous les entiers naturels n tels que $n+1$ divise n^2+1.

25 **Division euclidienne**

Déterminer le reste de la division euclidienne de $25\,043^{12\,345}$ par 11.

26 **Division euclidienne**

Déterminer les valeurs de l'entier naturel n pour lesquelles :

$$1+9^n+5^n+7^n\equiv 0\ [6]\,.$$

27 **Division euclidienne**

Montrer que, pour tout entier naturel n :

$$5^n+4n+7\equiv 0\ [8]\,.$$

Les exercices du chapitre 9

28 ★ **Division euclidienne**

Déterminer le chiffre des unités dans l'écriture décimale de 7^{7^7}.

29 **Congruences**

Démontrer que si un entier naturel est congru à 3 modulo 4, alors il ne peut pas s'écrire comme la somme de deux carrés.

30 **Congruences**

Démontrer que : $\forall n \in \mathbb{N}, (2n+1)^2 \equiv 1\ [8]$.

31 **Congruences**

Soient m et n deux entiers relatifs.

Montrer que si $m^2+n^2 \equiv 0\ [7]$, alors $m \equiv 0\ [7]$ et $n \equiv 0\ [7]$.

32 **Division euclidienne**

Déterminer le chiffre des unités dans l'écriture décimale de $1997^{1999^{2001}}$.

33 **Ecriture d'un entier naturel en une base**

Soit b un entier naturel supérieur ou égal à 3.

On considère les nombres entiers $\overline{20}^b$, $\overline{33}^b$ et $\overline{1100}^b$.

Trouver cette base (donc b) sachant que $\overline{20}^b \times \overline{33}^b = \overline{1100}^b$.

34 **Congruences** 🖫

Soit n un entier relatif.

1) Montrer que si n est pair, alors $n^2 \equiv 0\ [8]$ ou $n^2 \equiv 4\ [8]$.

2) Montrer que si n est impair, alors $n^2 \equiv 1\ [8]$.

35 **Divisibilité**

1) Montrer que : $\forall n \in \mathbb{N}-\{0,1\}, 2^n \mid 5^{2^{n-2}}-1$.

2) Montrer que : $\forall n \in \mathbb{N}-\{0,1\}, \neg(2^{n+1} \mid 5^{2^{n-2}}-1)$.

36 ★ **Divisibilité**

Montrer que : $\forall n \in \mathbb{N}^*, 2n+1 \mid \sum_{k=1}^{2n} \frac{(2n)!}{k}$.

37 **Divisibilité**

Montrer que : $\forall n \in \mathbb{N}^*, 40^n \cdot n! \mid (5n)!$.

38 **Divisibilité**

Montrer que le seul entier naturel n supérieur ou égal 2 tel que $2n-1$ divise $(3n^2-3n+1)(3n^2-3n+2)$ est 3.

39 ★ **Divisibilité**

Montrer que : $\forall n \geqslant 4, \exists k \in \mathbb{N}, \begin{cases} n! < k < (n+1)! \\ n^3 \mid k \end{cases}$.

40 **Divisibilité**

Soient a, b, c et d des entiers relatifs tels que $ad+bc \neq 0$.

On suppose que $ad+bc$ divise a, b, c et d.

Montrer alors que :

$$ad+bc \in \{-1,1\}.$$

41 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x,y) :

$$15x^2 = 9+7y^2.$$

42 **Divisibilité**

Montrer que : $\forall (a,b,c) \in \mathbb{Z}^3, a+b+c \mid a^3+b^3+c^3-3abc$.

43 ★ **Divisibilité**

On note $d : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ l'application qui, à chaque entier naturel n non nul, associe le nombre de diviseurs supérieur ou égaux à 1 de n.

Montrer que :

$$\forall a \in \mathbb{N}-\{0,1\}, \forall n \in \mathbb{N}^*, d(n) \leqslant d(a^n-1).$$

44 **Divisibilité** 🖫

Soient n et k deux entiers naturels non nuls, $d_1, ..., d_k$ des diviseurs de n compris entre 1 et n (au sens large) tels que :

$$d_1 < ... < d_k.$$

Montrer que :

$$\left(\prod_{i=1}^{k} d_i\right)^2 = n^k.$$

45 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x,y) :

$$2x+3y = xy.$$

46 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x,y) :

$$x^2-y^2-x+3y = 30.$$

47 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^* \times \mathbb{Z}^*$ l'équation d'inconnue (x,y) :

$$\frac{1}{x}+\frac{1}{y} = \frac{1}{5}.$$

48 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x,y) :

$$x^2-3xy+2y^2+x-3y-6 = 0.$$

49 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x,y) :

