

THE JOY OF NUMBERS

1. CONGRUENCE

Let a, b, m be any three integers. Recall from last time that $a \equiv b \pmod m$ if $m \mid a - b$, which means that there exists an integer k such that $km = a - b$. We noticed that if this is the case then m divides $b - a$ and this implies that $b \equiv a \pmod m$. This seems a pretty obvious thing but it is a very important property:

$$a \equiv b \pmod m \text{ then } b \equiv a \pmod m \text{ (**Reflexivity**)}$$

In fact not all the relation enjoy this property: if $a < b$ then $b < a$ doesn't always happen.

We also notice that in any case $a \equiv a \pmod m$.

$$\text{For every integer } a, a \equiv a \pmod m \text{ (**Symmetry**)}$$

At this point we decided to prove the first homework from last time.

(1.1) **Proposition.** *Let x and y be two integers. Let $x \in S_y$ then $S_x = S_y$.*

Proof. Recall $S_y = \{a \in \mathbb{Z} \mid a \equiv y \pmod m\}$, which by the way we decided to call $[y]$. What we know is that $x \in S_y$ and therefore $m \mid y - x$, which means that there exists an integer h such that

$$(1.1.1) \quad y - x = hm.$$

What we need to prove is that the two sets $S_x = S_y$, and we decided to prove that by showing first $S_x \subseteq S_y$ and then $S_y \subseteq S_x$. For $S_x \subseteq S_y$, pick an element $a \in S_x$ we need to show that $a \in S_y$. From the fact that $a \in S_x$ we have that there exists an integer h_1 such that $mh_1 = y - a$. Express y in terms of x and a , and substitute in 1.1.1 to obtain:

$$mh_1 + a - x = hm, \quad \text{and therefore} \quad a - x = (h - h_1)m,$$

which says that $a \equiv x \pmod m$. This says that $a \in S_x$. In the same way we proved that $S_y \subseteq S_x$. □

Really what we proved in the above theorem is the following property:

$$a \equiv b \pmod m \text{ and } b \equiv c \pmod m \text{ then } a \equiv c \pmod m \text{ (**Transitivity**)}$$

Instead of doing more proofs of the homeworks, we worked some examples:

a	b such that $b \equiv a \pmod 5$
0	-5, 5, 10, 15, 20, 25 ...
1	-4, 6, 11, 16, 21, 26, ...
2	-3, 7, 12, 17, 22, 27, ...
3	-2, 8, 13, 18, 23, 28, ...
4	-1, 9, 14, 19, 24, 29, ...
5	0, 5, 10, 15, 20, 25, ...

We noticed that $4 + 1 \equiv 0 \pmod 5$. What is $9 + 6$ modulo 5? and $19 + 16$ modulo 5?

Date: October 12, 2007.

(1.2) **Conjecture.** For every $x \in [4]$ and every $y \in [1]$, $x + y \equiv 0 \pmod{5}$.

You guys are really fast, and the proof came out really quickly:

Proof. (Conjecture 1.2) We know that there exists an integer h such that $5h = 4 - x$, and an integer k such that $5k = 1 - y$. Adding the two equations side to side we will have $5h + 5k = 4 + 1 - x - y$ and therefore $(x + y) - 0 = 5(1 - h - k)$, showing $x + y \equiv 0 \pmod{5}$. \square

What is the general conjecture?

(1.3) **Conjecture.** Let x, y, a, b , and m be integers. If $x \in [a]$ and $y \in [b]$ then $x + y \equiv a + b \pmod{m}$.

As an homework for next time, find a proof of the conjecture (if there is one).