Chapitre 9 : Arithmétique sur $\mathbb{Z}$

Dr Nicolas Provost - PCSI1 - LMB

1 Division euclidienne et divisibilité

Théorème 1.1. *Pour tout couple $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que :*

$$a = bq + r \text{ avec } 0 \leq r < |b|. \tag{1}$$

L'entier q s'appelle le quotient de la division euclidienne et r est le reste.

Définition. *On dit que b divise a et on note $b|a$ si le reste dans la division euclidienne est nul.*
On dit que a_1 est congrue à a_2 modulo b et on note $a_1 = a_2[b]$ s'ils ont le même reste dans leurs divisions euclidiennes par b.

Proposition 1.2. *La divisibilité est une relation d'ordre sur $\mathbb{N}^*$ qui n'est pas totale.*
Pour tout $b \neq 0$, la congruence modulo b est une relation d'équivalence sur $\mathbb{Z}$.

Proposition 1.3. *Si $a_1 = r_1[b]$ et $a_2 = r_2[b]$ alors $a_1 + a_2 = r_1 + r_2[b]$ et $a_1 a_2 = r_1 r_2[b]$.*
Si $a = r[b]$ et $n \in \mathbb{N}^*$ alors $an = rn[bn]$ et $a^n = r^n[b]$.

2 PGCD et PPCM

Définition. *Soient $a, b \in \mathbb{Z}$ deux entiers.*

PGCD *On appelle Plus Grand Commun Diviseur de a et b et on note $PGCD(a,b)$ le plus grand entier $d \in \mathbb{N}^*$ tel que : $d|a$ et $d|b$.*

PPCM *On appelle Plus Petit Commun Multiple de a et b et on note $PPCM(a,b)$ le plus petit entier naturel non nul $m \in \mathbb{N}^*$ tel que : $a|m$ et $b|m$.*

Proposition 2.1. **a)** *Le $PGCD(a,b)$ est l'unique $d \in \mathbb{N}$ tel que :* $\begin{cases} d|a \text{ et } d|b \\ \forall k \in \mathbb{Z}, (k|a \text{ et } k|b) \Rightarrow k|d. \end{cases}$

b) *Le $PPCM(a,b)$ est l'unique $m \in \mathbb{N}^*$ tel que :* $\begin{cases} a|m \text{ et } b|m \\ \forall k \in \mathbb{Z}, (a|k \text{ et } b|k) \Rightarrow m|k. \end{cases}$

⊗ On obtient en particulier $a\mathbb{Z} \cap b\mathbb{Z} = PPCM(a,b)\mathbb{Z}$.

Théorème 2.2 (Algorithme d'Euclide)**.** *On effectue les divisions euclidiennes successives des restes $r_n = q_n r_{n+1} + r_{n+2}$ avec $r_0 = a$ et $r_1 = b$. Le dernier reste non nul est $PGCD(a,b)$.*

⊗ On peut programmer l'algorithme d'Euclide en construisant la suite des restes $(r_n)_{n \geq 0}$.

```
def PGCD(a, b):
    r0, r1 = a, b
    while r1!=0:
        r0, r1 = r1, r0%r1
    return r0
```

Définition. *On dit que a et b sont premiers entre eux si $PGCD(a,b)=1$.*

Théorème 2.3 (Bézout)**.** *a et b sont premiers entre eux ssi il existe $(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1$.*

⊗ On obtient en particulier $a\mathbb{Z}+b\mathbb{Z}=PGCD(a,b)\mathbb{Z}$.
⊗ On peut programmer la remontée d'Euclide sous forme matricielle avec $M_n\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}r_n\\r_{n+1}\end{pmatrix}$.
On montre que $M_{n+1}=\begin{pmatrix}0&1\\1&-q_n\end{pmatrix}M_n$ et au rang d'arrêt $M_N=\begin{pmatrix}u&v\\-b&a\end{pmatrix}$.

```
import numpy as np
def bezout(a, b):
    r0, r1 = a, b
    M = np.matrix([1,0],[0,1])
    while r1!=0:
        r0, r1, q = r1, r0%r1, r0//r1
        M = np.matrix([0,1],[1,-q])*M
    return M[0][0], M[0][1]
```

Théorème 2.4 (Gauss)**.** *Si d divise ab et si d est premier avec a alors d divise b.*

Proposition 2.5. *Pour tout $a,b\in\mathbb{Z}$, on a : $PGCD(a,b)PPCM(a,b)=|ab|$.*

3 Nombres premiers

Définition. *On dit que $p\in\mathbb{N}$ est un nombre premier s'il admet exactement deux diviseurs 1 et p.*

⊗ Pour tout $a\in\mathbb{Z}$, on a la disjonction $p|a$ ou p est premier avec a.
⊗ Les premiers nombres premiers sont $2,3,5,7,11,13,17,19,...$, ils peuvent être obtenus à l'aide du crible d'Eratosthène.

```
def crible(N):
    l = [False,False] + [True]*(N-1)
    p = 2
    while p*p<=N:
        if l[p]:
            for m in range(p*p, N+1, p):
                l[m] = False
        p+=1
    return [p for p in range(N+1) if l[p]]
```

Théorème 3.1. *Il existe une infinité de nombres premiers.*

Proposition 3.2. *Tout entier $n\in\mathbb{N}^*$ dispose d'une unique décomposition en produit de facteurs premiers : $n=\prod_{i=1}^r p_i^{\alpha_i}$ avec p_i des nombres premiers et $\alpha_i\in\mathbb{N}^*$.*

Proposition 3.3. *Si $a=\prod\limits_{p\ premier} p^{\alpha_p}$ et $b=\prod\limits_{p\ premier} p^{\beta_p}$ alors :*

$$PGCD(a,b)=\prod_{p\ premier} p^{\min(\alpha_p,\beta_p)}\ et\ PPCM(a,b)=\prod_{p\ premier} p^{\max(\alpha_p,\beta_p)} \tag{2}$$