COURS D'ARITHMÉTIQUE 2018 - 2019

Dr Goli Etienne

UNIVERSITÉ
POLYTECHNIQUE
DE BINGERVILLE

Table des matières

Notations

Notation	Définition
$\mathbb{N}$	Ensemble des entiers naturels
$\mathbb{Z}$	Ensemble des entiers relatifs
$\mathbb{R}$	Ensemble des nombres réels
Im	Image d'une application
$\ker$	Noyau d'une application linéaire
|.|	Valeur absolue
$\|\cdot\|_X$	Application norme sur l'ensemble X
$\oplus$	La somme directe
$\sum$	Symbole de sommation
$\prod$	Symbole du produit
$\circ$	La composition des applications
$\cap$	L'intersection
$\cup$	L'union
$\neq$	La non égalitïé
$\subset$	L'inclusion
$\in$	Appartenance
$\notin$	non Appartenance
$\forall$	Symbole universel "pour tout"
$\exists$	Symbole universel "il existe"
$u^{(k)}$	Dérivée d'ordre k de u définie sur une partie de $\mathbb{R}$
$a\|b$	a divise b
$E(x) = [x]$	partie enti‘ere de x
pgcd	plus grand commun diviseur
$a \wedge b$	$\mathrm{pgcd}(a, b)$
ppcm	plus petit commun multiple
$a \vee b$	$\mathrm{ppcm}(a, b)$
$a \equiv b[N]$	a est congru à b modulo N
$\overline{a_n ... a_0}^b$	écriture en base b
$n!$	factorielle de n : $n! = 1 \times 2 \times \ ... \ \times n$

C_n^k	coefficient binomial : $C_n^k = \frac{n!}{k!(n-k)!}$
$[[a, b]]$	$\{x \in \mathbb{Z} \mid a \leq x \leq b\}$

Chapitre 1

ARITHMÉTIQUE DANS $\mathbb{Z}$

1.1 Relation de divisibilité, division euclidienne dans $\mathbb{Z}$

1.1.1 Diviseurs, multiples

Définition 1.1.1. *Étant donnés deux entiers relatifs a et b, on dit que a est un* ***diviseur*** *de b, ou que b est un* ***multiple*** *de a, s'il existe $k \in \mathbb{Z}$ tel que $b = ka$.*

Notation 1.1.1.

- *Si d est un diviseur de a on note $d|a$.*
- *L'ensemble des diviseurs de a est noté $\mathcal{D}(a)$.*
- *L'ensemble des multiples de a est noté $\mathcal{M}(a)$ ou $a\mathbb{Z}$.*

Exemple 1.1.1.

- *1 et -1 divisent tous les entiers, mais ne sont divisibles que par 1 et -1.*
- *0 est un multiple de tous les entiers, mais n'est diviseur que de lui-même.*
- $\mathcal{D}(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Remarque 1.1.1.

- *La relation "divise" est réflexive et transitive, mais n'est pas une relation d'ordre dans $\mathbb{Z}$, car elle n'est pas antisymétrique.*
- *En revanche, d'après la proposition suivante, sa restriction à $\mathbb{N}$ est une relation d'ordre. Pour cet ordre, le plus petit élément de $\mathbb{N}$ est 1, et le plus grand 0.*
- *La divisibilité sur $\mathbb{N}^*$ est liée à l'ordre naturel de $\mathbb{N}^*$ par la relation :*

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

En effet, si $a|b$ alors $b = ka$ avec $k \in \mathbb{Z}$ et, puisque a et b sont strictement positifs, on a $k \in \mathbb{N}^*$ et par suite $b \geq a$.
Ce résultat est faux dans $\mathbb{N}$ puisque, par exemple, $1|0$.

Proposition 1.1.1. *On a :*

$$(a|b \quad et \quad b|a) \quad \Leftrightarrow \quad |a| = |b|.$$

Proposition 1.1.2. *Soient a et b deux entiers relatifs.*

1 *Si $(u, v) \in \mathbb{Z}^2$, alors :*

$$(d|a \quad et \quad d|b) \Rightarrow d|au + bv.$$

2 *Si x est un entier non nul, alors :*

$$a|b \Leftrightarrow ax|bx.$$

1.1.2 Critères de divisibilité

a) Critères de divisibilité par 2

Un entier est divisible par 2 si, et seulement s'il se termine par un 0, un 2, un 4, un 6 ou un 8.

Exemple 1.1.2.
1 576 et 279 834 sont divisibles par 2 car 1 576 se termine par 6 et 279 834 se termine par 4.

b) Critères de divisibilité par 3

Un entier est divisible par 3 si, et seulement si la somme de ses chiffres l'est.

Exemple 1.1.3.
471 et 8 643 sont divisibles par 3 car 4+7+1 = 12 et 8+6+4+3 = 21 et 12 et 21 sont divisibles par 3.

c) Critères de divisibilité par 4

Un entier est divisible par 4 si, et seulement si le nombre formé par ses deux derniers chiffres (en base 10) l'est.

Exemple 1.1.4.
276, 5 848 et 57 316 sont divisibles par 4 car 76, 48 et 16 le sont.

d) Critères de divisibilité par 5

Un entier est divisible par 5 si, et seulement s'il se termine par un 0 ou par un 5.

Exemple 1.1.5.
Les nombres 385 ; 780 ; 24 165 sont divisibles par 5.

e) Critères de divisibilité par 6

Un nombre est divisible par 6 s'il est divisible par 3 et par 2.

Exemple 1.1.6.
79 254 est divisible par 6 car 79 254 est divisible par 2 et par 3 en effet il se termine par 4 et 7+9+2+5+1 = 24 et 2+4 = 6.

f) Critères de divisibilité par 7

1ère méthode : **le chiffre des unités**

Etape 1 Supprimons le chiffre u des unités du nombre donné.

Etape 2 On retranche du nombre obtenu le double de u .

Le nombre initial est divisible par 7 si le nombre obtenu est divisible par 7.

Exemple 1.1.7.
Soit $a = 341$

Etape 1 *On supprime 1 on obtient 34.*

Etape 2 *34 - 2 = 32.*

32 n'est pas divisible par 7 donc 341 ne l'est pas non plus.

Exemple 1.1.8.
Soit $b = 182$

Etape 1 *On supprime 2 on obtient 18.*

Etape 2 *8 - 2×2 = 14.*

14 est pas divisible par 7 donc 182 l'est.

Exemple 1.1.9.
Soit $c = 17381$

Etape 1 *On supprime 1 on obtient 1738.*

Etape 2 *1738 - 2 = 1736.*

soit $d = 1736$

Etape 1 *On supprime 6 à 1736 on obtient 173.*

Etape 2 *173 - 2×6 = 161.*

soit $e = 161$

Etape 1 *On supprime 1 à 161 on obtient 16.*

Etape 2 *16 - 2 = 14.*

e est pas divisible par 7 donc $c = 17381$ *l'est aussi.*

2ème méthode : **Critère pour un grand nombre**
Supposons que l'on veuille savoir si un nombre contenant un grand nombre de chiffres est divisible par 7. Il suffit de séparer ce nombre par tranche de 3 chiffres en partant des unités et d'insérer alternativement des $-$ et des $+$ entre les tranches à partir du début du nombre en commençant par un $-$. On effectue l'opération ainsi écrite et si le résultat est divisible par 7, alors le nombre considéré est divisible par 7. Bien sûr pour voir si le résultat de l'opération précédente est divisible par 7, on peut utiliser la méthode de divisibilité par 7 exposée ci-dessus.

Exemple 1.1.10.
Soit le nombre 5527579818992. On le sépare par tranche de trois chiffres à partir des unités.

$$5|527|579|818|992.$$

On intercale alternativement des $+$ *et des* $-$ *à partir du début en commençant par un* $-$.

$$5 - 527 + 579 - 818 + 992.$$

On effectue l'opération ainsi écrite.

$$5 - 527 + 579 - 818 + 992 = 231$$

On regarde si 231 est divisible à l'aide de la méthode 1.

$$23 - 2 \times 1 = 21 = 7 \times 3$$

On trouve un résultat divisible par 7 donc 5527579818992 est divisible par 7.

g) Critères de divisibilité par 8

Un entier est divisible par 8 si, et seulement si le nombre formé par ses trois derniers chiffres (en base 10) l'est.

