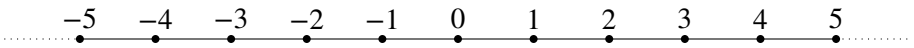
2 - Integers

Jean-Baptiste Campesato

In this chapter, we are going to construct the set $\mathbb{Z}$ of integers and then to study its properties. The informal idea consists in extending $\mathbb{N}$ by adding its *symmetry* with respect to 0:



For this purpose, we have to give a meaning to the notation $-n$ where n is a natural number and then we have to extend from $\mathbb{N}$ to $\mathbb{Z}$ the operations $(+,\times)$ and the order $(\leq)$.

There are several ways to formally do that. The usual one consists in defining $\mathbb{Z} = (\mathbb{N}\times\mathbb{N})/\sim$ for the equivalence relation $(a,b)\sim(c,d) \Leftrightarrow a+d=b+c$. Let me explain what does it mean: intuitively (a,b) stands for $a-b$, but, since such an expression is not unique (e.g. $7-5=10-8$), we need to "identify" some couples (e.g. $(7,5)=(10,8)$). This construction has several advantages (it is easy to extend $+$, $\times$ and $\leq$) but it needs an additional layer of abstraction (equivalence relations, equivalence classes...).

Instead, I will use a more naive approach. The counterpart is that extending the operations will be a little bit tedious with several cases to handle (e.g. the definition of $a+b$ will depend on the signs of a and b, so we have 4 cases just to define the addition...).

Note that what we are going to describe in a few lines took centuries to be developped and accepted: during the 18th century, most mathematicians were still reluctant about using negative numbers.

Contents

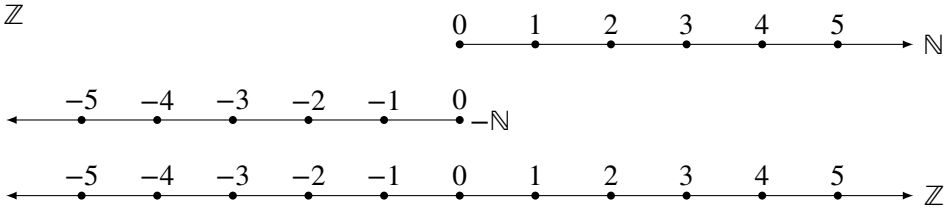
1 Construction of the integers

1.1 Definition

Definition 1. For any $n \in \mathbb{N} \setminus \{0\}$, we formally introduce the symbol $-n$ read as *minus n* and we fix the convention that $-0 = 0$.
We define the set $-\mathbb{N} \coloneqq \{-n \ : \ n \in \mathbb{N}\}$. Then the *set of integers* is $\mathbb{Z} \coloneqq (-\mathbb{N}) \cup \mathbb{N}$.

Remark 2. $(-\mathbb{N}) \cap \mathbb{N} = \{0\}$

Remark 3. $\mathbb{N} \subset \mathbb{Z}$



1.2 Operations

Definition 4. For $m, n \in \mathbb{N}$, we set:
(i) $m + n$ for the usual addition in $\mathbb{N}$
(ii) $(-m) + (-n) = -(m + n)$
(iii) $m + (-n) = \begin{cases} k \text{ where } k \text{ is the unique natural integer such that } m = n + k \text{ if } n \leq m \\ -k \text{ where } k \text{ is the unique natural integer such that } n = m + k \text{ if } m \leq n \end{cases}$
(iv) $(-m) + n = n + (-m)$ where $n + (-m)$ is defined in (iii)

We've just defined $+ : \begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ (a, b) & \mapsto & a + b \end{array}$.

Remark 5. We have to check that the overlapping cases $m = 0$ or $n = 0$ are not contradictory.

Definition 6. For $m, n \in \mathbb{N}$, we set:
(i) $m \times n$ for the usual product in $\mathbb{N}$
(ii) $(-m) \times (-n) = m \times n$
(iii) $m \times (-n) = -(m \times n)$
(iv) $(-m) \times n = -(m \times n)$

We've just defined $\times : \begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ (a, b) & \mapsto & a \times b \end{array}$.

Remark 7. We may simply write ab for $a \times b$ when there is no possible confusion.

Remark 8. Note that the addition and product on $\mathbb{Z}$ are compatible with the addition and product on $\mathbb{N}$.

Definition 9. For $n \in \mathbb{N}$, we set $-(-n) = n$. Then $-a$ is well-defined for every $a \in \mathbb{Z}$.

Proposition 10.
- $+$ *is associative:* $\forall a, b, c \in \mathbb{Z},\ (a + b) + c = a + (b + c)$
- 0 *is the unit of* $+$*:* $\forall a \in \mathbb{Z},\ a + 0 = 0 + a = a$
- $-a$ *is the additive inverse of* a*:* $\forall a \in \mathbb{Z},\ a + (-a) = (-a) + a = 0$
- $+$ *is commutative:* $\forall a, b \in \mathbb{Z},\ a + b = b + a$
- $\times$ *is associative:* $\forall a, b, c \in \mathbb{Z},\ (ab)c = a(bc)$
- $\times$ *is distributive with respect to* $+$*:* $\forall a, b, c \in \mathbb{Z},\ a \times (b + c) = ab + ac$ *et* $(a + b)c = ac + bc$
- 1 *is the unit of* $\times$*:* $\forall a \in \mathbb{Z},\ 1 \times a = a \times 1 = a$
- $\times$ *is commutative:* $\forall a, b \in \mathbb{Z},\ ab = ba$
- $\forall a, b \in \mathbb{Z},\ ab = 0 \Rightarrow \big(a = 0 \text{ or } b = 0\big)$

The above properties are easy to prove but the proofs are tedious with several cases depending on the signs.

