Lecture 7 : The arithmetic of $\mathbb{Z}$

ENSIA 2023-2024

Contents

Euclidean division

Theorem 1

$\forall\, a \in \mathbb{Z}, \forall\, b \in \mathbb{N}^*$, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

a: dividend

b: divisor

q : quotient

r : remainder

Euclidean division

- The existence

Let $a \in \mathbb{Z}, b \in \mathbb{N}^*$. Set

$$E = \{p \in \mathbb{Z};\ a \geq bp\}$$

If $a \geq 0,\ 0 \in E$.

If $a < 0, a \in E$.

Then $E \neq \emptyset$.

On the other hand,

If $a \geq 0$ then $\forall p \in E, p \leq a$.

If $a < 0$ then $\forall p \in E, p \leq -a$.

We deduce that E is a nonempty upper bounded subset of $\mathbb{Z}$. Then E admits a maximal element ; denote $\max(E) = q$.

Euclidean division

Set $a = bq + r$, then $r = a - bq$. We have $r \in \mathbb{Z}$.

As $q \in E$, then $a \geq bq$, thus $r \geq 0$,

On the other hand, $q + 1 \notin E$ gives $a < b(q + 1)$, thus $r < b$.

- The unicity

Let (q, r) and $(q', r') \in \mathbb{Z}^2$ such that

$a = bq + r$ with $0 \leq r < b$ and $a = bq' + r'$ with $0 \leq r' < b$, thus

$b(q - q') = r' - r$ and $-\mathrm{b} < r - r' < b$. This implies that $|q - q'| < 1$, therefore

$q = q'$ and $r = r'$.

GCD, LCM

Definition :

Let $a, b \in \mathbb{Z}^*$. We say that a divides b and we denote $a \,/\, b$ if there exists $c \in \mathbb{Z}$ such that $b = ac$.

If a/b, we say that b is a multiple of a or that a is a divisor of b.

Let $a, b \in \mathbb{Z}^*$. The set of common divisors of a and b is finite and admits a greatest common divisor denoted $GCD(a, b)$.

The set of elements of $\mathbb{N}^*$ which are common multiples of a and b admits a least common multiple denoted $LCM(a, b)$.

Notations : $GCD(a, b) = a \wedge b, LCM(a, b) = a \vee b$.

GCD, LCM

Proposition

Let $a, b \in \mathbb{Z}^*$. Set $a\mathbb{Z} + b\mathbb{Z} = \{x + y; x \in a\mathbb{Z}, y \in b\mathbb{Z}\}$.

1) $a/b \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$
2) $a\mathbb{Z} \cap b\mathbb{Z} = LCM(a, b)\mathbb{Z}$
3) $a\mathbb{Z} + b\mathbb{Z} = GCD(a, b)\mathbb{Z}$

GCD, LCM

Proof of 3)

$a\mathbb{Z} + \mathrm{b}\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$. Then there exists $n \in \mathbb{N}^*$ such that

$a\mathbb{Z} + \mathrm{b}\mathbb{Z} = n\mathbb{Z}$.

Set $a \wedge b = d$ and show that $n = d$.

We have d/a and d/b, then $a\mathbb{Z} \subseteq d\mathbb{Z}$ and $b\mathbb{Z} \subseteq d\mathbb{Z}$.

Therefore $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$ and the $n\mathbb{Z} \subseteq d\mathbb{Z}$. This implies that d/n.

Then there exists $k \in \mathbb{N}^*$, $n = dk$.

We have $a \in n\mathbb{Z}$, so

n/a and $n/b \Longrightarrow n$ is a common divisor of a and $b \Longrightarrow n \leq d \Longrightarrow n = d$.

Some properties

$\forall a, b, \lambda \in \mathbb{Z}^*$, we have

1) $\mathrm{GCD}(\lambda a, \lambda b) = |\lambda| GCD(a, b)$
2) $\mathrm{LCM}(\lambda a, \lambda b) = |\lambda| LCM(a, b)$
3) λ / a and $\lambda / b \Leftrightarrow \lambda \ / \ GCD(a, b)$
4) a / λ and $b / \lambda \Leftrightarrow LCM(a, b) \ / \ \lambda$
5) $GCD(a, b) = 1 \Longrightarrow LCM(a, b) = |ab|$

EUCLID'S ALGORITHM

We use the algorithm to compute de GCD.

Let $a, b \in \mathbb{N}^*$ with $a \geq b$.

If b/a then $a \wedge b = b$.