Exemple 1.1.11.
69 776 et 98 024 sont divisibles par 8 car $776 = 8 \times 97$ *et* $24 = 8 \times 3$.

h) Critères de divisibilité par 9

Un entier est divisible par 9 si, et seulement si la somme de ses chiffres l'est.

Exemple 1.1.12.
12 345 678 est divisible par 9 car 1+2+3+4+5+6+7+8 = 36 et 36 est divisible par 9.

i) Critères de divisibilité par 10

Un entier est divisible par 10 si, et seulement s'il se termine par un 0 (combine les critères pour 2 et 5).

Exemple 1.1.13.
10 ; 430 ; 45 134 980 sont divisibles par 10

j) Critères de divisibilité par 11

Un entier est divisible par 11 si, et seulement si la somme des ses chiffres (en base 10) de rang pair diminuée de la somme de ses chiffres de rang impair est divisible par 11.

Exemple 1.1.14.
54 967 est divisible par 11 car (7 + 9 + 5) - (6 + 4) = 11 l'est.

k) Critères de divisibilité par 25

Un nombre est divisible par 25 lorsque les deux chiffres de droite sont : 00, 25, 50 ou 75.

Exemple 1.1.15.
Le nombre 74 275 est divisible par 25, mais pas le nombre 5 555.

l) Critères de divisibilité par 100

Un nombre est divisible par 100 lorsque les deux chiffres de droite sont : 00.

Exemple 1.1.16.
335 000 et 152 000 sont divisibles par 100.

m) Critères de divisibilité par 125

un nombre est divisible par 125 lorsque les 3 chiffres de droite forment un nombre multiple de 125 : 125, 250, 375, 500, 625, 750, 875.

Exemple 1.1.17.
745 375 est divisible par 125.

n) Critères de divisibilité par 1000

Un nombre est divisible par 1000 lorsque les trois chiffres de droite sont : 000

Exemple 1.1.18.
335 000 et 152 000 sont divisibles par 1000.

1.1.3 Division euclidienne sur $\mathbb{Z}$

Théorème 1.1.1. *Soient a un entier relatif et b un entier naturel non nul. Il existe un unique couple d'entiers relatifs (q, r) tel que :*

$$a = bq + r \qquad \text{avec} \qquad 0 \leq r < b. \qquad (*)$$

- *q est appelé **quotient** de la division euclidienne de a par b,*
- *r est appelé **reste** de la division euclidienne de a par b.*

Remarque 1.1.2.

- *Si q est le quotient et r le reste de la division euclidienne de a par $b \neq 0$, on a l'équivalence :*

$$\forall q \in \mathbb{Z}, \quad q \leq \frac{a}{b} < q + 1 \Leftrightarrow bq \leq a < bq + b.$$

- *Si q est le quotient de la division euclidienne de l'entier naturel a par b, l'ensemble $A = \{n \in \mathbb{N} |\ nb \leq a\}$ est l'intervalle $[[0, q]]$.*
- *Étant donnés $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, notons q et r les quotient et reste de la division euclidienne de a par b.*
  - *Si $r = 0$, alors $a = bq$ et donc $b|a$.*
  - *Réciproquement, si $b|a$, alors on a $a = kb + 0$ avec $k \in \mathbb{Z}$ et $0 \leq 0 < b$. L'unicité de la division euclidienne nous donne donc $k = q$ et $r = 0$. On a donc l'équivalence $b|a \Leftrightarrow r = 0$.*

Exemple 1.1.19. *Voici des divisions euclidiennes*

$$\begin{array}{r|l} 12 & 5 \\ \hline 2 & 2 \end{array} \qquad \text{donc}$$

- ⋆ *Division de 12 par 5 : $12 = 5 \times 2 + 2$*
- ⋆ *Division de 12 par -5 : $12 = (-5) \times (-2) + 2$*
- ⋆ *Division de -12 par 5 :$-12 = 5 \times (-3) + 2$*
- ⋆ *Division de -12 par -5 :$-12 = (-5) \times 3 + 3$*

Exemple 1.1.20.

- *$a = 271$ et $b = 19$.*

$$\begin{array}{r|l} 2\,7\,1 & 1\,9 \\ \cline{2-2} 8\,1 & 1\,4 \\ 5 & \end{array}$$

  On a $271 = 19 \times 14 + 5$ et $0 \leq 5 < 19$ donc $q = 14$ et $r = 5$.

- *$a = -271$ et $b = 19$.*

  On a $-271 = 19(-14) + (-5)$ mais -5 est négatif

  $-271 = 19(-15) + 14$ avec $0 \leq 14 < 19$ donc $q = -15$ et $r = 14$.

1.1.4 Décomposition en base b

Théorème 1.1.2 (Décomposition en base b). *Soit $b \geq 2$ un entier. Tout entier $a > 0$ s'écrit de fa¸con unique sous la forme :*

$$a = a_0 + a_1 b + a_2 b^2 + \ldots + a_k b^k$$

où k est un entier, les a_i sont des entiers compris entre 0 et $b-1$ et où $a_k \neq 0$. On note parfois $a = \overline{a_k a_{k-1} \ldots a_0}^b$. Cette notation est l'écriture en base b de a.

Remarque 1.1.3. *Dans le cas où $b = 10$, les a_i correspondent exactement aux chiffres usuels de a. On s'aperçoit que 10 ne joue pas un role particulier vis-à-vis de la représentation des nombres : par exemple, on aurait pu noter 143 au lieu de 80 si on avait décidé de compter en base 7.*

Exemple 1.1.21.

1 *Ecrire 1248 en base 3.*

$$\begin{array}{r|l} 1\,2\,4\,8 & 3 \\ \cline{2-2} 0\,4 & 4\,1\,6 \\ 1\,8 & \\ 0 & \end{array} \quad \begin{array}{r|l} 4\,1\,6 & 3 \\ \cline{2-2} 1\,1 & 1\,3\,8 \\ 2\,6 & \\ 2 & \end{array} \quad \begin{array}{r|l} 1\,3\,8 & 3 \\ \cline{2-2} 1\,8 & 4\,6 \\ 0 & \end{array} \quad \begin{array}{r|l} 4\,6 & 3 \\ \cline{2-2} 1\,6 & 1\,5 \\ 1 & \end{array} \quad \begin{array}{r|l} 1\,5 & 3 \\ \cline{2-2} 0 & 5 \end{array} \quad \begin{array}{r|l} 5 & 3 \\ \cline{2-2} 2 & 1 \end{array}$$

Ce qui nous donne $1248 = \overline{1201020}^3$.

2 *Ecrire 1248 en base 5.*

$$\begin{array}{r|l} 1\,2\,4\,8 & 5 \\ \cline{2-2} 2\,4 & 2\,4\,9 \\ 4\,8 & \\ 3 & \end{array} \quad \begin{array}{r|l} 2\,4\,9 & 5 \\ \cline{2-2} 4\,9 & 4\,9 \\ 4 & \end{array} \quad \begin{array}{r|l} 4\,9 & 5 \\ \cline{2-2} 4 & 9 \end{array} \quad \begin{array}{r|l} 9 & 5 \\ \cline{2-2} 4 & 1 \end{array}$$

Ce qui nous donne $1248 = \overline{14443}^5$.

3 *Ecrire 1248 en base 2.*

$$\begin{array}{r|l} 1\,2\,4\,8 & \underline{\;2\;\;\;\;\;\;} \\ 0\,4 & 6\,2\,4 \\ 0\,8 & \\ 0 & \end{array} \quad \begin{array}{r|l} 6\,2\,4 & \underline{\;2\;\;\;\;\;\;} \\ 0\,2 & 3\,1\,2 \\ 0\,4 & \\ 0 & \end{array} \quad \begin{array}{r|l} 3\,1\,2 & \underline{\;2\;\;\;\;\;\;} \\ 1\,1 & 1\,5\,6 \\ 1\,2 & \\ 0 & \end{array} \quad \begin{array}{r|l} 1\,5\,6 & \underline{\;2\;\;\;\;} \\ 1\,6 & 7\,8 \\ 0 & \end{array} \quad \begin{array}{r|l} 7\,8 & \underline{\;2\;\;\;\;} \\ 1\,8 & 3\,9 \\ 0 & \end{array} \quad \begin{array}{r|l} 3\,9 & \underline{\;2\;\;\;\;} \\ 1\,9 & 1\,9 \\ 1 & \end{array}$$

$$\begin{array}{r|l} 1\,9 & \underline{\;2\;} \\ 1 & 9 \end{array} \quad \begin{array}{r|l} 9 & \underline{\;2\;} \\ 1 & 4 \end{array} \quad \begin{array}{r|l} 4 & \underline{\;2\;} \\ 0 & 2 \end{array} \quad \begin{array}{r|l} 2 & \underline{\;2\;} \\ 0 & 1 \end{array}$$

Ce qui nous donne $1248 = \overline{10011100000}^2$.

