lecture 6
Thursday Jan. 23

Last time: congruence of integers

$\boxed{\text{Def: } a \equiv b \mod d \quad \text{if} \quad d \mid (a-b).}$

Proposition: Let $a, b \in \mathbb{Z}$ and $d \in \mathbb{Z}$, $d \neq 0$

Then $a \equiv b \mod d$ if and only if (iff) a and b have the same remainder when divided by d.

Pf: $a \equiv b \mod d \underset{\text{def. of congruence}}{\iff} d \mid (a-b)$

Divide with remainder: $a = dq_1 + r_1$, $b = dq_2 + r_2$ $\quad \boxed{\begin{array}{l} 0 \leq r_1 < d \\ 0 \leq r_2 < d. \end{array}}$

Then $\boxed{a - b = d(\underbrace{q_1 - q_2}_{\text{integer}}) + (r_1 - r_2).}$

So, $d \mid a-b \iff d \mid (r_1 - r_2)$

(because $d \mid d(q_1 - q_2)$)

we want to prove: in our situation,

$d \mid (r_1 - r_2) \iff r_1 = r_2$

By definition of r_1, r_2, we have: $0 \leq r_1 < d$
$0 \leq r_2 < d.$

Then $-d < r_1 - r_2 < d$

The only integer between $-d$ and d that is divisible by d is 0.

Thus, $d \mid (r_1 - r_2) \iff r_1 = r_2 = 0$, $\blacksquare$

Some notation:

since, because, therefore:

Q since P	:	$P \Rightarrow Q$
since Q, P	:	$Q \Rightarrow P$
P because Q	:	$Q \Rightarrow P$
P, therefore, Q		$P \Rightarrow Q$

Banned: $\because$ and $\therefore$

because if you try to use one to mean $P \Rightarrow Q$ and the other to mean $Q \Rightarrow P$ we have no way of telling which one you mean.

Worse: they easily look like: $\therefore$

Please use words.

Also: "iff" to mean "if and only if" is OK but not encouraged.

"s.t." for "such that" - OK.

Upshot:

when you divide a by d, there is unique (only one) remainder, but there is an infinite set of integers congruent to a mod d.

Example $\{ \overset{\mathbb{Z}}{x} : x \equiv 12 \bmod 25 \} = \{ x \in \mathbb{Z} : 25 \mid (x-12) \}$

$= \{ \dots, -38, -13, \overset{\text{remainder}}{12}, 37, 62, \dots \}$

Remainder of 62 mod 25 is $\underline{\underline{12}}$

(For any number in this set its remainder mod ~~\$~~25 is the smallest ~~positive~~ non-negative number in the set.)

(our Proposition says they all have the same remainder).

Problem 3 from last class worksheet:

any positive integer (written in the decimal system) is congruent ~~to~~ to the sum of its digits mod 9.

Understanding the problem: example:

take $a = 137$. Claim: $137 \equiv \underbrace{1+3+7}_{11} \bmod 9$

verify: $137 - 11 = 126 = 9 \cdot 14$

Try again: $5872 \overset{?}{\equiv} \underbrace{5+8+7+2}_{22} \bmod 9$

$5872 - 22 = 5850 = 9 \cdot 650$ works again!

Proof: we need notation to relate the number to its digits:

$\overline{a_n \ldots a_2 a_1 a_0}$ — will mean the number made up of digits $a_n, a_{n-1}, \ldots, a_0$

giving names to the digits.

$(a_n, a_{n-1}, \ldots, a_0 \in \{0,1,\ldots,9\})$

explanation of notation:

for 5872,

$a_0 = 2$
$a_1 = 7$
$a_2 = 8$
$a_3 = 5$

$\boxed{\text{and } \overline{a_3 a_2 a_1 a_0} = 5872}$

$n = 3$

Key point: $\overline{a_n a_{n-1} \ldots a_1 a_0}$

$= a_0 \cdot 10^0 + a_1 \cdot 10^1 + \ldots + a_n \cdot 10^n$

because of the way decimal system works.

our example: $5872 = 2 \cdot 10^0 + 7 \cdot 10 + 8 \cdot 100 + 5 \cdot 1000$

By definition of congruence, we need to prove: $a - (\text{sum of the digits of } a)$ is divisible by 9.

We have: $a = \overline{a_n a_{n-1} \ldots a_0}$, then

$a - (\text{sum of the digits})$

$= 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \ldots + 10^0 \cdot \cancel{a_0}$

$- (a_n + a_{n-1} + \ldots + \cancel{a_0})$

$= a_n (10^n - 1) + a_{n-1}(10^{n-1} - 1) + \ldots + a_1 (10 - 1) + 0$

$= a_n \cdot \underbrace{99\ldots9}_{n} + a_{n-1} \cdot (99\ldots9) + \ldots + a_1 \cdot 9 = 9(a_n \cdot \underbrace{1111}_{n} + \ldots + a_1)$

number of many 1's

(Lemma: for all $n \geq 0$, $10^n - 1$ is divisible by 9).

will prove later; easy to believe:

$10^n - 1$ is a number written down by n 9's.

Back to logic.

Quantifiers: $\exists$ - "exists"
existential quantifier

$\forall$ - "for all"
(universal quantifier)

Quantifiers are used with open sentences, to make actual statements.

Example: '$x > 2$' $= P(x)$ - open sentence
(true/false depends on x)

write: "$\forall x \in \mathbb{R}$, $x > 2$"

"for all real numbers x, $x > 2$ holds"

- false statement (no longer an open sentence)

"$\exists\, x \in \mathbb{R}$, s.t. $x > 2$" - true statement.

s.t. = such that:

in words: "exists a real number x such that $x > 2$"

"$\exists x \in \mathbb{R} : x > 2$" - also ok, I prefer comma:

"$\exists\, x \in \mathbb{R}$, $x > 2$"

More examples: Let P be the set of prime numbers.

- $\forall\, p \in P$, $p+2 \in P$ False: take $p = 13$, $p+2 = 15$ not prime.
- $\exists\, p \in P$, $p+2 \in P$ True: take $p = 3$, $p+2 = 5 \in P$.

counterexample shows it is false.

example proves an existential statement is true.

Worksheet 5: Quantifiers, part 1

Let us make some notation: let S be the set of all students in the class, and for every student $s \in S$, denote by $F(s)$ the set of all friends of s. For a person p, let $a(p)$ be the age of p.

1. Using this notation, write in symbols the statement: "There exists a student in the class all of *whose* friends are older than him/her".

hint $\exists p \in S, \ \ldots \ a(F(s)) > a(p)$

not ok: what is age (set ??)

Need: name another variable that ranges over $F(s)$.

2. Make similar notation and then write symbolically the statement "There exists a tree in Stanley park *such that* all the neighbouring trees are at least as tall as this tree."

will do next class. Please think about it!

3. Is this statement about Stanley park true or false?

6