Remark. From now on, we may simply write $a - b$ for $a + (-b)$ and $-a + b$ for $(-a) + b$.

Corollary 11. $\forall a, b, c \in \mathbb{Z},\ \big(ac = bc \text{ and } c \neq 0\big) \implies a = b$

Proof. Let $a, b, c \in \mathbb{Z}$ be such that $ac = bc$ and $c \neq 0$.
Then $(a - b)c = 0$. So either $a - b = 0$ or $c = 0$. Since $c \neq 0$, we get $a - b = 0$, i.e. $a = b$.. ■

1.3 Order

Definition 12. We define the binary relation $\leq$ on $\mathbb{Z}$ by

$$\forall a, b \in \mathbb{Z},\ a \leq b \Leftrightarrow b - a \in \mathbb{N}$$

Proposition 13. *$\leq$ defines a total order on $\mathbb{Z}$.*

Proof.

- *Reflexivity.* Let $a \in \mathbb{Z}$, then $a - a = 0 \in \mathbb{N}$ so $a \leq a$.
- *Antisymmetry.* Let $a, b \in \mathbb{Z}$. Assume that $a \leq b$ and that $b \leq a$. Then $b - a \in \mathbb{N}$ and $a - b \in \mathbb{N}$. So $a - b = -(b - a) \in (-\mathbb{N})$. Hence $a - b \in (-\mathbb{N}) \cap \mathbb{N} = \{0\}$ and thus $a = b$.
- *Transitivity.* Let $a, b, c \in \mathbb{Z}$. Assume that $a \leq b$ and that $b \leq c$. Then $b - a \in \mathbb{N}$ and $c - b \in \mathbb{N}$.
  Thus $c - a = (c - b) + (b - a) \in \mathbb{N}$, i.e. $a \leq c$.
- Let $a, b \in \mathbb{Z}$. Then $b - a \in \mathbb{Z} = (-\mathbb{N}) \cup (\mathbb{N})$.
  First case: $b - a \in \mathbb{N}$ then $a \leq b$.
  Second case: $b - a \in (-\mathbb{N})$, then $a - b = -(b - a) \in \mathbb{N}$ and $b \leq a$.
  Hence the order is total.

■

Proposition 14. *The order on $\mathbb{Z}$ is compatible with the order on $\mathbb{N}$.*

Proof. Let $a, b \in \mathbb{N}$.

- Assume that $a \leq_{\mathbb{Z}} b$. Then $k = b - a \in \mathbb{N}$. So $b = a + k$, i.e. $a \leq_{\mathbb{N}} b$.
- Assume that $a \leq_{\mathbb{N}} b$. Then $b = a + k$ for some $k \in \mathbb{N}$. Then $b - a = k \in \mathbb{N}$, i.e. $a \leq_{\mathbb{Z}} b$.

■

Proposition 15.

1. $\mathbb{N} = \{a \in \mathbb{Z},\ 0 \leq a\}$
2. $\forall a, b, c \in \mathbb{Z},\ a \leq b \Leftrightarrow a + c \leq b + c$
3. $\forall a, b, c, d \in \mathbb{Z},\ \big(a \leq b \text{ and } c \leq d\big) \Rightarrow a + c \leq b + d$
4. $\forall a, b \in \mathbb{Z},\ \forall c \in \mathbb{N} \setminus \{0\},\ a \leq b \Leftrightarrow ac \leq bc$
5. $\forall a, b \in \mathbb{Z},\ \forall c \in (-\mathbb{N}) \setminus \{0\},\ a \leq b \Leftrightarrow bc \leq ac$

Proof.

1. Let $a \in \mathbb{Z}$. Then $0 \leq a \Leftrightarrow a = a - 0 \in \mathbb{N}$.
2. Let $a, b, c \in \mathbb{Z}$. Then $a \leq b \Leftrightarrow b - a \in \mathbb{N} \Leftrightarrow (b + c) - (a + c) \in \mathbb{N} \Leftrightarrow a + c \leq b + c$.
3. Let $a, b, c, d \in \mathbb{Z}$. Assume that $a \leq b$ and that $c \leq d$. Then $b - a \in \mathbb{N}$ and $d - c \in \mathbb{N}$.
   Hence $(b + d) - (a + c) = (b - a) + (d - c) \in \mathbb{N}$, i.e. $a + c \leq b + d$.
4. Let $a, b \in \mathbb{Z}$ and $c \in \mathbb{N}$.
   $\Rightarrow$: Assume that $a \leq b$. Then $b - a \in \mathbb{N}$, thus $bc - ac = (b - a)c \in \mathbb{N}$. Therefore $ac \leq bc$.
   $\Leftarrow$: Assume that $c \neq 0$ and that $ac \leq bc$. Then $bc - ac = (b - a)c \in \mathbb{N}$. Assume by contradiction that $(b - a) \in (-\mathbb{N}) \setminus \{0\}$ then, by definition of the multiplication, $(b - a)c \in (-\mathbb{N}) \setminus \{0\}$, which is a contradiction. Hence $b - a \in \mathbb{N}$, i.e. $a \leq b$.
5. Let $a, b \in \mathbb{Z}$ and $c \in (-\mathbb{N})$.
   $\Rightarrow$: Assume that $a \leq b$. Then $b - a \in \mathbb{N}$, thus $ac - bc = (b - a)(-c) \in \mathbb{N}$. Therefore $bc \leq ac$.
   $\Leftarrow$: Assume that $c \neq 0$ and that $bc \leq ac$. Then $ac - bc = (b - a)(-c) \in \mathbb{N}$. And we conclude as in 4.