Exemple 1.1.22.

1 *Ecrire en base 10,* $a = \overline{110100100}^2$.

$$a = 1\times 2^8 + 1\times 2^7 + 0\times 2^6 + 1\times 5^5 + 0\times 2^4 + 0\times 2^3 + 1\times 2^2 + 0\times 2^1 + 0\times 2^0 = 420$$

2 *Ecrire en base 10,* $b = \overline{1130506}^7$.

$$b = 1\times 7^6 + 1\times 7^5 + 3\times 7^4 + 0\times 7^3 + 5\times 7^2 + 0\times 7^1 + 6\times 7^0 = 141910$$

1.2 pgcd, ppmc, Théorèmes d'Euclide et de Bézout

Définition 1.2.1 (pgcd, ppcm).

1 *Le* pgcd *de a et b, noté* $a \wedge b$ *ou* $\mathrm{pgcd}(a, b)$ *ou* $\mathrm{PGCD}(a, b)$*, est :*

a *le plus grand des diviseurs communs à a et b lorsque* $(a, b) \neq (0, 0)$,

b *0 lorsque* $a = b = 0$.

2 *Le* ppcm *de a et b, noté* $a \vee b$ *ou* $\mathrm{ppcm}(a, b)$ *ou* $\mathrm{PPCM}(a, b)$*, est :*

a *le plus petit des multiples strictement positifs communs à a et b lorsque* $ab \neq 0$,

b *0 lorsque* $a = 0$ *ou* $b = 0$.

Remarque 1.2.1.

— *Étant donnés deux entiers relatifs a et b, on a :*

$$a \wedge b = |a| \wedge |b|.$$

C'est pourquoi l'on supposera souvent par la suite que a et b sont des entiers naturels.

— *Par définition, on a, pour tout* $a \in \mathbb{Z}$ *:* $a \wedge 0 = |a|$.

— *Si* $a = b = 0$*, les diviseurs communs à* a *et* b *sont tous les entiers, et il n'en existe donc pas de plus grand pour la relation d'ordre* $\leq$.
— *Si* $ab = 0$*, seul 0 est un multiple commun à* a *et* b *et il n'existe donc pas de multiple strictement positif commun à* a *et* b.

Exemple 1.2.1. *Déterminons* pgcd*(32, 12).*
Les ensembles des diviseurs positifs des entiers 12 et 32 sont $\mathcal{D}^+(12) = \{1, 2, 3, 4, 6, 12\}$ *et* $\mathcal{D}^+(32) = \{1, 2, 4, 8, 16, 32\}$. *On a*

$$\mathcal{D}^+(12) \cap \mathcal{D}^+(32) = \{1, 2, 4\}.$$

Donc, pgcd*(32, 12) = 4.*

Théorème 1.2.1 (Théorème d'Euclide). *Soient deux entiers* $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$. *Effectuons la division euclidienne de l'entier a par l'entier b :*

$$\exists (q, r) \in \mathbb{N}^2 : \quad a = bq + r \quad \text{et} \quad 0 \leq r < b$$

Alors :

$$a \wedge b = b \wedge r.$$

Remarque 1.2.2. *Le théorème précédent justifie l'algorithme d'Euclide pour trouver le* pgcd *de deux entiers non nuls* $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$. *On pose* $r_0 = a$, $r_1 = b$ *et on définit ensuite* $\forall k \geq 1$, *les couples* (q_k, r_k) *en utilisant une division euclidienne :*

$$\text{si } r_k \neq 0, \quad \exists! (q_k, r_{k+1}) \in \mathbb{Z}^2 \text{ tel que } r_{k-1} = q_k r_k + r_{k+1} \quad \text{et} \quad 0 \leq r_{k+1} < r_k.$$

Comme la suite d'entiers (r_k) *est strictement décroissante, il existe un rang* $n \geq 1$ *tel que* $r_n \neq 0$ *et* $r_{n+1} = 0$. *D'après le théorème d'Euclide, on a* $\forall k \in [0, n-1]$, $a \wedge b = rk \wedge r_{k+1}$. *Comme* r_n *divise* r_{n-1}, *on a* $r_n \wedge r_{n-1} = r_n$. *Par conséquent, le dernier reste non-nul* r_n *est le* pgcd *des entiers* (a, b).

Exemple 1.2.2. *Calculons par l'algorithme d'*EUCLIDE *le PGCD des nombres* 125 *et* 55.

$$\begin{aligned} 125 &= 55 \times 2 + 15 \\ 55 &= 15 \times 3 + 10 \\ 15 &= 10 \times 1 + 5 \\ 10 &= 5 \times 2 + 0 \end{aligned}$$

Le PGCD des nombres 125 *et* 55 *est le dernier reste non nul du procédé, c'est-à-dire* 5.

Exemple 1.2.3. *Calcul de* pgcd*(931,513) en utilisant l'algorithme d'Euclide :*

$$\begin{aligned} 931 &= 513 \times 1 + 418 \\ 513 &= 418 \times 1 + 95 \\ 418 &= 95 \times 4 + 38 \\ 95 &= 38 \times 2 + 19 \\ 38 &= 19 \times 2 + 0 \end{aligned}$$

Donc $\mathrm{pgcd}(931, 513) = 19$.

Définition 1.2.2 (Nombres premiers entre eux). *On dit que deux nombres a et b sont premiers entre eux si et seulement si leur plus grand diviseur commun est 1, autrement dit si et seulement si*

$$a \wedge b = 1.$$

Exemple 1.2.4. *Déterminons le* pgcd *des entiers 366 et 43 en utilisant l'algorithme d'Euclide :*

$$\begin{aligned} 366 &= 43 \times 8 + 22 \\ 43 &= 22 \times 1 + 21 \\ 22 &= 21 \times 1 + 1 \\ 21 &= 2 \times 1 + 0. \end{aligned}$$

On a $366 \wedge 43 = 1$. *Donc 366 et 43 sont premiers entre eux.*

Théorème 1.2.2 (Coefficients de Bézout). *Soient deux entiers non nuls $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Il existe $(u, v) \in \mathbb{Z}^2$ tels que*

$$au + bv = a \wedge b.$$

Un tel couple (u, v) est appelé couple de coefficients de Bézout de a et b.

Remarque 1.2.3.

1) *Il n'y a pas unicité du couple de coefficients de Bézout de deux entiers.*
2) *Les coefficients de Bézout peuvent s'obtenir en " remontant " l'algorithme d'Euclide.*

Exemple 1.2.5. *Calculons les coefficients de Bézout pour $a = 600$ et $b = 124$. On a*

$$\begin{aligned} 600 &= 4 \times 124 + 104 \\ 124 &= 1 \times 104 + 20 \\ 104 &= 5 \times 20 + 4 \\ 20 &= 5 \times 4 + 0 \end{aligned}$$

Méthode 1 : " remontée " de l'algorithme d'Euclide.

$$\begin{aligned}
4 &= 104 - 5 \times 20 \\
4 &= 104 - 5 \times (124 - 1 \times 104) \qquad car \qquad 20 = 124 - 1 \times 104 \\
4 &= 6 \times 104 - 5 \times 124 \\
4 &= 6 \times (600 - 4 \times 124) - 5 \times 124 \qquad car \qquad 104 = 600 - 4 \times 124 \\
4 &= 6 \times 600 - 29 \times 124 \\
4 &= 6 \times 600 + (-29) \times 124
\end{aligned}$$

Ainsi pour $u = 6$ *et* $v = -29$, *on a* $600u + 124v = 4 = 600 \wedge 124$.