$$2x^3+xy-7 = 0.$$

50 **Equation diophantienne**

Résoudre dans $\mathbb{N}^2$ l'équation d'inconnue (x,y) :

$$x^3+xy+y^3 = 209.$$

51 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x,y) :

$$x(x+1)(x+7)(x+8) = y^2.$$

52 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x,y) :

$$x^2 = 9y^2-39y+40.$$

53 **Equation diophantienne**

Résoudre dans $\mathbb{N}^2$ l'équation d'inconnue (x,y) :

$$3^x = 8+y^2.$$

Les exercices du chapitre 9

54 **Equation diophantienne**

Résoudre dans $\mathbb{N}^3$ le système d'équations d'inconnu (x, y, z) :

$$\begin{cases} x^3 - y^3 - z^3 = 3xyz \\ x^2 = 2(y+z) \end{cases}.$$

55 **Equation diophantienne**

Résoudre dans $(\mathbb{N}^*)^3$ le système d'équations d'inconnu (x, y, z) :

$$\begin{cases} z^2 = x^2 + y^2 \\ xy = 2(x+y+z) \end{cases}.$$

56 **Divisibilité**

Montrer que, pour tout entier naturel n :

1) $5 \mid 2^{2n+1} + 3^{2n+1}$ 2) $9 \mid 4^n - 1 - 3n$.

57 **Divisibilité**

Montrer que, pour tout entier naturel n :

1) $11 \mid 3^{n+3} - 4^{4n+2}$ 2) $16 \mid 5^n - 1 - 4n$.

58 **Divisibilité**

Montrer que, pour tout entier naturel n :

1) $17 \mid 2^{6n+3} + 3^{4n+2}$ 2) $17 \mid 2^{7n+1} + 3^{2n+1} + 5^{10n+1} + 7^{6n+1}$.

59 **Divisibilité**

Montrer que, pour tout entier naturel n :

1) $18 \mid 2^{2n+2} + 24n + 14$ 2) $19 \mid 2^{3n+4} + 3^{3n+1}$.

60 **Divisibilité**

Montrer que, pour tout entier naturel n :

1) $19 \mid 2^{2^{6n+2}} + 3$ 2) $21 \mid 2^{4^{n+1}} + 5$.

61 **Divisibilité**

Montrer que, pour tout entier naturel n :

1) $25 \mid 2^{n+2} \times 3^n + 5n - 4$ 2) $29 \mid 2^{5n+1} + 3^{n+3}$.

62 **Divisibilité**

Montrer que, pour tout entier naturel n :

1) $31 \mid 2^{4n+1} + 3^{6n+9}$ 2) $32 \mid 8n^2 + 4n - 3(5^n - 1)$.

63 **Divisibilité**

Montrer que, pour tout entier naturel n :

1) $33 \mid 5^{2n+1} + 11^{2n+1} + 17^{2n+1}$ 2) $41 \mid 5 \times 7^{2n+2} + 2^{3n}$.

64 **Divisibilité**

Montrer que, pour tout entier naturel n :

1) $73 \mid 9^{2n+1} + 8^{n+2}$ 2) $111 \mid 10^{6n} + 10^{3n} - 2$.

65 **Divisibilité**

Montrer que, pour tout entier naturel n :

1) $288 \mid 7^{2n+1} - 48n - 7$ 2) $2304 \mid 7^{2n} - 2352n - 1$.

66 **Divisibilité**

Soient a un entier relatif impair et n un entier naturel supérieur ou égal à 3.

Montrer que :

$$a^{2^{n-2}} \equiv 1 \,[2^n].$$

67 **Divisibilité** 🖫

Montrer que : $\forall (a, b, c) \in \mathbb{Z}^3, 7 \mid a^3 + b^3 + c^3 \Rightarrow 7 \mid abc$.

68 **Divisibilité**

Déterminer tous les entiers relatifs n tels que :

$$10 \mid n^2 + (n+1)^2 + (n+3)^2.$$

69 **Divisibilité**

Déterminer tous les entiers naturels n tels que :

$$8 \mid 3^n + 4n + 1.$$

70 **Divisibilité**

Déterminer tous les entiers naturels n tels que :

1) $21 \mid 2^{2n} + 2^n + 1$ 2) $7 \mid 2^{2^n} + 2^n + 1$.

71 **Divisibilité**

Montrer que : $\forall n \in \mathbb{N} - \{0, 1\}, \neg(2^n \mid 3^n + 1)$.

72 ★ **Divisibilité**

Montrer que : $\forall (a, b) \in \mathbb{N}^2, \neg(23 \mid 2^a + 3^b)$.