■

Remark 16. Given $a, b, c \in \mathbb{Z}$, it is common to lighten the notation by writing $a \leq b \leq c$ for $\big(a \leq b \text{ and } b \leq c\big)$.

Theorem 17.

1. *A non-empty subset A of $\mathbb{Z}$ which is bounded from below has a least element, i.e.*

$$\exists m \in A,\ \forall a \in A,\ m \leq a$$

2. *A non-empty subset A of $\mathbb{Z}$ which is bounded from above has a greatest element, i.e.*

$$\exists M \in A,\ \forall a \in A,\ a \leq M$$

Proof.

1. Assume that A is a non-empty subset of $\mathbb{Z}$ which is bounded from below.
   Then there exists $k \in \mathbb{Z}$ such that $\forall a \in A,\ k \leq a$. Define $S = \{a - k \ :\ a \in A\}$.
   Then S is a non-empty subset of $\mathbb{N}$ (indeed, $\forall a \in A,\ 0 \leq a - k$).
   By the well-ordering principle, there exists $\tilde{m} \in S$ such that $\forall a \in A,\ \tilde{m} \leq a - k$.
   Then $m = \tilde{m} + k$ is the least element of A (note that $\tilde{m} \in S$ so $m = \tilde{m} + k \in A$)

2. Assume that A is a non-empty subset of $\mathbb{Z}$ which is bounded from above. Then $(-A) = \{-a \ :\ a \in A\}$ is a non-empty subset of $\mathbb{Z}$ which is bounded from below (prove it).
   By the above, there exists $m \in (-A)$ such that $\forall a \in A,\ m \leq -a$. Hence $\forall a \in A,\ a \leq -m$.
   Thus $M \coloneqq -m$ is the greatest element of A.

■

2 Absolute value

Definition 18. For $n \in \mathbb{Z}$, we define the *absolute value of n* by $|n| \coloneqq \begin{cases} n & \text{if } n \in \mathbb{N} \\ -n & \text{if } n \in (-\mathbb{N}) \end{cases}$.

Proposition 19.

(i) $\forall n \in \mathbb{Z},\ |n| \in \mathbb{N}$
(ii) $\forall n \in \mathbb{Z},\ n \leq |n|$
(iii) $\forall n \in \mathbb{Z},\ |n| = 0 \Leftrightarrow n = 0$
(iv) $\forall a, b \in \mathbb{Z},\ |ab| = |a||b|$
(v) $\forall a, b \in \mathbb{Z},\ |a| \leq b \Leftrightarrow -b \leq a \leq b$
(vi) $\forall a, b \in \mathbb{Z},\ |a + b| \leq |a| + |b|$ (triangle inequality)

Proof.

(i) *First case:* if $n \in \mathbb{N}$ then $|n| = n \in \mathbb{N}$.
Second case: if $n \in (-\mathbb{N})$ then $n = -m$ for some $m \in \mathbb{N}$ and $|n| = -n = -(-m) = m \in \mathbb{N}$.
(ii) *First case:* $n \in \mathbb{N}$. Then $n \leq n = |n|$.
Second case: $n \in (-\mathbb{N})$. Then $n \leq 0 \leq |n|$.
(iii) Note that $|0| = 0$ and that if $n \neq 0$ then $|n| \neq 0$.
(iv) You have to study separately the four cases depending on the signs of a and b.
(v) 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 $|a| \leq b \Leftrightarrow -a \leq b \Leftrightarrow -b \leq a \Leftrightarrow -b \leq a \leq b$.
(vi) Since $a + b \leq |a| + |b|$ and $-(a + b) = -a - b \leq |-a| + |-b| = |a| + |b|$, we get $|a + b| \leq |a| + |b|$.

■

3 Euclidean division

Theorem 20 (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 called the quotient *and the* remainder *of the division of a by b.*

Proof.
Existence:
First case: assume that $0 < b$.
We set[1] $E = \{p \in \mathbb{Z} \ : \ bp \leq a\}$.

- $E \neq \emptyset$, indeed if $0 \leq a$ then $0 \in E$, otherwise $a \in E$.
- $|a|$ is an upper bound of E.
  Indeed, let $p \in E$.
  If $p \leq 0$ then $p \leq 0 \leq |a|$.
  Otherwise, if $0 < p$ then $1 \leq b \implies p \leq bp \leq a \leq |a|$.

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.
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 $0 \leq r < -b = |b|$.

