Reminder: an equivalence relation on a
partitions the set $A$ into equivalence
classes.

Example: $[n]_d = \text{class of an integer}
\mod d$

$= \{ a \in \mathbb{Z} \mid a \equiv n \mod d \}$

Key point (see 11.5): if you take two
integers from the same class mod $d$

$\wedge a, a'$

and $b, b'$ from some other class

then $aa'$ and $bb'$ end up in the same class.

And $a + a'$, $b + b'$ will be in the same class.

So: you can do arithmetic operations on
congruence classes!

$\text{Ex: } [3^k]_4 = [3]_4^k = [-1]_4^k = [(-1)^{k}]_4 = [1]_4 \text{ if even}$

because $3 \equiv -1 \mod 4$
Worksheet 13: Congruence of integers; Functions

1. Let \( d \in \mathbb{N} \). Prove that

\[
(a \equiv b \mod d) \land (a' \equiv b' \mod d) \Rightarrow aa' \equiv bb' \mod d.
\]

\( a \equiv b \mod d \) means: \( d \mid b-a \), so \( b-a = dk \) for some \( k \in \mathbb{Z} \).

Similarly, \( b' \equiv a' \mod d \) for some \( k' \in \mathbb{Z} \).

Then:
\[
b = dk + a, \quad b' = dk' + a'
\]

Thus:
\[
bb' = (dk + a)(dk' + a') = d(kk' + k + dka') + aa'.
\]

2. Prove that if an integer \( a \) is written with the digits \( a_n, \ldots, a_0 \), then \( a \) and \( a_0 + \cdots + a_n \) are in the same congruence class \( \mod 9 \).

Example:
\[
[12345678910111213]_9 = [1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9]_9 = [3]_9.
\]

3. Prove that for any integers \( a \) and \( b \), the sum \( a^2 + b^2 \) lies in one of the classes \([1], [0], \) or \([2] \mod 4 \). Deduce that the number 1000535 cannot be represented as a sum of two squares.

4. Prove that there do not exist integers \( a, b \) and \( c \) such that

\[
12345678910111213 = a^2 + 25b^2 + 5c^2.
\]
Textbook solution to #1:

Want to prove: \( d \mid bb' - aa' \)

Write \( bb' - aa' = b(b' - a') + ba' - aa' \)

\[ bb' - ba' \]

\[ = b(b' - a') + a'(b - a) \]

so \( d \mid bb' - aa' \), both are divisible by \( d \) by properties of congruences proved earlier.

Also prove: \( a \equiv a' \mod d \)

\( b \equiv b' \mod d \)

Then \( a + b \equiv a' + b' \mod d \).

Consequence: We can do operations (+, \( \times \)) on congruence classes \( \mod d \).

Can write \([a] \cdot [b] = [ab]\) (here \([a] \) is class \( \mod d \)).

\([a] + [b] = [a + b]\)

and these operations are well defined.
Question 2 explanation:

What I am saying is:
take a number, for example, 372
suppose we want to find its remainder
mod 9. A quick way: add up its digits:
\[ 3 + 7 + 2 = 12 \mod 9 \]
Answer: 3.

Our problem says: \( \overline{abc} \) = number written with digits a,b,c
\[ \overline{abc} \equiv a + b + c \mod 9 \] (or \( \equiv a \mod 3 \))
11
\[ 100a + 10b + c \]
Want to prove: \( \overline{abc} \equiv a + b + c \mod 9 \)
\[ \Rightarrow (100a + 10b + c) - (a + b + c) \]
3 divisible by 9.
we get: \( 99a + 9b \) - it is divisible by 9, and we are done.

In general: Lemma \( \forall n \in \mathbb{N}, 10^n \equiv 1 \mod 9 \)
Pf of Lemma: \[ [10^n]_9 = [10]_9^n = [1^0]_9^n = [1]_9 \]
(this is saying: \( 10 \equiv 1 \mod 9 \)
\[ \Rightarrow 10^n \equiv 1^n \mod 9 \) by
properties of congruences).

Now, suppose we have a number:
\[ A = \overline{a_n a_{n-1} \ldots a_0} \] written with the digits \( a_0, a_1, \ldots, a_n \)

Then \[ A = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_0 \]
\[ \equiv a_n \cdot 1 + a_{n-1} \cdot 1 + \ldots + a_0 \mod 9 \] by Lemma.
so we are done!
5. Let \( A = \{1, 2, 3\} \), and let \( B = \{a, b, c, d\} \). Let \( R = \{(1, a), (2, b), (2, c), (3, a), (3, d)\} \) - a relation from \( A \) to \( B \). Draw a diagram representing this relation.

6. Represent the function \( f : \mathbb{R} \to \mathbb{R} \) defined by \( f(x) = x^2 \) as a relation.

\[
R = \{(x, x^2) \mid x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}
\]

7. Represent the sequence \( a_n = \frac{1}{n} \) as a relation; think of it as a function from \( \mathbb{N} \) to \( \mathbb{R} \).

8. Give an example of a function that is injective but not surjective.

As a relation our sequence \( a_n \) is:

\[
\{(n, \frac{1}{n}) \mid n \in \mathbb{N}\} \subseteq \mathbb{N} \times \mathbb{R}
\]

It is a function from \( \mathbb{N} \) to \( \mathbb{R} \) domain \( \mathbb{N} \) codomain.
Functions (Chapter 12!) (Read 12.1 - 12.3)

A function \( f : A \rightarrow B \) is a relation \( R \) on \( A \times B \), such that every element of \( A \) appears exactly once as the first coordinate of an element of \( R \): \( \forall a \in A, \exists! (x, y) \in R \) such that \( x = a \).

Example: our question 5 in the worksheet is a relation from \( A \) to \( B \) which is not a function because \((2, b)\) and \((2, c)\) both are \( x \in R \).

\[ A = \{1, 2, 3\} \]
\[ B = \{a, b, c, d\} \]
\[ R = \{(1, b), (2, d), (3, a)\} \]

Every element of \( A \) has exactly one arrow coming out of it!
Def: In this situation, \( f : A \rightarrow B \)

\( A \) is called the domain of \( f \)

and \( B \) - the codomain of \( f \).

Remarks: The way we defined it here, \( f \) is defined at every element of the domain (in calculus before, you have \( f : \mathbb{R} \rightarrow \mathbb{R} \) but it's maybe not defined at some points, e.g., \( \frac{1}{x} \) not def'd at \( x = 0 \).

Here we write: \( f(x) = \frac{1}{x} \)

\[ f : \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R} \]

Codomain contains range of \( f \) but does not have to equal it:

\( f(x) = x^2 \) \( f : \mathbb{R} \rightarrow \mathbb{R} \) - OK.

\[ \text{range} (f) = \{ y \in \mathbb{R} \mid y \geq 0 \} \]