73 **Equation diophantienne**

Montrer que l'équation suivante d'inconnue (x, y) n'a pas de solution dans $\mathbb{Z}^2$:

$$x^2 + 5y^2 = 3.$$

74 **Equation diophantienne**

Montrer que l'équation suivante d'inconnue (x, y) n'a pas de solution dans $\mathbb{Z}^2$:

$$x^2 - 5y^2 = 3.$$

75 **Equation diophantienne**

Montrer que l'équation suivante d'inconnue (x, y) n'a pas de solution dans $\mathbb{Z}^2$:

$$15x^2 - 7y^2 = 9.$$

76 **Equation diophantienne**

Montrer que l'équation suivante d'inconnue (x, y, z) n'a pas de solution dans $\mathbb{Z}^3$:

$$x^2 + y^2 - 8z - 6 = 0.$$

77 **Equation diophantienne**

Montrer que l'équation suivante d'inconnue (x, y) n'a pas de solution dans $\mathbb{Z}^2$:

$$x^3 - 3y^3 + 6y^2 - 16x + 8 = 0.$$

78 **Equation diophantienne**

Montrer que l'équation suivante d'inconnue (x, y) n'a pas de solution dans $\mathbb{N}^* \times \mathbb{N}^*$:

$$x^3 + 11^3 = y^3.$$

79 **Congruences**

Quel est le dernier chiffre dans l'écriture décimale de $\sum_{k=1}^{10} k^{100}$?

Les exercices du chapitre 9

80 ★ **Equation diophantienne**

Résoudre dans $(\mathbb{N}^*)^3$ le système d'équations d'inconnu (x, y, z) :

$$\begin{cases} x + y \equiv 1\,[z] \\ y + z \equiv 1\,[x] \\ z + x \equiv 1\,[y] \end{cases}.$$

81 **Congruences**

Soit n un entier relatif.

Montrer que si n est impair, alors $n^4 \equiv 1\,[16]$.

82 **Divisibilité**

Montrer que : $\forall n \in \mathbb{N}^*, 5 \mid 1^n + 2^n + 3^n + 4^n \Leftrightarrow \neg(4 \mid n)$.

83 **Congruences**

Soient a et b deux entiers naturels tels que $a \geqslant 4b$.

Montrer que :

$$3^a + 1 \equiv 0\,[10] \Rightarrow \begin{cases} 3^{a+4b} + 1 \equiv 0\,[10] \\ 3^{a-4b} + 1 \equiv 0\,[10] \end{cases}.$$

84 ★ **Nombres de Fermat** 🖫

Pour tout entier naturel n non nul, on note $F_n = 2^{2^n} + 1$.

Montrer que :

$$\forall n \in \mathbb{N}^*, F_n \mid 2^{F_n} - 2.$$

85 **Divisibilité**

Montrer que : $\forall (x, y) \in \mathbb{Z}^2, 17 \mid 2x + 3y \Leftrightarrow 17 \mid 9x + 5y$.

86 **Equation du second degré dans Z/nZ**

On admet que le triplet $(\mathbb{Z}/13\mathbb{Z}, +, \times)$ est un corps.

Résoudre dans $\mathbb{Z}/13\mathbb{Z}$, l'équation d'inconnue x :

$$x^2 + x + \overline{7} = \overline{0}.$$

87 **Equation du second degré dans Z/nZ**

Résoudre dans $\mathbb{Z}/12\mathbb{Z}$, l'équation d'inconnue x :

$$x^2 - \overline{4}x + \overline{3} = \overline{0}.$$

88 ★ **Divisibilité** 🖫

Etant donné cinq entiers relatifs, montrer qu'il en existe nécessairement trois dont la somme est divisible par 3.

89 **Ecriture d'un nombre en une base**

Soit b un entier naturel supérieur ou égal à 2.

Dans la base b, un nombre s'écrit $\overline{1254}^b$ et son double $\overline{2541}^b$.

Quel est ce nombre et quelle est la base ?

90 **Numération**

Soit n un entier compris entre 100 et 999.

Déterminer le produit de $7n$ par 143.

91 **Devinette**

Quel est le plus petit entier naturel divisible par chacun des nombres entiers de 1 à 10 ?

92 **Divisibilité** 🖫

Soient a et b deux entiers relatifs.

Montrer que l'un des nombres a, b, $a + b$, $a - b$ est divisible par 3.

93 **Divisibilité**

Soient a, b et c des entiers naturels tels que :

$$a^2 = b^2 + c^2.$$

Montrer que :

1) l'un au moins des entiers b et c est divisible par 3 ;

2) l'un au moins des entiers a, b et c est divisible par 5 ;

3) l'un au moins des entiers b et c est divisible par 2 ;

4) l'un au moins des entiers b et c est divisible par 4.