Uniqueness: assume that we have two suitable couples (q, r) and (q', r').
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 $0 \leq |q - q'| < 1$.
But we proved in the first chapter that there is no natural number between 0 and 1.
Therefore $|q - q'| = 0$, which implies that $q - q' = 0$, i.e. $q = q'$.
Finally, $r' = b - aq' = b - aq = r$. ■

Examples 21.

- 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 $r = 3$.

Proposition 22. *Given* $n \in \mathbb{Z}$,

- *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),

and these cases are exclusive.

Proof. Let $n \in \mathbb{Z}$. By the Euclidean division by 2, there exist $k, r \in \mathbb{Z}$ such that $n = 2k + r$ and $0 \leq r \leq 1$. But we know from the last chapter that there is no natural number between 0 and 1. Hence either $r = 0$ or $r = 1$. These cases are exclusive by the uniqueness of the Euclidean division. ■

[1] When $b > 0$, the informal idea of this proof consists in determining *how many times* we can add b before exceeding a, which will give the quotient. Then the remainder will be obtained by filling the difference in order to reach a.
Intuitively, if the quotient exists, it has to be the greatest p such that $bp \leq a$. We have to prove the existence of such a number and then to check formally that this idea is actually correct.

4 Divisibility

Definition 23. Given $a, b \in \mathbb{Z}$, we say that *a is divisible by b* if there exists $k \in \mathbb{Z}$ such that $a = bk$.
In this case we write $b|a$ and we also say that *b is divisor of a* or that *a is a multiple of b*.

Examples 24. • $(-5)|10$ • $5 \nmid (-11)$
(*we will study divisibility criteria later in the term*)

Remarks 25.
- Any integer is a divisor of 0, i.e $\forall b \in \mathbb{Z}$, $b|0$. Indeed, $0 = b \times 0$.
- Any integer is divisible by 1 and itself, i.e. $\forall a \in \mathbb{Z}$, $1|a$ and $a|a$. Indeed, $a = 1 \times a = a \times 1$.
- The only integer divisible by 0 is 0 itself, i.e. $\forall a \in \mathbb{Z}$, $0|a \implies a = 0$.
  Indeed, then $a = 0 \times k$ for some $k \in \mathbb{Z}$ and hence $a = 0$.
- When $b \neq 0$, $b|a$ if and only if the remainder of the Euclidean division of a by b is $r = 0$.

Proposition 26.
1. $\forall a, b \in \mathbb{Z}$, $\big(a|b \text{ and } b|a\big) \implies |a| = |b|$
2. $\forall a, b, c \in \mathbb{Z}$, $\big(a|b \text{ and } b|c\big) \implies a|c$
3. $\forall a, b, c, d \in \mathbb{Z}$, $\big(a|b \text{ and } c|d\big) \implies ac|bd$
4. $\forall a, b, c, \lambda, \mu \in \mathbb{Z}$, $\big(a|b \text{ and } a|c\big) \implies a|(\lambda b + \mu c)$
5. $\forall a \in \mathbb{Z}$, $a|1 \implies |a| = 1$

Proof.
1. Let $a, b \in \mathbb{Z}$ satisfying $a|b$ and $b|a$. If $a = 0$ then $b = 0$ (from $0|b$). So we may assume that $a \neq 0$.
   There exist $k, l \in \mathbb{Z}$ such that $b = ak$ and $a = bl$. Then $a = bl = akl$, thus $1 = kl$ since $a \neq 0$.
   Therefore, $1 = |1| = |kl| = |k| \times |l|$. Since $|k|, |l| \in \mathbb{N}$, we get that $|k| = |l| = 1$.
   Finally, $|a| = |bl| = |b| \times |l| = |b| \times 1 = |b|$.
2. Let $a, b, c \in \mathbb{Z}$ satisfying $a|b$ and $b|c$. Then $b = ak$ and $c = bl$ for some $k, l \in \mathbb{Z}$.
   Therefore $c = bl = akl$, so $a|c$.
3. Let $a, b, c, d \in \mathbb{Z}$ satisfying $a|b$ and $c|d$. Then $b = ak$ and $d = cl$ for some $k, l \in \mathbb{Z}$.
   Therefore $bd = ackl$, so $ac|bd$.
4. Let $a, b, c \in \mathbb{Z}$ satisfying $a|b$ and $a|c$. Then $b = ka$ and $c = la$ for some $k, l \in \mathbb{Z}$.
   Hence $\lambda b + \mu c = \lambda ka + \mu la = (\lambda k + \mu l)a$. Thus $a|(\lambda b + \mu c)$.
5. Let $a \in \mathbb{Z}$. Assume that $a|1$. Then $a|1$ and $1|a$. So by the first item, $|a| = 1$.

■

5 Greatest common divisor

Theorem 27. *Given $a, b \in \mathbb{Z}$ not both zero, the set common divisors of a and b admits a greatest element denoted* $\gcd(a, b)$ *and called the* greatest common divisor of a and b.

