Chapitre 3. PGCD et Applications

Boulanger Yann

20 juin 2025

Table des matières

1 Introduction

Une motivation : l'arithmétique est au cœur du cryptage des communications.
Pour crypter un message on commence par le transformer en un (ou plusieurs) nombre(s).
Le processus de codage et décodage fait appel à plusieurs notions de ce chapitre :

— Choix de deux nombres premiers p et q que l'on garde secrets, on pose $n = p \times q$.
— La clé secrète et la clé publique se calculent à l'aide de l'algorithme d'Euclide et des coefficients de Bézout.
— Les calculs de cryptage se font modulo n.
— Le décodage fonctionne grâce à une variante du petit théorème de Fermat.

2 Division euclidienne et PGCD

2.1 Divisibilité et division euclidienne

Définition 1 Soient $a, b \in \mathbb{Z}$. On dit que b divise a, noté $b|a$, s'il existe $q \in \mathbb{Z}$ tel que $a = bq$.

Exemples

— $7|21$, $6|48$, a est pair si et seulement si $2|a$.
— Pour tout $a \in \mathbb{Z}$, $a|0$ et $1|a$.
— Si $a|1$ alors $a = \pm 1$.
— Si $a|b$ et $b|a$ alors $a = \pm b$.
— Si $a|b$ et $b|c$ alors $a|c$.
— Si $a|b$ et $a|c$ alors $a|b + c$.

Théorème 1
Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$. Il existe des entiers $q, r \in \mathbb{Z}$ tels que :

$$a = bq + r \quad \text{avec } 0 \leq r < b.$$

De plus, q et r sont uniques.

Exemple : $6789 = 34 \times 199 + 23$.

2.2 PGCD de deux entiers

Définition 2
Soient $a, b \in \mathbb{Z}$, non tous les deux nuls.
Le plus grand entier qui divise à la fois a et b s'appelle le **plus grand diviseur commun**, noté $\text{pgcd}(a, b)$.

Exemples

$$\text{pgcd}(21, 14) = 7, \quad \text{pgcd}(12, 32) = 4, \quad \text{pgcd}(21, 26) = 1.$$

2.3 Algorithme d'Euclide

Lemme 1 Si $a = bq + r$ alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Exemple

$$\begin{aligned} 600 &= 124 \times 4 + 104 \\ 124 &= 104 \times 1 + 20 \\ 104 &= 20 \times 5 + 4 \\ 20 &= 4 \times 5 + 0 \end{aligned} \Rightarrow \text{pgcd}(600, 124) = 4.$$

2.4 Nombres premiers entre eux

Définition 3
Deux entiers a, b sont **premiers entre eux** si $\text{pgcd}(a, b) = 1$.

Exemple : a et $a + 1$ sont premiers entre eux.

Remarque On peut toujours écrire $a = a'd$, $b = b'd$ avec $\text{pgcd}(a', b') = 1$ si $d = \text{pgcd}(a, b)$.

3 Théorème de Bézout

Théorème 2
Soient $a, b \in \mathbb{Z}$. Il existe $u, v \in \mathbb{Z}$ tels que

$$au + bv = \text{pgcd}(a, b).$$

Exemple : Pour $a = 600$, $b = 124$, on obtient :

$$600 \times 6 + 124 \times (-29) = 4.$$

3.1 Corollaires du théorème de Bézout

— Si $d|a$ et $d|b$ alors $d|\text{pgcd}(a, b)$.
— a et b sont premiers entre eux $\Leftrightarrow$ il existe u, v tels que $au + bv = 1$.
— (Lemme de Gauss) Si $a|bc$ et $\text{pgcd}(a, b) = 1$ alors $a|c$.

4 Équation diophantienne $ax + by = c$

Proposition 1

1. $ax + by = c$ a des solutions entières si et seulement si $\text{pgcd}(a, b)|c$.
2. Si c'est le cas, toutes les solutions sont de la forme : $(x, y) = (x_0 - \beta k, y_0 + \alpha k)$ pour $k \in \mathbb{Z}$.

Exemple : Résoudre $161x + 368y = 115$:

$$\begin{aligned} 368 &= 161 \times 2 + 46 \\ 161 &= 46 \times 3 + 23 \\ 46 &= 23 \times 2 + 0 \Rightarrow \text{pgcd} = 23 \Rightarrow 115 = 5 \times 23 \end{aligned}$$

On trouve une solution particulière $(x_0, y_0) = (35, -15)$, et toutes les solutions sont de la forme :

$$x = 35 - 16k, \quad y = -15 + 7k, \quad k \in \mathbb{Z}.$$

5 PPCM

Définition 4
Le **ppcm** (plus petit multiple commun) de a et b est le plus petit entier > 0 divisible par a et par b.

Relation.

$$\text{pgcd}(a, b) \times \text{ppcm}(a, b) = |ab|.$$

Fin de chapitre