Some notations about sets

$$
\begin{aligned}
\mathbb{N} &= \{0,1,2,\ldots\} && \text{natural numbers} \\
\mathbb{Z} &= \{\ldots,-2,-1,0,1,2,\ldots\} && \text{integers} \\
\mathbb{Z}_{>0} &= \{1,2,3,\ldots\} && \text{positive integers} \\
\mathbb{Z}_{\geq a} &= \{a,a+1,a+2,\ldots\} && \text{integers greater than or equal to } a \\
\mathbb{Q} &= \left\{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\}\right\} && \text{rational numbers}
\end{aligned}
$$

1.2 Congruences modulo an integer

Definition 1.2.1: Congruence modulo an integer (p16)

Let $n \in \mathbb{Z}$ be an integer. Given $a, b \in \mathbb{Z}$, we say that a and b are **congruent modulo** n if $a - b$ is a multiple of n.

$$
\begin{aligned}
a \text{ and } b \text{ are congruent modulo } n &\iff \exists k \in \mathbb{Z} : a - b = k \cdot n \\
&\iff a \equiv b \pmod{n}
\end{aligned}
$$

Definition 1.2.2: Congruence class modulo an integer (p17)

For $a, n \in \mathbb{Z}$ we define the **congruence class of** a **modulo** n as

$$a + n\mathbb{Z} := \{a + k \cdot n \mid k \in \mathbb{Z}\}$$

Any element from a congruence class is called a **representative** of that class. Note that it always holds that $a \in a + n\mathbb{Z}$

Lemma 1.2.3 (p17)

Let $a, b, n \in \mathbb{Z}$. Then

$$b \in a + n\mathbb{Z} \iff a \equiv b \pmod{n}$$

1.3 Equivalence relations

A relation $\sim$ on a set A is a subset of $A \times A$. We can describe a relation $\sim$ on A completely by using the set

$$R := \{(a,b) \in A \times A \mid a \sim b\}$$

Definition 1.3.1: Equivalence relation (p19)

Let A be a set. An **equivalence relation** $\sim$ on A is a relation on A that satisfies the following properties:

$$
\begin{aligned}
&1.\textbf{Reflexivity} && \forall a \in A: && a \sim a \\
&2.\textbf{Symmetry} && \forall a, b \in A: && a \sim b \Rightarrow b \sim a \\
&3.\textbf{Transitivity} && \forall a, b, c \in A: && a \sim b \wedge b \sim c \Rightarrow a \sim c
\end{aligned}
$$

Given an equivalence relation $\sim$ on a set A and an element $a \in A$, we define the **equivalence class** of a as

$$
\begin{aligned}
[a]_\sim &:= \{b \in A \mid a \sim b\} \\
&= \{b \in A \mid b \sim a\} && \text{because by 1.3.1 (2) } a \sim b \iff b \sim a
\end{aligned}
$$

An element $r \in [a]_\sim$ is called a **representative** of the equivalence class $[a]_\sim$.

1-1 Correspondence: Equivalence class and congruence class

The equivalence class of an integer $a \in \mathbb{Z}$ under the congruent modulo n relation, is precisely the congruence class $a + n\mathbb{Z}$:

$$[a]_{\equiv \pmod{n}} = a + n\mathbb{Z}$$

Proof: Let $b \in [a]_{\equiv \pmod{n}}$. Then $a \equiv b \pmod{n}$, which means $b \in a + n\mathbb{Z}$. Conversely, if $b \in a + n\mathbb{Z}$, then $b = a + k \cdot n$ for some $k \in \mathbb{Z}$, which implies $a \equiv b \pmod{n}$. Thus, we have shown that $[a]_{\equiv \pmod{n}} = a + n\mathbb{Z}$.

Theorem 1.3.3: Properties of equivalence classes (p20-21)

Let A be a set and $\sim$ an equivalence relation on A. Then we have:

1. $\forall a \in A$, $a \in [a]_\sim$.
2. The set A is covered by the equivalence classes: $\bigcup_{a \in A} [a]_\sim = A$.
3. $\forall a, b \in A$, either
   - $[a]_\sim = [b]_\sim$
   - $[a]_\sim \cap [b]_\sim = \emptyset$
4. $\forall a, b \in A : a \sim b \iff [a]_\sim = [b]_\sim$.

Corollary 1.3.4: Properties of congruence modulo an integer (p21)

1. $\forall a \in \mathbb{Z}$, $a \in a + n\mathbb{Z}$.
2. The set $\mathbb{Z}$ is covered by the congruence classes modulo n: $\bigcup_{a \in \mathbb{Z}} (a + n\mathbb{Z}) = \mathbb{Z}$.
3. $\forall a, b \in \mathbb{Z}$, either
   - $a + n\mathbb{Z} = b + n\mathbb{Z}$
   - $(a + n\mathbb{Z}) \cap (b + n\mathbb{Z}) = \emptyset$
4. $\forall a, b \in \mathbb{Z} : a + n\mathbb{Z} = b + n\mathbb{Z} \iff a \equiv b \pmod{n}$.

Fact 1.3.5: Division with remainder (p22)

Let $a, n \in \mathbb{Z}$ with $n > 0$. Then there exist **unique** integers $q, r \in \mathbb{Z}$ such that

1. $a = q \cdot n + r$
2. $0 \leq r < n$

Denote:

- $q = a \operatorname{quot} n$, the **quotient** of a divided by n
- $r = a \bmod n$, the **remainder** of a divided by n

Lemma 1.3.6 (p22)

Let $a, n \in \mathbb{Z}$ with $n > 0$. Then

$$a \equiv (a \bmod n) \pmod{n}$$

Proof: you just need to show that $a - (a \bmod n)$ is a multiple of n (because that's the definition of congruence modulo n). This is guaranteed by the division with remainder theorem, since $a = (a \operatorname{quot} n) \cdot n + (a \bmod n)$, so $a - (a \bmod n) = (a \operatorname{quot} n) \cdot n$.