94 **Ecriture d'un nombre entier en une base**

Soit b un entier naturel supérieur ou égal à 2.

L'entier 341 (en base 10) s'écrit $\overline{2331}^b$ en base b.

Déterminer la base b.

95 **Equation diophantienne**

Résoudre dans $\mathbb{Z}$ le système d'équations d'inconnu n :

$$\begin{cases} 4n + 1 \equiv 0\,[5] \\ 4n + 1 \equiv 0\,[7] \end{cases}.$$

96 **Division euclidienne**

Soit a un entier relatif.

1) Montrer que le reste de la division euclidienne de a^2 par 8 est égal à 0, 1 ou 4.

Soit n un entier naturel.

2) Montrer que si 8 divise $n - 7$, alors n ne peut pas être la somme de trois carrés d'entiers.

97 **Division euclidienne**

Quel est le dernier chiffre dans l'écriture décimale de $7^{3^{3^4}}$?

98 **Divisibilité**

Déterminer l'ensemble des entiers relatifs n tels que $n^2 + 7 \mid n^3 + 5$.

99 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x, y) :

$$x^2 = 9y^2 - 39y + 40.$$

100 **Equation diophantienne**

1) Montrer que l'équation d'inconnue (x, y), $x^2 - 3y^2 = 17$ n'a pas de solution dans $\mathbb{Z}^2$.

2) Montrer que l'équation d'inconnue (x, y), $x^3 + y^3 = 3$ n'a pas de solution dans $\mathbb{Z}^2$.

101 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x, y) :

$$x^2 + y^2 - 2x + 4y - 5 = 0.$$

102 **Divisibilité**

Montrer que : $\forall (a, b) \in \mathbb{Z}^2, 24a^2 + 1 = b^2 \Rightarrow 5 \mid ab$.

103 ★ **Equation diophantienne**

Montrer que le système d'équations d'inconnu (x, y, z) suivant, n'a pas de solution dans $\mathbb{Z}^3$:

$$\begin{cases} x^3 + y^3 + z^3 = 7 \\ xyz = 7(x^2 + y^2 + z^2) + 1 \end{cases}.$$

Les exercices du chapitre 9

104 **Congruences**

Montrer que : $\forall n \in \mathbb{N}, 13 \mid 2^{2^{8n+6}} + 10$.

105 **Divisibilité**

Montrer que : $\forall n \in \mathbb{N}, 14 \mid 3^{4n+2} + 5^{2n+1}$.

106 **Division euclidienne**

Soit n un entier naturel non nul.

Déterminer le reste de la division euclidienne de 10^{10^n} par 7.

107 ★★★ **Equation diophantienne**

Soit n un entier naturel supérieur ou égal à 3.

On considère l'équation d'inconnue (x, y, z) :

$$x^n + y^n = z^n .$$

Montrer qu'elle admet aucune solution dans $\mathbb{Z}^3 \setminus \{(0,0,0)\}$.

108 **Divisibilité** 🖫

Soient n un entier naturel non nul et d un diviseur positif de n.

1) Montrer que :

$$\forall a \in \mathbb{N}^*, a^d - 1 \mid a^n - 1 .$$

2) Montrer que $2^{100} - 1$ est divisible par 3 et par 31.

109 **Devinette**

Soit n un entier naturel carré d'un nombre entier.

On suppose qu'en base 10, son écriture décimale est composée de quatre chiffres tous inférieurs ou égaux à 6.

Si on ajoute 3 à chacun de ces chiffres, on obtient encore un carré parfait.

Trouver le nombre n.

110 **Equation diophantienne**

Résoudre dans $\mathbb{N}^3$ puis dans $\mathbb{Z}^3$ l'équation d'inconnue (x, y, z) :

$$10x + 15y + 6z = 73 .$$

111 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ le système d'équations d'inconnu (x, y) :

$$\begin{cases} x - 2y + z = 0 \\ x + 2y - 2z = 1 \end{cases} .$$

112 **Divisibilité**

Montrer que : $\forall (m, n) \in \mathbb{Z}^2, 7 \mid m^2 + n^2 \Leftrightarrow \begin{cases} 7 \mid m \\ 7 \mid n \end{cases}$.

113 **Equation diophantienne**

Résoudre dans $\mathbb{N}^2$ les équations d'inconnues (x, y) :

1) $2^x - 5^y \equiv 3\ [24]$ 2) $2^x - 5^y \equiv 5\ [24]$.