Proof. Let $a, b \in \mathbb{Z}$ not both zero. We set $S = \{d \in \mathbb{Z} \ : \ d|a \text{ and } d|b\}$.
- S is non-empty since it contains 1.
- Since a and b are not both zero, we know that $a \neq 0$ or $b \neq 0$.
  Without loss of generality, let assume that $a \neq 0$.
  Let $d \in S$ then $a = dk$ for some $k \in \mathbb{Z}$. Note that $k \neq 0$ (otherwise $a = dk = 0$), hence $1 \leq |k|$.
  Thus $d \leq |d| \leq |d| \times |k| = |dk| = |a|$. Hence S is bounded from above by $|a|$.

Therefore, S admits a greatest element (as an non-empty subset of $\mathbb{Z}$ bounded from above). ■

Remark 28. Note that $\gcd(a, b) \geq 1$ since 1 is a common divisor of a and b (particularly $\gcd(a, b) \in \mathbb{N}$).

Proposition 29. *Let $a, b \in \mathbb{Z}$ not both zero and $d \in \mathbb{N} \setminus \{0\}$. Then*

$$\left\{ \begin{array}{l} d|a \\ d|b \\ \forall \delta \in \mathbb{N}, \ \big(\delta|a \text{ and } \delta|b\big) \implies \delta|d \end{array} \right| \implies d = \gcd(a, b)$$

Remark 30. We will see later that the converse holds (Proposition 35.(3)).

Proof. Let $a, b \in \mathbb{Z}$ not both zero and $d \in \mathbb{N} \setminus \{0\}$. Assume that $d|a$, $d|b$ and that d is a multiple of every non-negative common divisors, i.e.

$$\forall \delta \in \mathbb{N},\ \big(\delta|a \text{ and } \delta|b\big) \implies \delta|d$$

Then d is a common divisor of a and b. We need to prove that it is the greatest one.
Let $\delta \in \mathbb{Z}$ be a common divisor of a and b.

- If $\delta \leq 0$ then $\delta \leq d$.
- If $\delta > 0$ then $d = \delta k$ for some $k \in \mathbb{Z}$.
  Note that $k \geq 1$ since $d, \delta > 0$. Thus $\delta \leq \delta k = d$

■

The following theorem is extremely useful! We will use it quite often to study gcd and also when studying modular arithmetic!

Theorem 31 (Bézout's identity)**.** *Given $a, b \in \mathbb{Z}$ not both zero, there exist $u, v \in \mathbb{Z}$ such that*

$$au + bv = \gcd(a, b)$$

Example 32. $\gcd(15, 25) = 5 = 15 \times 2 + 25 \times (-1)$.
We will see below an algorithm in order to find a suitable couple (u, v).

Remarks 33.

- The couple (u, v) is not unique: $5 = 15 \times 27 + 25 \times (-16)$.
- The converse is false: $2 = 3 \times 4 + 5 \times (-2)$ but $\gcd(3, 5) = 1 \neq 2$.
  Nonetheless, we will see later that there is a partial converse when $\gcd(a, b) = 1$.

Proof of Theorem 31. Let $a, b \in \mathbb{Z}$ not both zero. Set $S = \{n \in \mathbb{N} \setminus \{0\} \ :\ \exists u, v \in \mathbb{Z},\ n = au + bv\}$.
Without loss of generality we may assume that $a \neq 0$.
Note that S is not empty. Indeed,

- If $a < 0$ then $n = a \times (-1) + b \times 0$ is in S, or,
- If $a > 0$ then $n = a \times 1 + b \times 0$ is in S.

Thus, by the well-ordering principle, S admits a least element d.
Since $d \in S$, we know that $d = au + bv$ for some $u, v \in \mathbb{Z}$.
Let's prove that $d = \gcd(a, b)$.

- By Euclidean division, there exist $q, r \in \mathbb{Z}$ such that $a = dq + r$ and $0 \leq r < |d| = d$.
  Assume by contradiction that $r \neq 0$.
  Then $r = a - qd = a - q(au + bv) = a \times (1 - qu) + b \times (-qv)$ is in S. Which contradicts the fact that d is the least element of S. Hence $r = 0$ and $a = dq$, i.e. $d|a$.
- Similarly $d|b$.
- Let $\delta \in \mathbb{Z}$ be another common divisor of a and b.
  Since $\delta|a$ and $\delta|b$, $a = \delta k$ and $b = \delta l$ for some $k, l \in \mathbb{Z}$. Hence $d = au + bv = \delta(ku + lv)$, i.e. $\delta|d$.

Therefore, by Proposition 29, $d = \gcd(a, b)$.
Hence $\gcd(a, b) = au + bv$ as requested. ■

Proposition 34. $\forall a \in \mathbb{Z} \setminus \{0\},\ \gcd(a, 0) = |a|$

Proof. By definition, $\gcd(a, 0)$ is the greatest divisor of a.
Since $a = |a| \times (\pm 1)$, we know that $|a|$ is a divisor of a. We have to check that it is the greatest one.
Let d be a non-negative divisor of a, then $a = dk$ for some $k \in \mathbb{Z}$.
Since $a \neq 0$, we know that $k \neq 0$.
Hence $1 \leq |k|$ from which we get that $d \leq d|k| = |d| \times |k| = |dk| = |a|$. ■

Proposition 35. *Let $a, b \in \mathbb{Z}$ not both zero, then*

1. $\gcd(a, b) = \gcd(b, a)$
2. $\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b)$
3. $\forall \delta \in \mathbb{Z}$, $\big(\delta | a \text{ and } \delta | b\big) \implies \delta | \gcd(a, b)$
4. $\forall \lambda \in \mathbb{Z} \setminus \{0\}$, $\gcd(\lambda a, \lambda b) = |\lambda| \gcd(a, b)$
5. $\forall k \in \mathbb{Z}$, $\gcd(a + kb, b) = \gcd(a, b)$

Proof. I will just prove 3, 4 and 5, the first two being easy to prove.

