Modular numbers

Integers can be divided by positive integers, if you allow remainders. You have to be a bit careful with the negative numbers. The key thing is that the quotient q and the remainder r satisfy the equations for $a \div b$:

$$a = bq + r \text{ and } 0 \le r < b$$

Notice that with this definition r is always positive

Examples

For $25 \div 6$:	For $-2 \div 6$:	For $-7 \div 6$:	For $-25 \div 6$:
$25 = 6 \cdot 4 + 1$	$-2 = 6 \cdot (-1) + 4$	$-7 = 6 \cdot (-2) + 5$	$-25 = 6 \cdot (-5) + 5$

There isn't a really common notation for the remainder of a division problem in math, so I'm going to use the one from Excel: in Excel, the remainder when dividing a by b is $\operatorname{mod}(a, b)$, so:

$\operatorname{mod}(25, 6) = 1$	$\operatorname{mod}(-2, 6) = 4$	$\operatorname{mod}(-7, 6) = 5$	$\operatorname{mod}(-25, 6) = 5$

Lets make a function:

One thing we can do is define a function: $f_6(n) = \operatorname{mod}(n, 6)$ Figure out and fill in the domain and range:

$$f_6 : \mathbb{Z} \to \{0,1,2,3,4,5\}$$

Is this function one-to-one?

No because $f_6(-7) = f_6(-25) = 5$

Is this function onto? $f_6(6) = 0$ $f_6(7) = 1$ $f_6(2) = 2$ $f_6(9) = 3$ $f_6(10) = 4$ $f(-7) = 5$

Onto

Look at pre-images:

There are lots of numbers in the pre-image of any of the possible remainders. These sets of numbers are going to be important, so we're going to name them. Finish these examples and definitions:

$[0]_6 = f_6^{\leftarrow}(0) = \{\ldots -12, -6, 0, 6, 12, \ldots\} = \{6n \mid n \in \mathbb{Z}\}$

$[1]_6 = f_6^{\leftarrow}(1) = \{\ldots -11, -5, 1, 7, 13, \ldots\} = \{1 + 6n \mid n \in \mathbb{Z}\}$

$[2]_6 = f_6^{\leftarrow}(2) = \{\ldots -10, -4, 2, 8, 14\} = \{2 + 6n \mid n \in \mathbb{Z}\}$

$[3]_6 =$

$[4]_6 =$

$[5]_6 = f_6^{\leftarrow}(5) = \{\ldots -7, -1, 5, 11, \ldots\} = \{5 + 6n \mid n \in \mathbb{Z}\}$

> The set whose elements are these sets is called $\mathbb{Z}_6$:
>
> $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\} \subseteq 2^{\mathbb{Z}}$

Why didn't I list $[6]_6$? $[6]_6 = [0]_6$

Do any of these sets overlap? No

Are there any integers that aren't in any of these sets?

If we did the same thing but with a function $f_5(n) = \operatorname{mod}(n, 5)$, how many pre-image sets would there be?

Notation: I'm going to call these sets ***congruence classes****, and say that two integers in the same set are* ***congruent****.*

Is this a function?:

$g:\mathbb{Z}_6\times\mathbb{Z}_6\to\mathbb{Z}_6$ such that $g([n]_6,[m]_6)=[a+b]_6$ where $a\in[n]_6$ and $b\in[m]_6$

The question is: is there only one output? There are lots of integers in each **congruence class** $[n]_6$: does it matter which one I pick when I'm doing $g([n]_6,[m]_6)=[a+b]_6$, or do I get the same answer for all of them?

Experiment time:

a. List 3 integers in $[4]_6$ $=[10]_6=[16]_6$ also $4\equiv 10\equiv 16 \pmod 6$

b. List 3 integers in $[5]_6$

c. Add up a bunch of pairs of numbers: one from list a and one from list b. What congruence class is each of the sums in?

Defining addition, subtraction and multiplication:

It turns out (algebra details coming next week) that adding, subtracting and multiplying numbers in equivalence classes always gives outputs in the same equivalence class (one output—it could be a function!) so it makes sense to say:

$[n]_6+[m]_6=[n+m]_6$

$[n]_6-[m]_6=[n-m]_6$

$[n]_6\cdot[m]_6=[n\cdot m]_6$

It's true that $[1]_6=[7]_6=[-5]_6$ are the same element of $\mathbb{Z}_6$, but we say that the first version (where it's represented by an integer between 1 and 5) is the ***simplified*** version.

We're going to be kind of lazy, and instead of writing $[4]_6+[5]_6=[9]_6=[3]_6$ we're almost always going to write $4+5\equiv 9\equiv 3 \pmod 6$

Compute and generalize:

1. $[2]_6+[5]_6=[1]_6$
2. $[4]_6\cdot[4]_6=[4]_6$
3. $[2]_6-[4]_6=[-2]_6=[-2+6]=[4]_6$

Compute mod 6:

4. $5\cdot 2\equiv$
5. $3+3\equiv$
6. $3-2\cdot 5\equiv$

7. $[2]_5+[4]_5=[6]_5=[1]_5$
8. $[6]_8+[5]_8=[3]_8$
9. $[5]_9\cdot[7]_9=[35]_9=[8]_9$

Compute mod 7:

10. $3\cdot 6\equiv$
11. $6+4\equiv$
12. $2-5\equiv$

More practice: section 3.1 pg 105 #1-31 odd