114 **Divisibilité**

Dans chacun des cas, déterminer les ensembles.

1) $\{n \in \mathbb{Z}, n - 1 \mid n + 3\}$ 2) $\{n \in \mathbb{Z}, n + 2 \mid n^2 + 2\}$.

115 **Divisibilité**

Montrer que $11 \mid 2^{123} + 3^{121}$.

116 ★ **Equation diophantienne**

Montrer que : $\forall a \in \mathbb{Z}, \exists (x, y) \in \mathbb{Z}^2, x^2 - y^2 = a^3$.

117 **Division euclidienne**

Quel est le reste de la division euclidienne de l'entier $1234^{4321} + 4321^{1234}$ par 7 ?

118 **Divisibilité**

Montrer que pour tout entier naturel n :

1) $6 \mid 5n^3 + n$ 2) $7 \mid 3^{2n+1} + 2^{n+2}$ 3) $11 \mid 3^{8n} \times 5^4 + 5^{6n} \times 7^3$

4) $15^2 \mid 16^n - 1 - 15n$.

119 **Division euclidienne**

1) Calculer le reste de la division euclidienne de $1986^{10\,000}$ par 31.

2) Calculer le reste de la division euclidienne de $51\,200^{2^{100}}$ par 41.

3) Calculer le reste de la division euclidienne de $1\,035\,125^{5642}$ par 17.

120 **Congruences**

1) Vérifier que $10^6 \equiv 1\ [7]$.

2) En déduire que :

$$\sum_{k=1}^{10} 10^{10^k} \equiv 5\ [7] .$$

121 **Divisibilité**

Montrer que pour tout entier naturel n :

1) $7 \mid 4^{2^n} + 2^{2^n} + 1$ 2) $9 \mid 2^{2n} + 15n - 1$.

122 **Divisibilité** 🖫

Soient a, b et c des entiers relatifs.

Montrer que si 9 divise $a^3 + b^3 + c^3$, alors 3 divise a ou b ou c.

123 ★★ **Comme aux olympiades !**

Soit A la somme des chiffres du nombre 4444^{4444} et B la somme des chiffres de A.

Trouver la somme des chiffres de B.

On pourra utiliser la preuve par 9.

D'après les olympiades 1975.

124 ★★ **Equation diophantienne**

Résoudre dans $\mathbb{N}^2$ l'équation d'inconnue (m, n) :

$$2^m - 3^n = 1 .$$

D'après lycée Louis-Le-Grand

125 **Divisibilité**

Pour tout entier naturel n non nul, on pose :

$$u_n = \sum_{k=1}^{n} k^2 k ! .$$

Montrer que $9 \mid u_n$ si et seulement si $n \neq 1$ et $n \neq 4$.

126 **Divisibilité** 🖫

Trouver tous les triplets (x, y, z) de $(\mathbb{N}^*)^3$ tels que :

$$x \mid y + z , \ y \mid z + x \text{ et } z \mid x + y .$$

127 ★ **Equation diophantienne**

Soient a et b deux entiers relatifs non nuls.

Montrer que l'équation suivante, d'inconnue (x, y) n'a pas de solution sans $(\mathbb{Z}^*)^2$:

$$(a^2 - b^2)x^2 - 4abxy - (a^2 - b^2)y^2 = 1 .$$

Les exercices du chapitre 9

128 ★ **Equation diophantienne**

Montrer que l'équation suivante, d'inconnue (x,y,z) n'a pas de solution dans $\mathbb{Z}^3$:

$$x^4+y^4+z^4-2y^2z^2-2z^2x^2-2x^2y^2=120\,.$$

129 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x,y) :

$$3x^2+xy-11=0\,.$$

130 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^3$ l'équation d'inconnue (x,y,z) :

$$x^3+y^3+z^3=(x+y+z)^3\,.$$

131 **Divisibilité**

Montrer que : $\forall n\in\mathbb{Z},\neg(169\mid n^2+20n+74)$.

132 **Divisibilité**

Montrer que : $\forall x\in\mathbb{N}-\{0,1\},\forall(n,k)\in(\mathbb{N}^*)^2,k\mid x^2-x\Rightarrow k\mid x^n-x$.

133 **Divisibilité**

1) Montrer que : $\forall n\in\mathbb{Z},9\mid n^3+(n+1)^3+(n+2)^3$.

2) Montrer que : $\forall n\in\mathbb{N},(2^n-1)^2\mid 2^{(2^n-1)n}-1$.

134 **Divisibilité**

Montrer que pour tout entier naturel n non nul :

1) $11\mid 2^{6n-5}+3^{2n}$ 2) $17\mid 3\times5^{2n-1}+2^{3n-2}$.