3. Let $a, b \in \mathbb{Z}$. Let $\delta \in \mathbb{Z}$. Assume that $\delta | a$ and $\delta | b$.
   By Bézout's theorem, $\gcd(a, b) = au + bv$ for some $u, v \in \mathbb{Z}$.
   Since $\delta | a$ and $\delta | b$, we have that $\delta \big| au + bv = \gcd(a, b)$.

4. Let $a, b \in \mathbb{Z}$ let $\lambda \in \mathbb{Z} \setminus \{0\}$. Since $|\lambda|$ divides λa and λb, then it divides $\gcd(\lambda a, \lambda b)$ by the third item.
   Hence $\gcd(\lambda a, \lambda b) = |\lambda| \times d$ for some $d \in \mathbb{Z}$. Let's prove that $d = \gcd(a, b)$.
   Let $n \in \mathbb{Z}$, then $n \big| a, b \Leftrightarrow |\lambda| n \big| \lambda a, \lambda b \Leftrightarrow |\lambda| n \big| \gcd(\lambda a, \lambda b) \Leftrightarrow n \big| d$.

5. Let $a, b, k \in \mathbb{Z}$. $\gcd(a, b) | a, b$ hence $\gcd(a, b) | a + kb$. Thus $\gcd(a, b) | \gcd(a + kb, b)$.
   Similarly, $\gcd(a + kb, b) | a + kb, b$ hence $\gcd(a + kb, b) | a + kb - kb = a$. Thus $\gcd(a + kb, b) | \gcd(a, b)$.
   Hence $|\gcd(a+kb, b)| = |\gcd(a, b)|$. Since they are both non-negative, we get $\gcd(a+kb, b) = \gcd(a, b)$.

■

6 Euclid's algorithm

Euclid's algorithm is an efficient way to compute the gcd of two numbers.

Let $a, b \in \mathbb{Z}$ not both zero.
Initialization of the algorithm. We set $a_0 \coloneqq |a|$ and $b_0 \coloneqq |b|$. Note that $\gcd(a_0, b_0) = \gcd(\pm a, \pm b) = \gcd(a, b)$.
Iteration. Assume that $a_n, b_n \in \mathbb{Z}$ are already constructed with $a_n, b_n \geq 0$ not both zero.

- If $b_n = 0$ then $\gcd(a_n, b_n) = a_n$ and the algorithm stops.
- Otherwise, by Euclidean division, there exist $q_n, r_n \in \mathbb{R}$ such that $a_n = b_n q_n + r_n$ and $0 \leq r_n < b_n$.
  We set $a_{n+1} \coloneqq b_n$ and $b_{n+1} \coloneqq r_n$, then $a_{n+1} = b_n > 0$ and $0 \leq b_{n+1} < b_n$.
  Moreover, using Proposition 35.(5),

$$\gcd(a_n, b_n) = \gcd(b_n q_n + r_n, b_n) = \gcd(r_n, b_n) = \gcd(b_n, r_n) = \gcd(a_{n+1}, b_{n+1})$$

  We repeat the iterative process with a_{n+1} and b_{n+1}.

Conclusion. Since the b_n are natural numbers and $0 \leq b_{n+1} < b_n$, there exists $N \in \mathbb{N}$ such that $b_N = 0$.
It proves that the algorithm ends after finitely many steps. Furthermore

$$\gcd(a, b) = \gcd(a_0, b_0) = \gcd(a_1, b_1) = \cdots = \gcd(a_N, b_N) = a_N$$

So the algorithm computes $\gcd(a, b)$ as expected.

Algorithm: Euclid's algorithm in pseudocode

Result: $\gcd(a, b)$ where $a, b \in \mathbb{Z}$ not both zero.
$a \leftarrow |a|$
$b \leftarrow |b|$
while $b \neq 0$ **do**
  $r \leftarrow a\%b$ (*the remainder of the Euclidean division* $a = bq + r$ *with* $0 \leq r < b$)
  $a \leftarrow b$
  $b \leftarrow r$
end
return a

Example 36. We want to compute $\gcd(600, -136)$:

$$\begin{array}{rcrcrcr|lll|rcl}
600 &=& 136 &\times& 4 &+& 56 & a_0 = 600, & b_0 = 136 & \gcd(600,-136) &=& \gcd(600,136)\\
136 &=& 56 &\times& 2 &+& 24 & a_1 = 136, & b_1 = 56 & \gcd(600,136) &=& \gcd(136,56)\\
56 &=& 24 &\times& 2 &+& 8 & a_2 = 56, & b_2 = 24 & \gcd(136,56) &=& \gcd(56,24)\\
24 &=& 8 &\times& 3 &+& 0 & a_3 = 24, & b_3 = 8 & \gcd(56,24) &=& \gcd(24,8)\\
 & & & & & & & a_4 = 8, & b_4 = 0 & \gcd(24,8) &=& \gcd(8,0) = 8
\end{array}$$

Hence $\gcd(600, -136) = 8$.