Méthode 2 : On peut obtenir les coefficients de Bézout en utilisant le calcul matriciel.
On utilise

$$\begin{aligned}
a = bq + r \quad &\Leftrightarrow \quad \begin{pmatrix} b \\ r \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \\
600 = 4 \times 124 + 104 \quad &\Leftrightarrow \quad \begin{pmatrix} 124 \\ 104 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 600 \\ 124 \end{pmatrix} \\
124 = 1 \times 104 + 20 \quad &\Leftrightarrow \quad \begin{pmatrix} 104 \\ 20 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 124 \\ 104 \end{pmatrix} \\
104 = 5 \times 20 + 4 \quad &\Leftrightarrow \quad \begin{pmatrix} 20 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} 104 \\ 20 \end{pmatrix} \\
20 = 5 \times 4 + 0 \quad &\Leftrightarrow \quad \begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} 20 \\ 4 \end{pmatrix}
\end{aligned}$$

$$\begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 600 \\ 124 \end{pmatrix}$$

$$\begin{pmatrix} 4 \\ 0 \end{pmatrix} \begin{pmatrix} 6 & -29 \\ -31 & 150 \end{pmatrix} \begin{pmatrix} 600 \\ 124 \end{pmatrix}$$

Par suite, $4 = 6 \times 600 - 29 \times 124$

Théorème 1.2.3 (Théorème de Bézout). *Soient deux entiers non nuls* $(a, b) \in (Z^*)^2$. *On a*

$$a \wedge b = 1 \Leftrightarrow [\exists (u, v) \in \mathbb{Z}^2 : \quad 1 = au + bv].$$

Théorème 1.2.4 (Théorème de Gauss). *Soient trois entiers non nuls* $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}^*$.

$$\Big[a | bc \qquad et \qquad a \wedge b = 1 \Big] \Rightarrow a \mid c.$$

Proposition 1.2.1 (Caractérisation des diviseurs et des multiples). *Soient deux entiers* $(a, b) \in \mathbb{Z}^2$.

1 *Soit un entier* $d \in \mathbb{Z}$. $\begin{cases} d|a \\ d|b \end{cases} \Leftrightarrow d \mid (a \wedge b)$.

2 *soit un entier* $m \in \mathbb{Z}$. $\begin{cases} a|m \\ b|m \end{cases} \Leftrightarrow (a \vee b) \mid m$.

Proposition 1.2.2. *Soient deux entiers non nuls* $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$. *Pour un entier* $k \in \mathbb{N}^*$,

$$(ka) \wedge (kb) = k(a \wedge b) \qquad \text{et} \qquad (ka) \vee (kb) = k(a \vee b).$$

Proposition 1.2.3 (Autres propriétés du pgcd). *Soient trois entiers relatifs non nuls* a, b *et* c.

1 *Soient trois entiers* $(d, a', b') \in \mathbb{N}^* \times \mathbb{Z}^2$ *tels que* $a = da'$, $b = db'$, *alors*

$$d = a \wedge b \Leftrightarrow a' \wedge b' = 1.$$

2 $\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Leftrightarrow a \wedge (bc) = 1.$

3 $\begin{cases} a|c \\ b|c \\ a \wedge b = 1 \end{cases} \Rightarrow ab|c.$

4 *pour tout couple* $(p, q) \in \mathbb{N}^* \times \mathbb{N}^*$, *si* $a \wedge b = 1$, *alors* $a^p \wedge b^q = 1$;

5 *pour tout entier* $k \in \mathbb{N}^*$, $a^k \wedge b^k = (a \wedge b)^k$.

Théorème 1.2.5 (Relation entre pgcd et ppcm). *Soient deux entiers non nuls* $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$.

1 *Si* $a \wedge b = 1$ *alors* $a \vee b = |ab|$;

2 $(a \wedge b)(a \vee b) = |ab|$.

Proposition 1.2.4. *Soient* $m, n \in \mathbb{Z}$ *et* $p \in \mathbb{Z}$.

$$p = \text{ppcm}(m, n) \Leftrightarrow m\mathbb{Z} \cap n\mathbb{Z} = p\mathbb{Z}.$$

Proposition 1.2.5. $m, n \in \mathbb{Z}$ *et* $d \in \mathbb{Z}$.

$$d = \text{pgcd}(m, n) \Leftrightarrow m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}.$$

1.3 Nombres premiers

1.3.1 Nombres premiers

Définition 1.3.1 (Nombre premier, nombre composé). *Un entier* $n \in \mathbb{N}$ *est dit premier si* $n \geq 2$ *et si ses seuls diviseurs dans* $\mathbb{N}$, *sont 1 ou lui-même :*

$$\forall k \in \mathbb{N}^*, \quad k|n \Rightarrow k \in \{1, n\}.$$

On note $\mathbb{P}$ l'ensemble des nombres premiers.
Si un entier $n \in \mathbb{N}$ n'est pas premier, on dit qu'il est composé.

Proposition 1.3.1. *Soit $n > 1$ un entier. Son plus petit diviseur $d > 1$ est un nombre premier. Si de plus n est composé, alors $d \leq \sqrt{n}$.*

Remarque 1.3.1. *On déduit de la propriété précédente que pour tester si un entier $n > 1$ est premier, il suffit de regarder s'il est divisible ou non par un des entiers compris entre 2 et $\sqrt{n}$. Par exemple, pour vérifier que 37 est premier, il suffit de voir qu'il n'est divisible ni par 2, ni par 3, ni par 4, ni par 5, ni par 6. On aurait également pu éviter les divisions par 4 et 6 si on savait par avance que ces nombres étaient composés.*

La remarque précédente nous amène à la méthode suivante, appelée crible d'Ératosthène pour lister tous les nombres premiers entre 1 et n :

- *On écrit à la suite les uns des autres tous les entiers compris entre 2 et n.*
- *On entoure le premier 2 et on barre tous ses multiples (i.e. tous les nombres pairs).*
- *On entoure ensuite le prochain nombre non barré (en l'occurrence 3) et on barre tous ses multiples. Ainsi de suite jusqu'à $\sqrt{n}$.*
- *On entoure finalement les nombres non barrés.*
- *Les nombres entourés sont alors exactement les nombres premiers compris entre 1 et n.*

Exemples 1.3.1.

1) *Les nombres premiers inférieurs à 100 classés dans l'ordre croissant sont, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 et 97.*
2) *Le entiers : 9, 12, 25, 123, 405, 2001 sont composés.*
3) *Le nombre 103 est-il premier ?*
   Comme $\sqrt{103} \approx 10,149$, il nous suffit de vérifier que 103 n'est divisible par aucun des nombres 2, 3, 5 et 7 . Les caractères de divisibilité montrent que 103 n'est pas divisible par 2 ou par 3 ou par 5. Pour 7 on effectue les divisions euclidiennes :
   $103 = 14 \times 7 + 5$, *le reste de la division de 103 par 7 est 5. 103 n'est donc pas divisible par 7.*
   On en conclut que 103 est un nombre premier.
4) *101 est premier.*
5) *91 n'est pas premier*

Remarque 1.3.2.

— *1 n'est pas premier et 2 est le seul nombre premier pair.*
— *Un entier positif est premier si et seulement si le cardinal de l'ensemble de ses diviseurs positifs est égal à 2.*

Proposition 1.3.2 (Propriétés des nombres premiers).

1 *Soit un entier $p \in \mathbb{N}$ premier, et $a \in \mathbb{Z}$ un entier. Alors, $p|a$ ou bien $p \wedge a = 1$.*

2 *Si n et m sont deux nombres premiers distincts, ils sont premiers entre eux : $n \neq m \Rightarrow n \wedge m = 1$.*

3 *Si n est un nombre premier et si $(a_1, . . ., a_k) \in \mathbb{Z}^k$,*

$$n|a_1...a_k \Rightarrow [\ \exists i \in [[1, n]] : \quad n|a_i\ \ ]$$

Proposition 1.3.3. *Tout entier supérieur à 2 admet un diviseur premier.*

Proposition 1.3.4. *L'ensemble $\mathbb{P}$ des nombres premiers est infini.*

1.3.2 Décomposition en facteurs premiers

Théorème 1.3.1. *Soit $n \geq 2$ un entier. Il existe des nombres premiers $p_1 < p_2 < \cdots < p_r$ et des exposants entiers $\alpha_1, \alpha_2, \ldots, \alpha_r \geq 1$ tels que :*

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}.$$

De plus les p_i et les α_i ($i = 1, \ldots, r$) sont uniques.

Pour obtenir la décomposition d'un entier naturel en produit de facteurs premiers on pourra utiliser l'une des deux méthodes suivantes appliquées à 300.