135 **Divisibilité**

1) Montrer que : $\forall n\in\mathbb{Z},120\mid n^5-5n^3+4n$.

2) Montrer que : $\forall n\in\mathbb{N},225\mid 4^{2n+2}-15n-16$.

136 **Divisibilité**

1) Montrer que : $\forall n\in\mathbb{Z},7\mid n(9n^2-1)(n^2-1)(4n^2-1)$.

2) Montrer que : $\forall n\in\mathbb{N},7\mid 4^{3n+1}+2^{3n+1}+1$.

137 **Divisibilité**

1) Montrer que : $\forall n\in\mathbb{N}-\{0,1\},8\mid 5^n+2\times3^{n-1}+1$.

2) Montrer que : $\forall n\in\mathbb{N},9\mid n4^{n+1}-(n+1)4^n+1$.

138 **Divisibilité**

Montrer que pour tout entier naturel n :

1) $11\mid 2^{6n+3}+3^{2n+1}$ 2) $13\mid 2^{4n+2}+3^{4n+2}$.

139 **Divisibilité**

1) Montrer que : $\forall n\in\mathbb{N},35\mid 3^{6n}-2^{6n}$.

2) Montrer que : $\forall n\in\mathbb{N},169\mid 3^{3n+3}-26n-27$.

140 **Divisibilité**

Soit n un entier naturel impair.

Montrer que :

$$512\mid n^{12}-n^8-n^4+1\,.$$

141 **Divisibilité**

Montrer que : $\forall n\in\mathbb{N},1897\mid 2903^n-803^n-464^n+261^n$.

142 **Divisibilité**

Montrer que : $\forall n\in\mathbb{N},n^2\mid(n+2)^{n+2}-2^{n+2}(n+1)^{n+1}$.

On pourra anticiper sur les coefficients binomiaux comme pour l'exercice 133-2.

143 **Division euclidienne**

Quel est le reste de la division euclidienne de 2792^{217} par 5 ?

144 **Division euclidienne**

Soient a un entier naturel supérieur ou égal à 3, b un entier supérieur ou égal à 2 et n un entier naturel non nul.

On note q le quotient de la division euclidienne de $a-1$ par b.

Calculer le quotient de la division euclidienne de ab^n-1 par b^{n+1}.

145 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^3$ l'équation d'inconnue (x,y,z) :

$$2x+3y+5z=1\,.$$

146 **Equation diophantienne**

Résoudre dans $\mathbb{N}^3$ l'équation d'inconnue (x,y,z) :

$$14x+15y+16z=247\,.$$

147 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^3$ le système d'équation d'inconnu (x,y,z) :

$$\begin{cases}2x+5y-11z=1\\x-12y+7z=2\end{cases}.$$

148 ★ **Division euclidienne**

Trouver tous les entiers naturels n tels que $1\leqslant n\leqslant105$, sachant que les restes des divisions euclidiennes de n par 3, 5 et 7 sont respectivement 1, 2 et 3.

149 **Divisibilité**

Trouver tous les entiers relatifs x tels que :

$$7\mid3x-10\,,\ 17\mid11x+8\ \text{ et }\ 5\mid16x-1\,.$$

150 **Equation diophantienne**

Résoudre dans $\mathbb{Z}$ le système d'équation d'inconnu x :

$$\begin{cases}x\equiv2\ [7]\\x\equiv1\ [8]\\x\equiv3\ [9]\end{cases}.$$

151 **Equation diophantienne**

Résoudre dans $\mathbb{N}^2$ l'équation d'inconnue (x,y) :

$$2^x-5^y\equiv1\ [24]\,.$$

152 ★ **Divisibilité**

Soient n un entier naturel tel que $n\geqslant3$ et $(a_1,...,a_{2n+1})\in\mathbb{Z}^{2n+1}$.

Montrer que :

$$9\mid\sum_{k=1}^{2n+1}a_k^3\Rightarrow3\mid\prod_{k=1}^{2n+1}a_k\,.$$

153 **Congruences**

Montrer qu'un entier relatif congru à 7 modulo 8 ne peut pas être la somme de trois carrés d'entiers.

Les exercices du chapitre 9

154 **Equation diophantienne**

Montrer que chacune des équations d'inconnues (x, y, z) :

$$x^3 + y^3 + z^3 = 94 \text{ et } x^3 + y^3 + z^3 = 95,$$

n'admet aucune solution dans $\mathbb{Z}^3$.

On pourra passer modulo 9.

155 **Divisibilité**

Montrer que : $\forall n \in \mathbb{N}, \neg(7 \mid 2^n + 3^n + 5^n)$.