It is possible to obtain a suitable Bézout's identity from the above algorithm by going backward.

$$\begin{aligned}
8 &= 56 + 24 \times (-2) && \text{since } 8 = 56 - 24 \times 2\\
&= 56 + (136 + 56 \times (-2)) \times (-2) && \text{since } 24 = 136 - 56 \times 2\\
&= 136 \times (-2) + 56 \times 5 &&\\
&= 136 \times (-2) + (600 + 136 \times (-4)) \times 5 && \text{since } 56 = 600 - 136 \times 4\\
8 &= 600 \times 5 + (-136) \times 22 &&
\end{aligned}$$

7 Coprime integers

Definition 37. Let $a, b \in \mathbb{Z}$ not both zero. We say that a and b are *coprime* (or *relatively prime*) if $\gcd(a, b) = 1$.

The following result states that the converse of Bézout's identity holds **for coprime numbers**.

Proposition 38. *Let $a, b \in \mathbb{Z}$ not both zero. Then*

$$\gcd(a, b) = 1 \Leftrightarrow \exists u, v \in \mathbb{Z},\ au + bv = 1$$

Proof.
$\Rightarrow$: it is simply Bézout's identity.
$\Leftarrow$: let $a, b \in \mathbb{Z}$ not both zero. Assume that $au + bv = 1$ for some $u, v \in \mathbb{Z}$.
Set $d = \gcd(a, b)$. Then $d|a$ and $d|b$, hence $d|(au + bv) = 1$. So $|d| = 1$. But since $d \in \mathbb{N}$, we get that $d = 1$. ■

Theorem 39 (Gauss' lemma)**.** $\forall a, b, c \in \mathbb{Z}$, $\begin{cases} \gcd(a, b) = 1 \\ a|bc \end{cases} \implies a|c$

Proof. Let $a, b, c \in \mathbb{Z}$ such that $\gcd(a, b) = 1$ and $a|bc$. Then there exists $k \in \mathbb{Z}$ such that $bc = ka$. By Bézout's identity, there exist $u, v \in \mathbb{Z}$ such that $1 = au + bv$.
Thus $c = (au + bv)c = auc + bcv = auc + kav = a(uc + kv)$. Hence $a|c$. ■

The following result is very useful.

Proposition 40. *Let $a, b, c \in \mathbb{Z}$. If $a|c$, $b|c$ and $\gcd(a, b) = 1$ then $ab|c$.*

Proof. Since $a|c$ and $b|c$, there exist $k, l \in \mathbb{Z}$ such that $c = ak$ and $c = bl$.
Since $\gcd(a, b) = 1$, by Bézout's identity, there exists $u, v \in \mathbb{Z}$ such that $au + bv = 1$.
Then $c = auc + bvc = aubl + bvak = ab(ul + vk)$, so that $ab|c$. ■

8 A diophantine equation

Theorem 41. *Let $a, b, c \in \mathbb{Z}$ with a and b not both zero.*
Then the equation $ax + by = c$ has an integer solution if and only if $\gcd(a, b)|c$.

Proof.
$\Rightarrow$: Assume that $ax + by = c$ for some $(x, y) \in \mathbb{Z}^2$.
Since $\gcd(a, b)|a$ and $\gcd(a, b)|b$, we get that $\gcd(a, b)|ax + by = c$.
$\Leftarrow$: Assume that $\gcd(a, b)|c$, then there exists $k \in \mathbb{Z}$ such that $c = k \gcd(a, b)$.
By Bézout's identity, there exists $(u, v) \in \mathbb{Z}^2$ such that $au + bv = \gcd(a, b)$ hence $aku + bkv = k \gcd(a, b) = c$.
Therefore (ku, kv) is an integer solution of the equation. ■

How to find all the integer solutions of an equation of the form $ax+by=c$ with $a\neq 0$, $b\neq 0$ and $\gcd(a,b)|c$?

- *Step 1:* reduction to the case where $\gcd(a,b)=1$.
  There exist $\tilde{a},\tilde{b},\tilde{c}\in\mathbb{Z}$ such that $a=\tilde{a}\gcd(a,b)$, $b=\tilde{b}\gcd(a,b)$ and $c=\tilde{c}\gcd(a,b)$.
  Hence $ax+by=c \Leftrightarrow \tilde{a}x+\tilde{b}y=\tilde{c}$.
  Note that $\gcd(a,b)=\gcd(\tilde{a}\gcd(a,b),\tilde{b}\gcd(a,b))=\gcd(a,b)\gcd(\tilde{a},\tilde{b})$. Hence $\gcd(\tilde{a},\tilde{b})=1$.

- *Step 2:* find a first solution.
  By Bézout's identity, there exist $u,v\in\mathbb{Z}$ such that $\tilde{a}u+\tilde{b}v=1$ (we may find such a couple (u,v) using Euclid's algorithm).
  Thence $\tilde{a}\tilde{c}u+\tilde{b}\tilde{c}v=\tilde{c}$. Therefore we obtain a solution $(x_0,y_0)=(\tilde{c}u,\tilde{c}v)$ of $\tilde{a}x+\tilde{b}y=\tilde{c}$.

