TD 6 - Arithmétique dans $\mathbb{Z}$

Prérequis

- ☐ Connaître les définitions de *divisibilité*, *pgcd*, *nombre premiers entre eux*.
- ☐ Connaître par coeur le théorème de la division euclidienne.
- ☐ Faire absolument la différence entre l'existence des identités de Bézout et le thèoréme de Bézout.
- ☐ Revoir les propriétés classiques de la divisibilité (quelles propriétés a la *relation* de divisibilité sur $\mathbb{Z}$? sur $\mathbb{N}$?)
- ☐ Revoir les propriétés standards du pgcd.
- ☐ Maîtriser l'algorithme de division euclidienne et l'algorithme d'Euclide.

Objectifs

- ☐ Savoir manipuler les définitions de divisibilité et de division euclidienne.
- ☐ Savoir calculer l'écriture en base b d'un nombre donné dans une base b'.
- ☐ Savoir calculer une identité de Bézout et les manipuler dans des énoncés plus abstraits.
- ☐ Savoir justifier qu'une équation $ax + by = c$ admet ou non des solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.
- ☐ Savoir déterminer l'ensemble des solutions dans $\mathbb{Z} \times \mathbb{Z}$ d'une équation $ax + by = c$.

1 Avant le TD

Échauffement 1. Soit $a, b \in \mathbb{Z}$. À partir des définitions de divisibilité et de division euclidienne vues en cours, montrer les propositions suivantes.

1. b divise a si et seulement si le reste de la division euclidienne de a par b est nul.
2. $a \mid b$ et $b \mid a \quad \iff \quad a = \pm b$.

2 Divisibilité et division euclidienne

Exercice 1 (Relation de divisibilité et théorie des ensembles)**.** Pour tout entier relatif k, on note D_k l'ensemble des diviseurs de k et $k\mathbb{Z}$ l'ensemble défini par $k\mathbb{Z} = \{kq, q \in \mathbb{Z}\}$. Montrer les propositions suivantes :

1. $\forall a, b \in \mathbb{Z}, \quad D_a = D_b \iff a = \pm b$.
2. $\forall a, b \in \mathbb{Z}, \quad a \mid b \iff b\mathbb{Z} \subset a\mathbb{Z}$.

Exercice 2 (Division par soustractions)**.** On considère l'algorithme suivant.

Algorithme 1 Algorithme de division par soustraction

Entrée : Deux entiers positifs a, b.
Sortie : q, r le quotient et reste de la division euclidienne de a par b

1: $r \leftarrow a$
2: $q \leftarrow 0$
3: **Tant que** $r \geq b$ **faire**
4: $\quad r \leftarrow r - b$
5: $\quad q = q + 1$
6: **fin Tant que**
7: **Retourner** q, r

1. Prouver que $a = bq + r$ est un invariant de boucle.
2. Prouver la terminaison et la correction de cet algorithme.

Exercice 3 (Écriture en base b)**.**

1. Écrire $n = 10011_{10}$ en base 3.
2. Écrire $n = 110011_2$ en base 6.
3. Écrire $3n$ en base 3 où $n = 21001_3$ sans aucun calcul.

Exercice 4 (Propriétés du PGCD et algorithme d'Euclide)**.**

1. Soit $a, b \in \mathbb{Z}$. En reprenant les notations de l'Exercice 1, montrer que pour tout entier $k \in \mathbb{Z}$:
   a. $D_a \cap D_b = D_{a+bk} \cap D_b$. Que signifie en français cette égalité ?
   b. $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a + bk, b)$.
2. En déduire les propositions suivantes :
   a. Si q et r sont le quotient et le reste de la division euclidienne de a par b alors, $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r)$.
   b. L'algorithme d'Euclide est correct et termine.
   c. Les diviseurs communs à a et b sont exactement les diviseurs de $\mathrm{PGCD}(a, b)$.

3 PGCD, nombre premiers entre eux et nombre premiers

Exercice 5. Un entier $p > 1$ est dit premier si ses seuls diviseurs positifs sont 1 et p. Soit p un nombre premier et $a, b \in \mathbb{Z}$. On suppose que $p \mid ab$.

1. Supposons de plus que $p \nmid a$. Montrer que $\mathrm{PGCD}(p, a) = 1$.
2. Montrer alors que $p \mid b$.
3. En déduire le lemme d'Euclide : si p est un nombre premier alors $p \mid ab \implies p \mid a$ ou $p \mid b$.

Exercice 6. Soit $a, b, c \in \mathbb{Z}$ avec a et b premiers entre eux. Montrer les propositions suivantes :

1. $a \mid c$ et $b \mid c \implies ab \mid c$.
2. (Lemme de Gauss) $a \mid bc \implies a \mid c$.

4 Euclide étendu et équations diophantiennes

Exercice 7 (Algorithme d'Euclide (étendu))**.**

1. Sans utiliser l'algorithme d'Euclide, calculer $\mathrm{PGCD}(105, 12)$.
2. Retrouver le même résultat avec l'algorithme d'Euclide.
3. Trouver $u, v \in \mathbb{Z}$ tels que $au + bv = \mathrm{PGCD}(a, b)$.

Exercice 8 (Quelques équations diophantiennes)**.**

1. Trouver une solution particulière, $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$, de l'équation $1075x + 63y = 1$.
2. Montrer que l'équation $1075x+63y = 1$ admet une infinité de solutions entières et déterminer l'ensemble de solutions.
3. Montrer que l'équation $1075x + 63y = 15$ admet une infinité de solutions entières et déterminer l'ensemble de solutions.
4. Prouver que l'équation $756x + 245y = 13$ n'admet aucune solution entière.

5 Après le TD

Exercice 9. Pour chacun des couples (a, b) suivants, déterminer le PGCD de (a, b) et trouver une solution $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ à l'équation $au + bv = \mathrm{PGCD}(a, b)$.

1. $(a, b) = (167, 115)$
2. $(a, b) = (153, 40)$
3. $(a, b) = (174, 48)$

Exercice 10. Pour chacune des équations suivantes, justifier s'il existe des solutions $(x, y) \in \mathbb{Z}$ ou non. Lorsque c'est le cas, déterminer une solution particulière, puis l'ensemble des solutions en justifiant soigneusement.

1. $167x + 115y = 1$
2. $153x + 40y = 3$
3. $174x + 48y = 3$
4. $174x + 48y = 6$
5. $174x + 48y = 12$