Chapter 2 part 1

Chapter 2

Congruences in $\mathbb{Z}$ and modular arithmetic

<u>Def</u> Let a, b, and n be integers, <u>$n>0$.</u>

$$\left.\begin{array}{l} a \text{ is congruent to } b \text{ modulo } n \\ \qquad\qquad (\text{mod } n) \\ a \equiv b \pmod{n} \end{array}\right\} \text{ means } \; n \mid (a-b)$$

Otherwise

$$\left.\begin{array}{l} a \text{ is not congr} \\ \text{to } b \text{ mod } n \\ a \not\equiv b \pmod{n} \end{array}\right\} \; n \nmid (a-b)$$

Congruence ($\equiv$) is a relation on $\mathbb{Z}$.

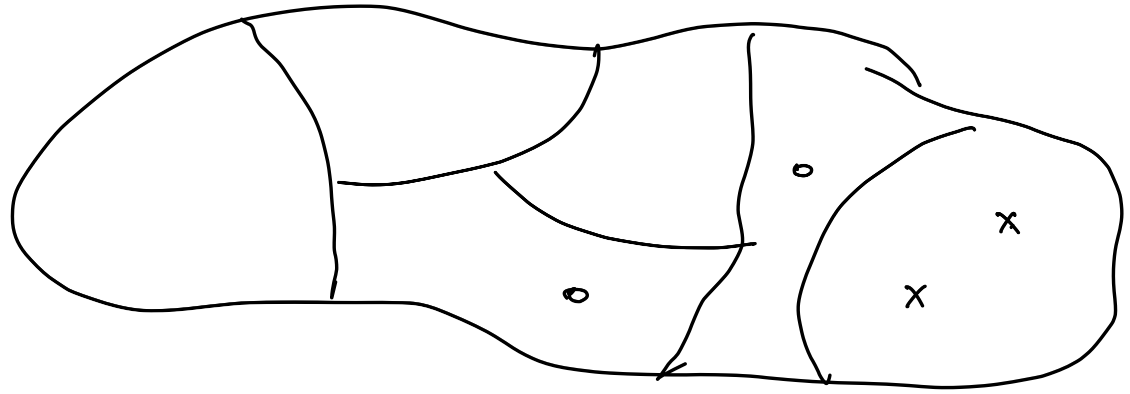
Th 2.1 The relation $\equiv$ on $\mathbb{Z}$ is an equivalence relation

Meaning:

reflexive	$a \equiv a \pmod{n}$
symmetric	$a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$
transitive	$\left.\begin{array}{l} a \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{array}\right\}$ implies $a \equiv c \pmod{n}$

Thus $\mathbb{Z}$ is partitioned into a disjoint union of equivalence classes

(Th 2.3, Cor 2.4)



Notation For $a \in \mathbb{Z}$ we (temporarily) denote by $[a]$ the equivalence class to which a belongs — a congruence class

$$[a] = \{ b \mid b \in \mathbb{Z},\ b \equiv a \pmod{n} \}$$
$$= \{ b \mid b \in \mathbb{Z},\ n \mid (a-b) \}$$
$$= \{ a + kn \mid k \in \mathbb{Z} \}$$

$n \mid (a-b)$

$a - b = -kn, \quad -k \in \mathbb{Z}$

$b = a + kn$

description of an equivalence class

a is a representative of its equivalence class

Description of all congruence classes modulo $n > 0$

Euclid's Lemma: for any integer a, we have

$$a = nq + r, \quad 0 \leq r < n.$$

We have $a \equiv r \pmod{n}$. $r \in [a]$ | $a - r = nq$, $n \mid (a-r)$

Every integer is congruent mod n to an integer in the interval $[0, \dots, n-1]$

Every congruence class has a representative among $[0, \dots, n-1]$

Integers from $[0, \dots, n-1]$ belong to different congruence classes because their differences are smaller than n, therefore not divisible by n.

The set of all congruence classes can be written as
$[0], [1], \ldots, [n-1]$

In particular, there are exactly n congruence classes modulo n (Cor 2.5)

<u>Notation</u> $\mathbb{Z}_n$ "$\mathbb{Z}$ mod n" - the set of congruence classes modulo n

$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ - set of n elements.