- *Step 3:* study the other solutions.
  Let $(x,y)\in\mathbb{Z}^2$ satisfying $\tilde{a}x+\tilde{b}y=\tilde{c}$. Then $\tilde{a}(x-x_0)+\tilde{b}(y-y_0)=0$, i.e. $\tilde{b}(y-y_0)=\tilde{a}(x_0-x)$.
  Since $\tilde{a}|\tilde{b}(y-y_0)$ and $\gcd(\tilde{a},\tilde{b})=1$, by Gauss' lemma, $\tilde{a}|y-y_0$, i.e. there exists $k\in\mathbb{Z}$ such that $k\tilde{a}=y-y_0$, i.e. $y=y_0+k\tilde{a}$.
  Then $\tilde{a}(x_0-x)=\tilde{b}(y-y_0)=k\tilde{a}\tilde{b}$. Since $\tilde{a}\neq 0$, we get $x_0-x=k\tilde{b}$, i.e. $x=x_0-k\tilde{b}$.
  We proved that there exists $k\in\mathbb{Z}$ such that $(x,y)=(x_0-k\tilde{b},y_0+k\tilde{a})$.

- *Step 4:* check the converse!
  We proved that if $(x,y)\in\mathbb{Z}^2$ is a solution, then there exists $k\in\mathbb{Z}$ such that $(x,y)=(x_0-k\tilde{b},y_0+k\tilde{a})$.
  It means that the solutions are among $(x,y)\in\left\{(x_0-k\tilde{b},y_0+k\tilde{a})\ :\ k\in\mathbb{Z}\right\}$.
  Otherwise stated, it means that $\left\{(x,y)\in\mathbb{Z}^2\ :\ \tilde{a}x+\tilde{b}y=\tilde{c}\right\}\subset\left\{(x_0-k\tilde{b},y_0+k\tilde{a})\ :\ k\in\mathbb{Z}\right\}$.
  It doesn't mean that they are all solutions, we need to check that separately, i.e. we need to prove the other inclusion.
  Conversely, let's prove that for every $k\in\mathbb{Z}$, $(x,y)=(x_0-k\tilde{b},y_0+k\tilde{a})$ is a solution:

$$\tilde{a}(x_0-k\tilde{b})+\tilde{b}(y_0+k\tilde{a})=\tilde{a}x_0+\tilde{b}y_0=\tilde{c}$$

- *Step 5:* Conclusion!
  The solutions are exactly the $(x,y)=(x_0-k\tilde{b},y_0+k\tilde{a})$ for $k\in\mathbb{Z}$.

See Slide 6 of Lecture 7 (Feb 2) for a concrete example.

A Appendix: properties of the strict order

Recall that given $a,b\in\mathbb{Z}$, $a<b$ means $\big(a\leq b \text{ and } a\neq b\big)$.
The following properties of $<$ are easy to derive from the ones of $\leq$.

- $\forall a,b,c\in\mathbb{Z},\ \big(a<b \text{ and } b\leq c\big)\implies a<c$
- $\forall a,b,c\in\mathbb{Z},\ \big(a\leq b \text{ and } b<c\big)\implies a<c$
- $\forall a,b,c,d\in\mathbb{Z},\ \big(a<b \text{ and } c\leq d\big)\implies a+c<b+d$
- $\forall a,b,c\in\mathbb{Z},\ a<b\implies a+c<b+c$
  (*that's a special case of the previous one where* $d=c$)
- $\forall a,b,c\in\mathbb{Z},\ \big(a<b \text{ and } c>0\big)\implies ac<bc$
- $\forall a,b,c\in\mathbb{Z},\ \big(a<b \text{ and } c<0\big)\implies ac>bc$
- $\forall a,b\in\mathbb{Z},\ a<b\Leftrightarrow a+1\leq b$
- Given $a,b\in\mathbb{Z}$, exactly one of the following occurs:
  (i) $a<b$
  (ii) $a=b$
  (iii) $a>b$
  Particularly, the negation of $a\leq b$ if $a>b$.

B Appendix: implementation of Euclid's algorithm in Julia

Euclid's algorithm in Julia (iterative)

```
function euclid(a::Integer, b::Integer)
    a != 0 || b != 0 || error("a and b must not be both zero")
    a = abs(a)
    b = abs(b)
    while b != 0
        r = a%b
        a = b
        b = r
    end
    return a
end
```

Actually, it is not important to replace a and b by their respective absolute values in the initialization. In this case, the sequence (b_n) is eventually non-negative so the algorithm stops as earlier and we just have to make sure that we return the absolute value of a at the end.

That being said, you should be careful because most programming languages don't use the above convention for Euclidean division. Instead, they require the remainder r to have the same sign as b, i.e. r satisfies $0 \leq r < b$ if $b > 0$ or $b < r \leq 0$ if $b < 0$.

But it doesn't matter for Euclid's algorithm: indeed, with this convention, the sequence $|b_n|$ is still decreasing, so the algorithm stops.

Therefore, we can simply write the following program (here $\gcd(0,0) = 0$ by convention).

Euclid's algorithm in Julia (recursive)

```
function euclid(a::Integer, b::Integer)
    b != 0 || return abs(a)
    return euclid(b,a%b)
end
```