156 **Carré parfait**

Montrer que pour tout entier naturel n, la somme $\sum_{k=0}^{4} (n+k)^2$ n'est le carré d'aucun entier.

On pourra passer modulo 25.

157 **Divisibilité**

On considère la suite u définie par :

$$\forall n \in \mathbb{N} - \{0, 1\}, u_n = 2^n - 3.$$

Montrer que cette suite comporte une infinité de termes divisibles par 5, une infinité de termes divisibles par 13 mais aucun terme divisible par 65.

158 **Equation diophantienne**

Résoudre dans $(\mathbb{N}^*)^2$ l'équation d'inconnue (x, y) :

$$\sum_{k=1}^{x} k\,! = y^2.$$

159 ★★ **Divisibilité** 🖫

Soient $n \in \mathbb{N}^*$ et $(a_1, ..., a_n) \in (\mathbb{N}^*)^n$.

Montrer qu'il existe une partie non vide E de $\{1, ..., n\}$ telle que la somme $\sum_{k \in E} a_k$ soit divisible par n.

160 **Carré parfait**

Soit a un entier naturel non nul.

Montrer que les entiers $a^4 + a^2 + 3$ et $a^4 + 12a^2 + 4$ ne sont pas des carrés parfaits.

161 ★ **Carré parfait** 🖫

Soient a, b et c trois entiers relatifs impairs.

Montrer que ni l'entier $ab + bc + ca$ ni l'entier $2(ab + bc + ca)$ ne peuvent être des carrés d'entiers.

162 ★ **Equation diophantienne** 🖫

Soient p un entier naturel et l'équation d'inconnue (x, y, z) :

$$x^2 + y^2 = pz^2 \quad (*).$$

Montrer que si $p \in \{3, 7, 11\}$, alors l'équation $(*)$ n'a pas de solution dans $\mathbb{Z}^3 \setminus \{(0, 0, 0)\}$.

163 **Carré parfait**

1) Montrer que l'équation d'inconnue u, $u^2 \equiv 12\ [17]$ n'a pas de solution dans $\mathbb{Z}$.

2) En déduire l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ tels que :

$$x^2 + 3xy - 2y^2 = 122.$$

164 ★★ **Congruences**

Montrer que :

$\forall (a, b, c, d) \in \mathbb{Z}^4, a^2 + 5b^2 - 2c^2 - 2cd - 3d^2 = 0 \Rightarrow a = b = c = d = 0$.

On pourra passer modulo 5.

165 ★★ **Equation diophantienne**

Résoudre dans $\mathbb{Z}^3$ l'équation d'inconnue (x, y, z) :

$$x^2 + y^2 + z^2 = x^2y^2.$$

166 ★★ **Equation diophantienne** 🖫

On considère l'équation d'inconnue (x, y, z) :

$$x^2 + y^2 + z^2 = 2xyz.$$

Montrer qu'elle n'admet pas de solution dans $\mathbb{Z}^3 \setminus \{(0, 0, 0)\}$.

167 ★★ **Equation diophantienne**

Soit n un entier naturel.

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x, y) :

$$x^2 + y^2 = 2^n.$$

168 ★ **Entiers naturels**

Soit E l'ensemble définit par l'égalité :

$$E = \{n \in \mathbb{N}, \exists (a, b, c) \in \mathbb{N}^3, n = a^2 + b^2 + c^2\}.$$

1) Montrer que $E \neq \mathbb{N}$.

2) Montrer que E n'est stable ni pour l'addition, ni pour la multiplication.

3) Démontrer que :

$$\forall n \in E, \forall k \in \mathbb{N}^*, n^k \in E.$$

169 ★ **Entiers naturels**

Montrer que : $\forall (a, b, c) \in (\mathbb{N}^*)^3, (2^a - 1)(2^b - 1) \neq 2^c + 1$.

170 ★★ **Entiers naturels**

Soit E l'ensemble définit par l'égalité :

$$E = \{2^a \times 3^b, (a, b) \in \mathbb{N}^2\}.$$

1) Montrer que tout entier supérieur ou égal à 1 peut être décomposé en une somme d'éléments de E dont aucun n'est un multiple d'un autre.

2) Ecrire alors l'entier 19 avec les contraintes citées plus haut.

171 ★★★ **Nombre de Fermat et équation**

Soient k un entier naturel supérieur ou égal à 3 et u la suite définie par :

$$u_0 = 1,\ u_1 = k \text{ et } \forall n \in \mathbb{N}, u_{n+2} - 2u_{n+1} + u_n = k - 2.$$

On pose pour tout entier naturel m, $F_m = 2^{2^m} + 1$.