If $b \nmid a$, we divide a by b using the euclidean division.

We have $a = bq_1 + r_1$ and $0 < r_1 < b, (q_1, r_1) \in \mathbb{N}^2$.

We show that $a \wedge b = b \wedge r_1$.

For all $c \in \mathbb{Z}$, we have

If $(c / a$ and $c / b)$ then $(c / a$ and $c / r_1)$ since $r_1 = a - bq_1$

If $(c / a$ and $c / r_1)$ then $(c / b$ and $c / a)$ since $a = bq_1 + r_1$

EUCLID'S ALGORITHM

The common divisors of a and b are then the common divisors of b and r_1,

and so $a \wedge b = b \wedge r_1$.

If r_1 / b then $a \wedge b = b \wedge r_1 = r_1$.

If $r_1 \nmid b$, we repeat the process.

We construct ordered pairs $(q_1, r_1), (q_2, r_2), \ldots$ such that

$$
\begin{gathered}
a = bq_1 + r_1,\ 0 < r_1 < b, \\
b = r_1 q_2 + r_2, 0 < r_2 < r_1 \\
\vdots \\
\vdots
\end{gathered}
$$

As $b > r_1 > r_2 \ldots$ and $b, r_1, r_2, \ldots \in \mathbb{N}^*$, The process stops after a finite number of steps.

EUCLID'S ALGORITHM

There exists then $N \in \mathbb{N}^*$ and $(q_1, r_1), (q_2, r_2), \ldots, (q_N, r_N)$ in $\mathbb{N}^2$ such that

$$a = bq_1 + r_1,\ 0 < r_1 < b,$$

$$b = r_1 q_2 + r_2, 0 < r_2 < r_1$$

$$\vdots$$

$$r_{N-2} = r_{N-1} q_N + r_N, 0 < r_N < r_{N-1} \text{ and } r_N / r_{N-1}$$

We have then

$$a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \cdots = r_{N-1} \wedge r_N = r_N.$$

Coprime numbers

Definition

Let $a, b \in \mathbb{Z}^*$. We say that a and b are coprime if $a \wedge b = 1$.

Bezout's Theorem

$$a \wedge b = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}^* \text{ such that } au + bv = 1$$

Gauss' theorem

$\forall a, b, c \in \mathbb{Z}^*$, we have

$$a/bc \text{ and } a \wedge b = 1 \Longrightarrow a/c$$

Theorem

$$\forall a, b \in \mathbb{Z}^*,\ (a \wedge b)(a \vee b) = |ab|.$$

Congruence

Let $n \in \mathbb{N}^*$. Recall the relation R defined on $\mathbb{Z}$ by

$$x \, R \, y \iff x - y \in n\mathbb{Z}$$

is an equivalence relation.

Instead of $xR\,y$, we denote $x \equiv y[n]$ and we read

« x is congruent to y modulo n »

Rules of congruence

1) $x \equiv 0[n] \Longrightarrow x$ is divisible by n
2) $x \equiv y[n] \Longrightarrow x$ and y have the same reminder when dividing x and y by n
3) $x \equiv x'[n]$ and $y \equiv y'[n] \Longrightarrow x + y \equiv x' + y'[n]$ and $xy \equiv x'y'[n]$
4) $x \equiv y + z[n] \Longrightarrow x - z \equiv y[n]$
5) $\forall\, k \in \mathbb{Z}, x \equiv y[n] \Longrightarrow x + k \equiv y + k[n]$
6) $\forall\, k \in \mathbb{Z}, x \equiv y[n] \Longrightarrow kx \equiv ky[n]$
7) $\forall\, m \in \mathbb{N}^*, x \equiv y[n] \Longrightarrow x^m \equiv y^m[n]$
8) $\forall\, k \in \mathbb{Z}^*$ such that $k \wedge n = 1$, we have

$$kx \equiv ky[n] \Longrightarrow x \equiv y[n]$$

Prime numbers

Definition

Let $p \in \mathbb{N}$. We say that p is prime if $p \geq 2$ and

$$\forall\ a \in \mathbb{N}^*,\ (a\ /\ p\ \Longrightarrow a = 1 \text{ or } a = p)$$

A prime number $a \in \mathbb{Z}$ is an integer such that $|a|$ is prime.

We will admit the following fundamental theorem of arithmetic :

Theorem

Any element of $\mathbb{N} - \{0,1\}$ can be represented uniquely as a product of prime numbers, up to the order of factors.