Méthode 1.3.1. *On écrit 300 sous la forme d'un produit, puis on recommence avec chacun des facteurs obtenus tant que c'est possible.*

$$300 = 30 \times 10 = 5 \times 6 \times 2 \times 5 = 2 \times 5 \times 5 \times 3 \times 2 = 2^2 \times 3 \times 5^2.$$

Méthode 1.3.2. *On effectue des divisions successives par les nombres premiers (2, 3, 5, 7, 11,...) tant que c'est possible. Les résultats sont placés dans un tableau.*

300	2
150	2
75	3
25	5
5	5
1	

300 est divisible par 2, le quotient est 150. 150 est divisible par 2, le quotient est 75. 75 n'est pas divisible par 2, mais 75 est divisible par 3, le quotient est 25. 25 est divisible par 5, le quotient est 5. 5 est divisible par 5, le quotient est 17 est n'est pas divisible par 5, mais 7 est divisible par 7, le quotient est 1, ce qui termine le tableau.
Le résultat dans la 2^{me} colonne du tableau donne : $300 = 2 \times 2 \times 3 \times 5 \times 5 = 2^2 \times 3 \times 5^2$.

Exemple 1.3.1. $504 = 2^3 \times 3^2 \times 7$

1.3.3 Expression du pgcd et du ppcm à l'aide des facteurs premiers

On obtient une expression du pgcd et du ppcm de deux entiers lorsqu'on connait leur décomposition en facteurs premiers. Précisément, si :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad et \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

où les p_i sont deux à deux distincts, mais les α_i et β_i sont éventuellement nuls, on a :

$$\operatorname{pgcd}(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}}.$$

$$\operatorname{ppcm}(a, b) = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \cdots p_k^{\max\{\alpha_k,\beta_k\}}.$$

Exemple 1.3.2. *Soit* $a = 60$ *et* $b = 16$. *On a :*

$$\begin{array}{r|l} 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \qquad et \qquad \begin{array}{r|l} 16 & 2 \\ 8 & 2 \\ 4 & 2 \\ 2 & 2 \\ 1 & \end{array}$$

Par suite, $a = 2^2 \times 3^1 \times 5^1$ *et* $b = 2^4 \times 3^0 \times 5^0$ *donc* $a \wedge b = 2^2 \times 3^0 \times 5^0 = 4$ *et* $a \vee b = 2^4 \times 3^1 \times 5^1 = 240$.

Exemple 1.3.3.

$$504 = 2^3 \times 3^2 \times 7, \quad 300 = 2^2 \times 3 \times 5^2.$$

Pour calculer le pgcd *on réécrit ces décompositions :*

$$504 = 2^3 \times 3^2 \times 5^0 \times 7^1, \quad 300 = 2^2 \times 3^1 \times 5^2 \times 7^0.$$

Le pgcd est le nombre obtenu en prenant le plus petit exposant de chaque facteur premier :

$$\operatorname{pgcd}(504, 300) = 2^2 \times 3^1 \times 5^0 \times 7^0 = 12.$$

Pour le ppcm *on prend le plus grand exposant de chaque facteur premier :*

$$\operatorname{ppcm}(504, 300) = 2^3 \times 3^2 \times 5^2 \times 7^1 = 12\,600$$

Chapitre 2

ARITHMÉTIQUE DANS $\mathbb{Z}/n\mathbb{Z}$

2.1 Congruences

2.1.1 Définition - propriétés

Définition 2.1.1. *Soit n un entier naturel non nul, a et b deux entiers relatifs . On dit que a est* ***congru à*** *b* ***modulo*** *n si $a-b$ est un multiple de n ; et on écrit*

$$a \equiv b[n] \qquad ou \qquad a \equiv b \ (mod\ n).$$

Remarque 2.1.1. *Si r désigne le reste de la division euclidienne de a par n alors $a \equiv r[n]$.*

Exemples 2.1.1.

$$15 \equiv 1[7], \quad 142 \equiv 2[7], \quad 3 \equiv -11[7], \quad 3 \equiv -4[7], \quad 2013 \equiv 3[10], \quad -13 \equiv 5[6]$$

Proposition 2.1.1. *Soient a et b deux entiers, et n et m des entiers naturels non nuls.*

1. *$a \equiv a\ [n]$ (réflexivité).*
2. *$a \equiv b\ [n] \Leftrightarrow b \equiv a\ ; [n]$ (symétrie).*
3. *Si $a \equiv b\ [n]$ et $b \equiv c[n]$, alors $a \equiv c\ [n]$ (transitivité).*
4. *Si $a \equiv b\ [n]$ et si $m|n$, alors $a \equiv b\ [m]$.*

Proposition 2.1.2. *Soit n un entier naturel non nul et a, a', b, b' quatre entiers relatifs.*

1. *Si $a \equiv a'[n]$ et $b \equiv b'[n]$ alors $a+b \equiv a'+b'[n]$.*
2. *Si $a \equiv a'[n]$ et $b \equiv b'[n]$ alors $a \times b \equiv a' \times b'[n]$.*
3. *si $a \equiv b[n]$ alors $a^k \equiv b^k[n] \qquad k \in \mathbb{N}$.*

Exemple 2.1.1. *Montrons que $\forall x \in \mathbb{Z}$, $(5x+8)^2 \equiv 4[5]$.*
On a $8 \equiv 3[5]$ et $3^2 \equiv 4[5]$. On a aussi $5 \equiv 0[5]$ donc $5x \equiv 0x[5]$. Par suite $5x+8 \equiv 3[5]$ et $(5x+8)^2 \equiv 3^2[5]$, ce qui donne $(5x+8)^2 \equiv 4[5]$.

Théorème 2.1.1. *Soit n un entier naturel non nul, a et a' deux entiers relatifs, r et r' les restes respectifs des divisions euclidiennes de a et a' par n.*

$$a \equiv a'[n] \Leftrightarrow r = r'$$

Théorème 2.1.2. *Soit $N > 1$ un entier et c un entier premier avec N. Alors il existe un entier c' tel que $cc' \equiv 1[n]$. Un tel entier c' est appelé un **inverse de c modulo** N.*

2.1.2 Équations diophantiennes

a) Définition - exemples

Définition 2.1.2. *On appelle **équation diophantienne** toute équation dont on cherche les solutions en nombres entiers.*

Exemples 2.1.2.

1) *Résoudre dans $\mathbb{Z}^2$, $ax + by = d$ avec $(a, b, c) \in \mathbb{R}^3$.*
2) *Résoudre dans $\mathbb{Z}^3$, $x^2 + y^2 = z^2$ avec $(a, b, c) \in \mathbb{R}^3$.*
3) *Résoudre dans $\mathbb{Z}$, $x^2 = 4k + 3$.*

b) L'équation $ax + by = c$

Proposition 2.1.3. *Considérons l'équation*

$$ax + by = c \tag{2.1}$$

où $a, b, c \in \mathbb{Z}$. Soit $d = \text{pgcd}(a, b)$

1 *L'équation (2.1) possède des solutions $(x, y) \in \mathbb{Z}^2$ si et seulement si $d|c$.*

2 *Si $d|c$ alors il existe même une infinité de solutions entières et elles sont exactement les*

$$(x, y) = (x_0 + ak, y_0 + bk)$$

avec $x_0, y_0, a, b \in \mathbb{Z}$ fixés et k parcourant $\mathbb{Z}$.

