Euclidean division

January 26^{th}, 2021

Absolute value – 1

Definition: absolute value of an integer

For $n \in \mathbb{Z}$, we define the *absolute value of* n by $|n| := \begin{cases} n & \text{if } n \in \mathbb{N} \\ -n & \text{if } n \in (-\mathbb{N}) \end{cases}$.

Absolute value – 2

Proposition

1. $\forall n \in \mathbb{Z},\ |n| \in \mathbb{N}$
2. $\forall n \in \mathbb{Z},\ n \leq |n|$
3. $\forall n \in \mathbb{Z},\ |n| = 0 \Leftrightarrow n = 0$
4. $\forall a, b \in \mathbb{Z},\ |ab| = |a||b|$
5. $\forall a, b \in \mathbb{Z},\ |a| \leq b \Leftrightarrow -b \leq a \leq b$

Absolute value – 2

Proposition

1. $\forall n \in \mathbb{Z}, |n| \in \mathbb{N}$
2. $\forall n \in \mathbb{Z}, n \leq |n|$
3. $\forall n \in \mathbb{Z}, |n| = 0 \Leftrightarrow n = 0$
4. $\forall a, b \in \mathbb{Z}, |ab| = |a||b|$
5. $\forall a, b \in \mathbb{Z}, |a| \leq b \Leftrightarrow -b \leq a \leq b$

Proof.

1. If $n \in \mathbb{N}$ then $|n| = n \in \mathbb{N}$.
   If $n \in (-\mathbb{N})$ then $n = -m$ for some $m \in \mathbb{N}$ and $|n| = -n = -(-m) = m \in \mathbb{N}$.
2. *First case:* $n \in \mathbb{N}$. Then $n \leq n = |n|$.
   Second case: $n \in (-\mathbb{N})$. Then $n \leq 0 \leq |n|$.
3. Note that $|0| = 0$ and that if $n \neq 0$ then $|n| \neq 0$.
4. You have to study separately the four cases depending on the signs of a and b.
5. If $b < 0$ then $|a| \leq b$ and $-b \leq a \leq b$ are both false. So we may assume that $b \in \mathbb{N}$. Then
   First case: $a \in \mathbb{N}$. Then $|a| \leq b \Leftrightarrow a \leq b \Leftrightarrow -b \leq a \leq b$.
   Second case: $a \in (-\mathbb{N})$. Then $|a| \leq b \Leftrightarrow -a \leq b \Leftrightarrow -b \leq a \Leftrightarrow -b \leq a \leq b$. ∎

Theorem: Euclidean division

Given $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$, there exists a unique couple $(q, r) \in \mathbb{Z}^2$ such that

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

The integers q and r are respectively the *quotient* and the *remainder* of the division of a by b.

Euclidean division – 1

Theorem: Euclidean division

Given $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$, there exists a unique couple $(q, r) \in \mathbb{Z}^2$ such that

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

The integers q and r are respectively the *quotient* and the *remainder* of the division of a by b.

Existence: *First case:* $b > 0$. We set $E = \{p \in \mathbb{Z} \ : \ bp \leq a\}$.

- $E \neq \varnothing$, indeed if $0 \leq a$ then $0 \in E$, otherwise $a \in E$.
- $|a|$ is an upper bound of E *(check it)*.

Thus E is a non-empty subset of $\mathbb{Z}$ which is bounded from above.
Hence it admits a greatest element, i.e. there exists $q \in E$ such that $\forall p \in E,\ p \leq q$.
We set $r = a - bq$. Since $q \in E$, $r = a - bq \geq 0$.
And $q + 1 \notin E$ since $q + 1 > q$ whereas q is the greatest element of E.
Therefore $b(q + 1) > a$, so $r = a - bq < b = |b|$.
We wrote $a = bq + r$ with $0 \leq r < |b|$ as expected.

Euclidean division – 1

Theorem: Euclidean division

Given $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$, there exists a unique couple $(q, r) \in \mathbb{Z}^2$ such that

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

The integers q and r are respectively the *quotient* and the *remainder* of the division of a by b.

Existence:
Second case: assume that $b < 0$.
Then we apply the first case to a and $-b > 0$:
there exists $(q, r) \in \mathbb{Z}^2$ such that $a = -bq + r = b(-q) + r$ with $0 \leq r < -b = |b|$.

Euclidean division – 1

Theorem: Euclidean division

Given $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$, there exists a unique couple $(q, r) \in \mathbb{Z}^2$ such that

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

The integers q and r are respectively the *quotient* and the *remainder* of the division of a by b.

Uniqueness: Let (q, r) and (q', r') be two suitable couples.
Then $r' - r = (a - bq') - (a - bq) = b(q - q')$. Besides

$$\begin{cases} 0 \leq r < |b| \\ 0 \leq r' < |b| \end{cases} \implies \begin{cases} -|b| < -r \leq 0 \\ 0 \leq r' < |b| \end{cases} \implies -|b| < r' - r < |b|$$

Thus $-|b| < b(q - q') < |b|$, from which we get $|b||q - q'| = |b(q - q')| < |b|$.
Since $|b| > 0$, we obtain $0 \leq |q - q'| < 1$.
Therefore $|q - q'| = 0$, which implies that $q - q' = 0$, i.e. $q = q'$.
Finally, $r' = b - aq' = b - aq = r$. ■

Euclidean division – 2

Examples

- Division of 22 by 5:

$$22 = 5 \times 4 + 2$$

  The quotient is $q = 4$ and the remainder is $r = 2$.

- Division of -22 by 5:

$$-22 = 5 \times (-5) + 3$$

  The quotient is $q = -5$ and the remainder is $r = 3$.

- Division of 22 by -5:

$$22 = (-5) \times (-4) + 2$$

  The quotient is $q = -4$ and the remainder is $r = 2$.

- Division of -22 by -5:

$$-22 = (-5) \times 5 + 3$$

  The quotient is $q = 5$ and the remainder is $r = 3$.

Euclidean division – 3

Proposition: parity of an integer

Given $n \in \mathbb{Z}$, exactly one of the followings occurs:

- either $n = 2k$ for some $k \in \mathbb{Z}$ *(then we say that n is even)*,
- or $n = 2k + 1$ for some $k \in \mathbb{Z}$ *(then we say that n is odd)*.

Euclidean division – 3

Proposition: parity of an integer

Given $n \in \mathbb{Z}$, exactly one of the followings occurs:

- either $n = 2k$ for some $k \in \mathbb{Z}$ *(then we say that n is even)*,
- or $n = 2k + 1$ for some $k \in \mathbb{Z}$ *(then we say that n is odd)*.

Proof. Let $n \in \mathbb{Z}$.
By Euclidean division by 2, there exist $k, r \in \mathbb{Z}$ such that $n = 2k + r$ and $0 \leq r < 2$.
Hence either $r = 0$ or $r = 1$.
And these cases are exclusive by the uniqueness of the Euclidean division. ∎