Direct consequence of Lemma 1.3.6 and Definition 1.3.1 (2)

Because $a \equiv (a \bmod n) \pmod{n}$ and by symmetry of equivalence relations, we also have:

$$(a \bmod n) \equiv a \pmod{n}$$

Theorem 1.3.7: *Standard Representative* $(a \bmod n)$ (p23)

Let $n \in \mathbb{Z}_{\geq 0}, a \in \mathbb{Z}$.

The **only** representative of the congruence class $a + n\mathbb{Z}$ in $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ is $a \bmod n$.

We call $a \bmod n$ the **standard representative** of the congruence class $a + n\mathbb{Z}$, and

$$a + n\mathbb{Z} = (a \bmod n) + n\mathbb{Z}$$

There are only n different congruence classes modulo n, namely

$$0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}$$

Corrollary 1.3.8

Let $a, b, n \in \mathbb{Z}$ with $n \geq 0$. Then

$$(a + b) \bmod n \overset{\Delta}{a} +_n b = ((a \bmod n) + (b \bmod n)) \bmod n$$

and

$$(a \cdot b) \bmod n \overset{\Delta}{a} \cdot_n b = ((a \bmod n) \cdot (b \bmod n)) \bmod n$$

1.4 Modular arithmetic

Definition 1.4.1: Modular addition and multiplication (p25)

Let $n \in \mathbb{Z}_{\geq 0}$ and choose $a, b \in \mathbb{Z}_n$ arbitrarily. We define the following modular operations:

$$\begin{aligned} a +_n b &:= (a + b) \bmod n \qquad & \textbf{addition modulo } n \\ a \cdot_n b &:= (a \cdot b) \bmod n \qquad & \textbf{multiplication modulo } n \end{aligned}$$

Theorem 1.4.2: Properties of modular addition and multiplication (p25-26)

Let $n \in \mathbb{Z}_{\geq 0}$. Then for all $a, b, c \in \mathbb{Z}_n$ we have:

1. $a +_n b = b +_n a$ (commutativity of addition)
2. $(a +_n b) +_n c = a +_n (b +_n c)$ (associativity of addition)
3. $a \cdot_n b = b \cdot_n a$ (commutativity of multiplication)
4. $(a \cdot_n b) \cdot_n c = a \cdot_n (b \cdot_n c)$ (associativity of multiplication)
5. $a \cdot_n (b +_n c) = (a \cdot_n b) +_n (a \cdot_n c)$ (distributivity)

1.5 The extended Euclidean algorithm (EEA) for integers

Euclid's algorithm for computing the greatest common divisor (gcd)

Use the following recursive definition to compute $\gcd(a, b)$ for given integers $a, b \in \mathbb{Z}_{\geq 0}$, by computing the sequence $(a_0, b_0), (a_1, b_1), (a_2, b_2), \dots$ of pairs of integers as follows:

$$\begin{bmatrix} a_n \\ b_n \end{bmatrix} := \begin{cases} \begin{bmatrix} N \\ M \end{bmatrix} & \text{if } n = 0 \\ \begin{bmatrix} a_{n-1} - b_{n-1} \\ b_{n-1} \end{bmatrix} & \text{if } n \geq 1 \text{ and } a_{n-1} \geq b_{n-1} \\ \begin{bmatrix} b_{n-1} \\ a_{n-1} \end{bmatrix} & \text{if } n \geq 1 \text{ and } a_{n-1} < b_{n-1} \end{cases}$$

Theorem 1.5.2: Correctness of Euclid's basic algorithm (p28)

Let $N, M \in \mathbb{N}$. Let a_n and b_n be defined as in the above algorithm. Then

$$\exists m \in \mathbb{N} : b_m = 0 \land a_m = \gcd(N, M)$$

The extended Euclidean algorithm (EEA)

In some applications, it is not enough to compute $\gcd(N, M)$, but is it also important to express $\gcd(N, M)$ in N and M. More precisely, to find integers r and s such that...

Bézout's identity (p29)

For any integers $N, M \in \mathbb{Z}$, there exist integers $r, s \in \mathbb{Z}$ such that

$$r \cdot N + s \cdot M = \gcd(N, M)$$

The *extended* Euclidean algorithm not only computes $\gcd(N, M)$, but also the integers r and s from Bézout's identity.

$$\begin{bmatrix} a_n & r_n & s_n \\ b_n & t_n & u_n \end{bmatrix} := \begin{cases} \begin{bmatrix} N & 1 & 0 \\ M & 0 & 1 \end{bmatrix} & \text{if } n = 0, \\ \begin{bmatrix} a_{n-1} - b_{n-1} & r_{n-1} - t_{n-1} & s_{n-1} - u_{n-1} \\ b_{n-1} & t_{n-1} & u_{n-1} \end{bmatrix} & \text{if } n \geq 1 \text{ and } a_{n-1} \geq b_{n-1}, \\ \begin{bmatrix} b_{n-1} & t_{n-1} & u_{n-1} \\ a_{n-1} & r_{n-1} & s_{n-1} \end{bmatrix} & \text{if } n \geq 1 \text{ and } a_{n-1} < b_{n-1}. \end{cases}$$

This algorithm begins with the following 2 by 3 matrix:

$$\begin{pmatrix} N & 1 & 0 \\ M & 0 & 1 \end{pmatrix}$$

This matrix is gradually modified using **row operations**, until it has the form:

$$\begin{pmatrix} \gcd(N, M) & r & s \\ 0 & * & * \end{pmatrix}$$

where r **and** s **are the integers we are looking for.**