Exemple 2.1.2. *Trouver les solutions entières de*

$$161x + 368y = 115 \tag{2.2}$$

• ***Première étape.*** Y a-t-il des solutions ? *L'algorithme d'Euclide. On effectue l'algorithme d'Euclide pour calculer le* pgcd *de $a = 161$ et $b = 368$.*

$$\begin{aligned} 368 &= 161 \times 2 + 46 \\ 161 &= 46 \times 3 + 23 \\ 46 &= 23 \times 2 + 0 \end{aligned}$$

Donc $368 \wedge 161 = 23$. *Comme* $115 = 5 \times 23$ *alors* $(368 \wedge 161)|115$. *Par le Théorème de Bézout, l'équation (2.2) admet des solutions entières.*

• ***Deuxième étape.*** Trouver une solution particulière *: la remontée de l'algorithme d'Euclide. On effectue la remontée de l'algorithme d'Euclide pour calculer les coefficients de Bézout.*

$$\begin{aligned} 23 &= 161 - 3 \times 46 \\ 23 &= 161 - 3 \times (368 - 161 \times 2) \qquad car \qquad 46 = 368 - 161 \times 2 \\ 23 &= 161 \times 7 - 368 \times 3 \end{aligned}$$

On trouve donc $161 \times 7 + 368 \times (-3) = 23$. *Comme* $115 = 5 \times 23$ *en multipliant par* 5 *on obtient :* $161 \times 35 + 368 \times (-15) = 115$.
Ainsi $(x_0, y_0) = (35, -15)$ *est une solution particulière de (2.2).*

• ***Troisième étape.*** Recherche de toutes les solutions. *Soit* $(x, y) \in \mathbb{Z}^2$ *une solution de (2.2). Nous savons que* (x_0, y_0) *est aussi solution. Ainsi :*

$$161x + 368y = 115 \qquad et \qquad 161x_0 + 368y_0 = 115.$$

La différence de ces deux égalités conduit à

$$\begin{aligned} 161 \times (x - x_0) + 368 \times (y - y_0) = 0 &\Rightarrow 23 \times 7 \times (x - x_0) + 23 \times 16 \times (y - y_0) = 0 \\ &\Rightarrow 7(x - x_0) = -16(y - y_0). \end{aligned} \tag{2.3}$$

Nous avons simplifié par 23 qui est le pgcd *de 161 et 368. (Attention, n'oubliez surtout pas cette simplification, sinon la suite du raisonnement serait fausse.) Ainsi* $7|16(y - y_0)$, *or* $\text{pgcd}(7, 16) = 1$ *donc par le Théorème de Gauss 1.2.4* $7|y - y_0$. *Il existe donc* $k \in \mathbb{Z}$ *tel que* $y - y_0 = 7 \times k$. *Repartant de l'équation (2.3) :* $7(x - x_0) = -16(y - y_0)$. *On obtient maintenant* $7(x - x_0) = -16 \times 7 \times k$. *D'où* $x - x_0 = -16k$. *(C'est le même* k *pour* x *et pour* y.*) Nous avons donc* $(x, y) = (x_0 - 16k, y_0 + 7k)$. *Il n'est pas dur de voir que tout couple de cette forme est solution de l'équation (2.2). Il reste donc juste à substituer* (x_0, y_0) *par sa valeur et nous obtenons : Les solutions entières de* $161x + 368y = 115$ *sont les* $(x, y) = (35 - 16k, -15 + 7k)$, k *parcourant* $\mathbb{Z}$.

Exercice 1. *Soit* (E) *l'équation* $6x + 7y = 57$.

1) *Déterminer un couple d'entiers relatifs* $(u\,; v)$ *tel que* $6u + 7v = 1$*puis en déduire une solution particulière de* (E).

2) *Résoudre* (E).

2.1.3 Équation de congruence $ax \equiv b \pmod n$

Proposition 2.1.4. *Soit $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$ fixés et $n \geq 2$. Considérons l'équation $ax \equiv b \pmod n$ d'inconnue $x \in \mathbb{Z}$:*

1. *Il existe des solutions si et seulement si $\operatorname{pgcd}(a,n)|b$.*
2. *Les solutions sont de la forme $x = x_0 + \ell \dfrac{n}{\operatorname{pgcd}(a,n)}$, $\ell \in \mathbb{Z}$ où x_0 est une solution particulière. Il existe donc $\operatorname{pgcd}(a,n)$ classes de solutions.*

Exemple 2.1.3. *Résolvons l'équation $9x \equiv 6 \pmod{24}$. Comme $\operatorname{pgcd}(9,24) = 3$ divise 6 la proposition ci-dessus nous affirme qu'il existe des solutions. Nous allons les calculer. (Il est toujours préférable de refaire rapidement les calculs que d'apprendre la formule). Trouver x tel que $9x \equiv 6 \pmod{24}$ est équivalent à trouver x et k tels que $9x = 6 + 24k$. Mis sous la forme $9x - 24k = 6$ il s'agit alors d'une équation que nous avons étudiée en détails. Il y a bien des solutions car $\operatorname{pgcd}(9,24) = 3$ divise 6. En divisant par le pgcd on obtient l'équation équivalente :*

$$3x - 8k = 2.$$

Pour le calcul du pgcd et d'une solution particulière nous utilisons normalement l'algorithme d'Euclide et sa remontée. Ici il est facile de trouver une solution particulière $(x_0 = 6, k_0 = 2)$ à la main.

Si (x,k) est une solution de $3x - 8k = 2$ alors par soustraction on obtient $3(x - x_0) - 8(k - k_0) = 0$ et on trouve $x = x_0 + 8\ell$, avec $\ell \in \mathbb{Z}$ (le terme k ne nous intéresse pas). Nous avons donc trouvé les x qui sont solutions de $3x - 8k = 2$, ce qui équivaut à $9x - 24k = 6$, ce qui équivaut encore à $9x \equiv 6 \pmod{24}$. Les solutions sont de la forme $x = 6 + 8\ell$. On préfère les regrouper en 3 classes modulo 24 :

$$x_1 = 6 + 24m, \quad x_2 = 14 + 24m, \quad x_3 = 22 + 24m \quad \text{avec } m \in \mathbb{Z}.$$

2.1.4 Théorème chinois

Le théorème chinois s'énonce comme suit :

Théorème 2.1.3 (Théorème chinois). *Soient $N_1,\ N_2,\ \dots,\ N_k$ des entiers strictement positifs deux à deux premiers entre eux, et $a_1,\ a_2,\ \dots,\ a_k$ des entiers quelconques. Alors il existe un entier a tel que le système de congruences :*

$$(S) \qquad \left\{ \begin{array}{lcl} z & \equiv & a_1[N_1] \\ z & \equiv & a_2[N_2] \\ . & & \\ . & & \\ . & & \\ z & \equiv & a_k[N_k] \end{array} \right.$$

soit équivalent à la simple congruence $z \equiv a[N_1N_2...N_k]$.
En particulier, le système précédent possède au moins une solution.

Corollaire 2.1.1. *Soient $N_1, \cdots, N_k$ des entiers, supérieurs ou égaux à deux, et deux à deux premiers entre eux. Soient $a_1, \cdots, a_k$ dans $\mathbb{Z}$. Alors le système*

$$(S) \qquad \begin{cases} z & \equiv & a_1[N_1] \\ z & \equiv & a_2[N_2] \\ . & & \\ . & & \\ . & & \\ z & \equiv & a_k[N_k] \end{cases}$$

admet au moins une solution z_0 et sa solution générale est $z_0 + N_1 \cdots N_k\mathbb{Z}$.

Méthode 2.1.1. *Voyons maintenant quelques méthodes pratiques pour déterminer z.*

1er cas *: $k = 2$. Soient k_1 et k_2 dans $\mathbb{Z}$ tels que $k_1N_1 + k_2N_2 = 1$.*

- *On peut bien entendu trouver z en écrivant qu'il existe u_1, u_2 dans $\mathbb{Z}$ tels que*

$$z = a_1 + u_1N_1 = (a_2 + u_2N_2).$$

On trouve u_1 et u_2 tels que $(a_2 - a_1) = u_1N_1 - u_2N_2$ puis on pose

$$z = a_1 + u_1N_1.$$

- *On peut procéder autrement. On cherche e_1 et e_2 tels que*

$$\begin{cases} e_1 & \equiv & 1 \ [N_1] \\ e_1 & \equiv & 0 \ [N_2] \end{cases} \qquad \begin{cases} e_2 & \equiv & 0 \ [N_1] \\ e_2 & \equiv & 1 \ [N_2] \end{cases}$$

On a donc $z_0 = a_1e_1 + a_2e_2$ est solution particulière de (S).

2ème cas *: $k \geq 3$. On utilise le même procédé. On sait calculer pour tout $i \in \{1, \cdots, k\}$ $e_i \in \mathbb{Z}$ vérifiant :*

$$\begin{cases} e_i & \equiv & 1 \ [N_i] \\ e_i & \equiv & 0 \ [\dfrac{N_1 \cdots N_k}{N_i}] \end{cases}$$

Alors $z_0 = \displaystyle\sum_{i=1}^{k} a_ie_i$ est solution particulière de (S).