Résoudre dans $\mathbb{N}^2$ l'équation d'inconnue (n, m) :

$$u_n = F_m.$$

172 **Divisibilité**

Montrer que : $\forall (a, b) \in \mathbb{Z}^2, 11 \mid a^2 + b^2 \Leftrightarrow \begin{cases} 11 \mid a \\ 11 \mid b \end{cases}$.

173 **Divisibilité**

Pour tout entier naturel n, on pose :

$$P_n = \prod_{k=1}^{n} (n + k).$$

Montrer que : $\forall n \in \mathbb{N}, 2^n \mid P_n$.

Les exercices du chapitre 9

174 **Equation diophantienne**

Résoudre dans $\mathbb{N}^2$ l'équation d'inconnue (x, y) :

$$9y^2 - (x+1)^2 = 32\,.$$

175 ★ **Comme aux oraux !**

Déterminer les deux derniers chiffres de l'écriture décimale de :

$$\sum_{k=1}^{2010} k\,!\,.$$

D'après lycée Louis-Le-grand (MPSI 2010)

176 **Divisibilité**

Montrer que la différence des cubes de deux entiers naturels consécutifs n'est jamais divisible par 5.

177 **Division euclidienne** 🖫

Soit k un entier naturel.

1) Quels sont les restes possibles de la division de k^2 par 4 ?

On pose, pour tout entier naturel n supérieur ou égal à 2 :

$$a_n = \underbrace{11...11}_{n \text{ chiffres}}\,.$$

2) Montrer que pour tout entier naturel n supérieur ou égal à 2, a_n n'est pas un carré parfait.

178 ★ **Division euclidienne**

Soit n un entier naturel.

1) Quels sont les restes possibles de la division de 10^n par 27 ?

2) L'entier naturel :

$$999\,888\,777\,666\,555\,444\,333\,222\,111\,,$$

est-il divisible par 27 ?

179 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x, y) :

$$4x^2 - xy - 17 = 0\,.$$

180 **Equation diophantienne**

Existe-t-il des couples $(x, y) \in \mathbb{Z}^2$ solutions de l'équation :

$$(x+1)^3 - x^3 = 5y + 3 \ ?$$

181 **Equation diophantienne**

Existe-t-il des triplets $(x, y, z) \in \mathbb{Z}^3$ solutions de l'équation :

$$x^2 - 2y^2 + 8z = 3 \ ?$$

182 ★ **« Grand théorème de Fermat »** 🖫

Soit n un entier naturel pair.

On considère l'équation d'inconnue (x, y, z) :

$$x^n + y^n = z^n\,.$$

Montrer qu'aucun triplet $(x, y, z) \in (\mathbb{N}^*)^3$ où x et y sont impairs n'est solution de cette équation.

183 ★ **Carré parfait**

1) Montrer que tout nombre entier impair peut être écrit comme différence de deux carrés d'entiers.

2) En est-il de même pour les entiers pairs ?

184 **Carré parfait**

Montrer que : $\forall n \in \mathbb{N}^*, (2 \mid 3^{2^n} + 1) \wedge \neg(4 \mid 3^{2^n} + 1)\,.$

185 ★ **Ecriture d'un entier naturel en une base**

Soient a et b deux entiers naturels.

On écrit $\overline{aabb}$ l'écriture en base 10 d'un entier naturel n.

Déterminer parmi ces entiers n ceux qui sont des carrés d'entiers.

186 ★ **Divisibilité**

Déterminer le plus grand entier naturel n non nul pour lequel $n^3 + 100$ est divisible par $n + 10$.

187 **Congruences** 🖫

Soit n un entier relatif.

Montrer que $n^2 \equiv 0\ [3]$ ou $n^2 \equiv 1\ [3]$.

188 **Congruences** 🖫

Soit n un entier relatif.

Montrer que $n^2 \equiv 0\ [4]$ ou $n^2 \equiv 1\ [4]$.

189 **Congruences** 🖫

Soit n un entier relatif.

Montrer que $n^2 \equiv -1\ [5]$ ou $n^2 \equiv 0\ [5]$ ou $n^2 \equiv 1\ [5]$.

190 **Congruences** 🖫

Soit n un entier relatif.

Montrer que $n^3 \equiv -1\ [9]$ ou $n^3 \equiv 0\ [9]$ ou $n^3 \equiv 1\ [9]$.

191 **Congruences** 🖫

Soit n un entier relatif.

Montrer que $n^4 \equiv 0\ [16]$ ou $n^4 \equiv 1\ [16]$.