Exemple 2.1.4. *Résolvons dans $\mathbb{Z}$ le système :*

$$\begin{cases} x & \equiv & 2[10] \\ x & \equiv & 5[13] \end{cases} . \tag{2.4}$$

1ere méthode :

Déterminons $10 \wedge 13$

$$\begin{aligned} 13 &= 1 \times 10 + 3 \\ 10 &= 3 \times 3 + 1 \\ 3 &= 3 \times 1 + 0 \end{aligned}$$

donc $10 \wedge 13 = 1$*. D'après le Théorème chinois 2.1.3,*

$$(2.4) \Leftrightarrow x \equiv a[130]$$

avec $a = 2+10(5-2)N_1'$ *et* $10N_1' \equiv 1[13]$*. On peut déterminer* N_1' *à partir des coefficients de Bézout de 10 et 13. On a*

$$\begin{aligned} 1 &= 10 - 3 \times 3 \\ 1 &= 10 - 3 \times (13 - 1 \times 10) \qquad car \qquad 3 = 13 - 1 \times 10 \\ 1 &= 4 \times 10 - 3 \times 13 \end{aligned}$$

On peut donc prendre $N_1' = 4$*, ce qui nous donne* $a = 122$*. Par suite,*

$$(2.4) \Leftrightarrow x = 122 + 130k \quad avec \quad k \in \mathbb{Z}.$$

2e méthode :

Déterminons une solution particulière : $x = 2 + 10k = 5 + 13k'$ *avec* $k, k' \in \mathbb{Z}$*.* $10k - 13k' = 3$*. Cherchons* $u, v \in \mathbb{Z}$ *tel que* $10u + 13v = 1$*.* $u = 4$ *et* $v = -3$ *conviennent. Prenons* $k = 12$*,* $k' = 9$ *ce qui donne* $x = 122$*.*

Soit x une autre solution. On a $\left\{ \begin{array}{lcl} x & \equiv & 122[10] \\ x & \equiv & 122[13] \end{array} \right.$ *donc* $10|x - 122$ *et* $13|x - 122$*, ce qui donne* $130|x - 122$ *et par suite* $x = 122 + 130k$ *avec* $k \in \mathbb{Z}$*.*

Inversement si $x = 122 + 130k$ *avec* $k \in \mathbb{Z}$*, on a*
$122 \equiv 2[10]$ *et* $130 \equiv 0[10]$ *donc* $x \equiv 2[10]$*.* $122 \equiv 5[13]$ *et* $130 \equiv 0[13]$ *donc* $x \equiv 2[13]$*.*
Par suite, $\left\{ \begin{array}{lcl} x & \equiv & 2[10] \\ x & \equiv & 5[13] \end{array} \right.$

3e méthode :

Cherchons e_1 *tel que* $\left\{ \begin{array}{lcl} e_1 & \equiv & 1 \ [10] \\ e_1 & \equiv & 0 \ [13] \end{array} \right.$
On peut choisir $e_1 = 91$

Cherchons e_2 *tel que* $\left\{ \begin{array}{lcl} e_2 & \equiv & 0 \ [10] \\ e_2 & \equiv & 1 \ [13] \end{array} \right.$
On peut choisir $e_2 = 40$*.*

Par suite, on a $x_0 = 2 \times 91 + 5 \times 40 = 182 + 200 = 382 = 122 + 260$.
$x = 382 + 130k' = 122 + 130k$ *avec* $k, k' \in \mathbb{Z}$

Exemple 2.1.5. *Résoudre dans* $\mathbb{Z}$ *:*

$$\begin{cases} z & \equiv & 1 \ [2] \\ z & \equiv & 2 \ [3] \\ z & \equiv & 3 \ [5] \end{cases}$$

Calcul de e_1. *On a* $\begin{cases} e_1 & \equiv & 1 \ [2] \\ e_1 & \equiv & 0 \ [15] \end{cases}$

$$\begin{array}{r|l} 15 & 2 \\ \hline 1 & 7 \end{array}$$

donc $1 = 15 - 2 \times 7$. *On peut choisir* $e_1 = 15$.

Calcul de e_2. *On a* $\begin{cases} e_2 & \equiv & 1 \ [3] \\ e_2 & \equiv & 0 \ [10] \end{cases}$

$$\begin{array}{r|l} 10 & 3 \\ \hline 1 & 3 \end{array}$$

donc $1 = 10 - 3 \times 3$. *On peut choisir* $e_2 = 10$.

Calcul de e_3. *On a* $\begin{cases} e_3 & \equiv & 1 \ [5] \\ e_3 & \equiv & 0 \ [6] \end{cases}$

$$\begin{array}{r|l} 15 & 2 \\ \hline 1 & 7 \end{array}$$

donc $1 = 6 - 5$. *On peut choisir* $e_3 = 6$.

Solution particulière : $15 + 2 \times 10 + 3 \times 6 = 53$.
Solution générale : $53 + 30\mathbb{Z}$.

2.2 Propriétés algébriques de $\mathbb{Z}/n\mathbb{Z}$

La relation $a \equiv b \ [n]$ est une relation d'équivalence sur $\mathbb{Z}$. On notera $\overline{a}$ le représentant de a.
L'ensemble de ces classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$, et s'appelle l'ensemble des entiers modulo n.

2.2.1 Structure

Proposition 2.2.1. *Pour* $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ *muni des deux lois :*

$$\overline{a+b} = \overline{a} + \overline{b} \qquad \overline{a \times b} = \overline{a} \times \overline{b}$$

est un anneau commutatif.

2.2.2 Éléments inversibles

Proposition 2.2.2. *Un élément $\overline{a}$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible si, et seulement si, a et n sont premiers entre eux.*

2.2.3 Cas particulier

Remarque 2.2.1. *$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.*

2.3 Indicatrice d'Euler

Définition 2.3.1. *la fonction d'Euler, encore appelée indicatrice d'Euler, est l'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ qui à chaque $n \in \mathbb{N}^*$ associe le nombre $\varphi(n)$ des entiers compris entre 1 et $n-1$ et premiers avec n.*

Lemme 2.3.1. *Si n est premier, alors $\varphi(n) = n - 1$.*

Lemme 2.3.2. *Pour tout nombre premier p et tout entier naturel $r \geq 1$, on a*

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1) = p^r(1 - \frac{1}{p}).$$

Lemme 2.3.3. *Si m et n sont premiers entre eux alors :*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Théorème 2.3.1. *Pour tout $n > 1$, on a :*

$$\varphi(n) = n \prod_i (1 - \frac{1}{p_i}),$$

où les p_i sont les facteurs premiers de n.

Exemple 2.3.1.

$$\varphi(1) = 1, \quad \varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2,$$

$$\varphi(5) = 4, \quad \varphi(6) = 2, \quad \varphi(15) = \varphi(3) \times \varphi(5) = 8.$$

Exemple 2.3.2. *On veut calculer $\varphi(300)$.*
On a $300 = 12 \times 25$ et $\operatorname{pgcd}(12, 25) = 1$.
$\varphi(12) = 12(1 - \frac{1}{3})(1 - \frac{1}{2}) = 12 \times \frac{2}{3} \times \frac{1}{2} = 4$ *liste : 1, 5, 7, 11*
$\varphi(25) = 25(1 - \frac{1}{5}) = 25 \times \frac{4}{5} = 20$
liste : 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24
$\varphi(300) = \varphi(12 \times 25) = \varphi(12) \times \varphi(25) = 4 \times 20 = 80.$

2.4 Théorèmes

2.4.1 Théorème d'Euler

Théorème 2.4.1. *Si a et n sont premiers entre eux avec $n \geq 2$, on a :*

$$a^{\varphi(n)} \equiv 1\ [n].$$

2.4.2 Petit théorème de Fermat

Théorème 2.4.2. *Si a n' est pas divisible par p (premier), alors $a^{P-1} \equiv 1 \ \ [p]$ (c'est-à-dire encore, $a^p \equiv a \ \ [p]$, ou encore, $a^P - a$ est toujours divisible par p).*

Exemple 2.4.1. *Calculons $14^{3141} \ (mod 17)$. Le nombre 17 étant premier on sait par petit théorème de Fermat que*

$$14^{16} \equiv 1 \ \ [17].$$

Écrivons la division euclidienne de 3141 par 16, on a $3141 = 16 \times 196 + 5$.
Alors

$$14^{3141} = 14^{(16\times196+5)} = 14^{(16\times196)} \times 14^5 = (14^{16})^{196} \times 14^5$$

On a $14^{16} \equiv 1 \ \ [17]$. Donc $(14^{16})^{196} \equiv 1^{196} \ \ [17]$. Par suite, $14^{(16\times196+5)} \equiv 14^5 \ \ [17]$.
Il ne reste plus qu'à calculer $14^5 \ \ [17]$. Cela peut se faire rapidement :
$14 \equiv -3 \ \ [17]$, donc $14^2 \equiv (-3)^2 \ \ [17] \equiv 9 \ \ [17]$, par suite
$14^3 \equiv 14^2 \times 14 \equiv 9 \times (-3) \equiv -27 \equiv 7 \ \ [17]$ d'où
$14^5 \equiv 14^3 \times 14^2 \equiv 9 \times 7 \equiv 63 \equiv 12 \ \ [17]$
Conclusion : $14^{3141} \equiv 14^5 \equiv 12 \ \ [17]$.

2.4.3 Théorème de Wilson

Théorème 2.4.3. *Pour que p divise $(p-1)! + 1$, il faut et il suffit que p soit premier.*

Exemple 2.4.2.

- *Si p est égal à 3, alors $(p-1)! + 1$ est égal à 3, un multiple de 3.*
- *Si p est égal à 4, alors $(p-1)! + 1$ est égal à 7 qui n'est pas multiple de 4.*
- *Si p est égal à 5, alors $(p-1)! + 1$ est égal à 25, un multiple de 5.*
- *Si p est égal à 6, alors $(p-1)! + 1$ est égal à 121 qui n'est pas multiple de 6.*
- *Si p est égal à 17, alors $(p-1)! + 1$ est égal à 20 922 789 888 001, un multiple de 17 car 17 × 1 230 752 346 353 = 20 922 789 888 001.*

Chapitre 3

EXERCICES

Exercice 2. *Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses :*

1 *60 a plus de diviseurs (positifs) que 100.*

2 *Étant donnés cinq nombres entiers consécutifs, on trouve toujours parmi eux au plus trois nombres pairs.*

3 *Si un nombre est divisible par 6 et par 8, alors il est divisible par 48.*

4 *Si un nombre premier divise le produit de deux entiers, alors il divise au moins un de ces deux entiers.*

5 *Si deux entiers sont premiers entre eux, alors chacun d'eux est premier avec leur somme.*

6 *Si* d *divise* a *et* b*, alors* d *divise leur* $PGCD$*.*

7 *S'il existe deux entiers* u *et* v *tels que* $au + bv = d$*, alors* $PGCD(a, b)$ *divise* d*.*

8 *Si le produit de deux entiers est congru à 0 modulo 6 alors l'un des deux est multiple de 6.*

9 *Aucun entier n'est tel que son carré soit congru à -1 modulo 5.*

10 *La puissance quatrième d'un entier quelconque est toujours congrue à 1 modulo 5.*

11 *Tous les nombres impairs sont premiers.*

12 *Aucun nombre pair n'est premier.*

13 *La différence entre deux nombres premiers est toujours deux.*

14 *Il y a une infinité de nombres premiers.*

Exercice 3. **1** *Compléter les phrases suivantes par les mots : divisible, multiple et diviseur.*

a *24 est* $\cdots\cdots\cdots$ *par 6.*

- **b** *45 est un ········· de 9.*
- **c** *2 est un ········· de 12.*
- **d** *12 est un········· de 36.*
- **e** *12 est ········· par 4.*
- **f** *25 a pour ········· 5.*
- **g** *7 a pour ········· 49.*

2 *On sait que 50 = 8 x 6 + 2. Compléter les phrases suivantes par les mots : quotient, reste, diviseur et dividende.*

- **a** *2 est le ········· de la division euclidienne de 50 par 8.*
- **b** *8 est le ········· de la division euclidienne de 50 par 8.*
- **c** *6 est le ········· de la division euclidienne de 50 par 8.*
- **d** *50 est le ········· de la division euclidienne de 50 par 8.*

Exercice 4. *Calculer* $\mathcal{D}(5)$, $\mathcal{D}(6)$ *et* $\mathcal{D}(8)$.

Exercice 5. *Mettez* $\times$ *dans la case qui convient :*

nombres \ divisible	par 2	par 3	par 4	par 5	par 6	par 7	par 8	par 9	par 10	par 11
7524										
5005005										
91328										
2805										

Exercice 6. **1** *Déterminer si les nombres suivants sont premiers : 319, 259.*

2 *Décomposer en produit de facteurs premiers 2520, 546 et 840.*

Exercice 7. **1** *Ecrire 13 en base 2, en base 3, puis en base 7*

2 *A est le nombre qui s'écrit 16524 dans le système à base 7. Ecrivez ce nombre en bases 10, puis 2 et enfin 16.*

Exercice 8.

1 *Démontrer que* $7^n + 1$ *est divisible par 8 si* n *est impair.*

2 *Dans le cas où n est pair, donner le reste de la division de* $7^n + 1$ *par 8.*

3 *Montrer que* $10^6 \equiv 1\ [7]$.

4 *Déterminer le chiffre des unités de* 3^{12}.

Exercice 9. *Déterminer, en utilisant la notion de congruence, le chiffre des unités de* 7^{7^7}

Exercice 10. *On considère les couples d'entiers (a, b) suivants.*

$$a)\ a = 60, \quad b = 84 \quad b)\ a = 360, \quad b = 240 \quad c)\ a = 160, \quad b = 171$$

Pour chacun de ces couples :

1. *Calculer $PGCD(a, b)$ par l'algorithme d'Euclide.*
2. *En déduire une identité de Bézout.*
3. *Calculer $PPMC(a, b)$.*
4. *Déterminer l'ensemble des couples (a, b) d'entiers relatifs tels que : $au + bv = PGCD(a, b)$*
5. *Donner la décomposition en facteurs premiers de a et b.*
6. *En déduire la décomposition en facteurs premiers de $PGCD(a, b)$ et $PPMC(a, b)$, et retrouver les résultats des questions 1 et 3.*

Exercice 11.

1. *Trouver une solution particulière de $13u + 5v = 3$*
2. *Déterminer tous les couples d'entiers $(u, v) \in \mathbb{Z}^2$ tels que $13u + 5v = 3$.*
3. *Déterminer les restes de la division euclidienne de 2^{2013} par 5 et par 13.*
4. *Déduire des deux questions qui précèdent le reste de la division euclidienne de 2^{2013} par 65.*

Exercice 12.

1. a. *Ecrire une identité de Bézout entre 99 et 56.*

   b. *Résoudre le système*

$$\begin{cases} x \equiv 2\ [56] \\ x \equiv 3\ [99]. \end{cases}$$

2. *Résoudre le système*

$$\begin{cases} x \equiv 3\ [17] \\ x \equiv 4\ [11] \\ x \equiv 5\ [6]. \end{cases}$$

Exercice 13.

1. *Montrer que $2^{1000} \equiv 2\ [7]$*
2. *Trouver le reste de la division de 100^{1000} par 13.*

Exercice 14. *Calculer $\varphi(105)$, $\varphi(120)$ et $\varphi(1000)$ où φ est la fonction indicatrice d'Euler*

Bibliographie

[1] **A. Bodin** : *Algèbre*. Exo 7 (2016).

[2] **A. Soyeur, F. Capaces, E. Vieillard-Baron** : *Cours de Mathématiques Sup MPSI PCSI PTSI TSI* . sesamath.net (2011).

[3] **C. Deschamps, A. Warusfel, F. Moulin, J. François Ruaud, A. AAiquel, J-C Sifre** : *Mathématiques TOUT-EN-UN • I^e année : cours exercices corrigés MPSI-PCSI*. Dunod, Paris, (2003).

[4] **D. Fredon** : *Mathématiques Résumé du cours en fiches MPSI - MP*. Dunod, Paris, (2010).

[5] **E. Ramis, C. Deschamps, J. Odoux** : *Cours de Mathématiques Spéciales Algèbre*. Masson (1993).

[6] **J. Dixmler** : *Cours de Mathématiques du premier cycle* 1^e *année*, Gauthier-villars, (1976).

[7] **M. Allano Chevalier, X. Oudot** : *Maths MPSI*. Hachette, (2008).

[8] **N. Bourbaki** : *Éléments de Mathématique : Algèbre*. Springer (1970).

[9] **P. Bornsztein, X. Caruso, P. Nolin, M. Tibouchi** : *Cours d'arithmétique*. (2004).