Modular Arithmetic
Instructor: Marizza Bailey
Name:

1. Introduction to Modular Arithmetic

If someone asks you what day it is 145 days from now, what would you answer?
Would you count 145 days, or find a quicker way?
Maybe, you would note that there are 7 days in a week, and, therefore, in seven days it would be the same day as today.
Then you would only have to find out how many groups of 7 fit into 145.
This could be easily done by dividing 7 into 145.
The answer, of course, would be 20, with 5 left over, or $145 = 7(20) + 5.$.
Then, it would only be necessary to count 5 days from today, and you would see that it would Saturday.

You may think this knowledge would only be useful to show off to friends, but you would be mistaken.
Programmers use this information to write calendar programs, and time programs, as well as others.

The mathematics that is involved in this problem is called modular arithmetic.
Instead of looking at a number as a value in and of itself, it is though of as a member of a *remainder class* relative to a number.
For Example, if we wanted to compute

$$12 \mod (5)$$

we would see that $12 = 5(2) + 2$, and therefore, 5 goes into 12 twice with remainder 2.
Hence,

$$12 \mod (5) = 2$$

.

See if you can compute the following:

(a) $17 \mod (3)$

(b) $39 \mod (4)$

(c) $137 \mod (6)$

(d) $234 \mod (10)$

(e) $365 \mod (7)$

(f) $73 \mod (52)$

(g) $256 \mod (12)$

Why were the last three problems significant? Could you think of word problems that might be associated to those computations?

Problem 1. How many years would it take for August 6 to be a Monday?

2. Modular Congruence

What does it mean that

$$7 \equiv 2 \mod (5)?$$

First of all, it means that the difference of 7 and 2 is a multiple of 5, i.e.,

$$7 - 2 = 5k$$

for some integer, k.
Is 7 actually equal to 2. What does equivalent mean?
An *equivalence relation* is a relation that is symmetric, reflexive and transitive. Symmetry means, since

$$7 \equiv 2 \mod (5)$$

then

$$2 \equiv 7 \mod (5).$$

Reflexive means that $2 \equiv 2 \mod (5)$ and transitive means that if $2 \equiv 7 \mod (5)$ and $17 \equiv 2 \mod (5)$ then $17 \equiv 7 \mod (5)$. The modulo 5 congruence class of 2 is

$$\{\cdots - 23, -18, -13, -8, -3, 2, 7, 12, 17, 22, 27, \dots\}$$

We call 2 the *residue* of this class modulo 5 and we call the congruence class, the *residue class.*

Lemma 1. *Let $a, b, n \in \mathbb{Z}$ be integers.*
The relation $a \equiv b$ if and only if $a \equiv b \mod (n)$ is an equivalence relation.

Proof 1. *We will prove that modulo is an equivalence relation by proving that it is symmetric, reflexive and transitive.*
symmetry
By definition, $a \equiv b \mod (n)$ implies that $a - b = nk$ for some integer k. Therefore, $b - a = -nk = n(-k)$ where $-k \in \mathbb{Z}$. Therefore, $b \equiv a \mod (n)$.
reflexive *Since $a - a = n(0)$ and 0 is an integer, then by definition, $a \equiv a \mod (n)$.*
transitive *Suppose $a \equiv b \mod (n)$ and $b \equiv c \mod (n)$, then by definition,*

$$a - b = nk_1 \qquad \textit{and} \qquad b - c = nk_2$$

Therefore, by adding both equations together, we get

$$a - b + b - c = nk_1 + nk_2$$

Simplification and factoring yields the desired result,

$$a - c = n(k_1 + k_2)$$

where $k_1 + k_2$ is an integer, and therefore $a \equiv c \mod (n)$.

3. Adding and Subtracting

Suppose you want to add two numbers modulo m. Would you be able to just add their residues? We'd like to believe that to be the case.
Let's look at an Example.

Example 1. Suppose you want to add 7 and 23 modulo 6.

$$7 + 23 = 30 \mod (6) = 0$$

and
$7 \mod (6) = 1$ and $23 \mod (6) = 5$, so $1 + 5 = 0 \mod (6)$.

Well, that was nice. I hope it happens like that all the time. Let's see.

Lemma 2. *Let $r_1 = a \mod (n)$ and $r_2 = b \mod (n)$,*
then $r_1 + r_2 \mod (n) = a + b \mod (n)$

Proof 2. *If* $r_1 = a \mod (n)$*, then* $r_1 - a = nk_1$*.*
Also, $r_2 = b \mod (n)$ *then* $r_2 - b = nk_2$
So if we add both equations together, we get

$$r_1 - a + r_2 - b = nk_1 + nk_2$$
$$(r_1 + r_2) - (a + b) = n(k_1 + k_2)$$

where k *is an integer. Therefore, by definition,* $(r_1+r_2) = (a+b) \mod (n)$

From this we can see that $-r = n - r \mod (n)$.

4. Exercises

Exercise 1. Add the following and simplify:

(a) $73 + 89 \mod (10)$

(b) $93 + 47 \mod (9)$

(c) $403 - 397 \mod (8)$

(d) $1214 + 1591 \mod (7)$

(e) $134 + 453 - 217 \mod (12)$

(f) $2372 + 971 - 1549 \mod (11)$

Exercise 2. Find the additive inverse of each number in the respective modulo class.

(a) $5 \mod (9)$

(b) $7 \mod (12)$

(c) $4 \mod (8)$

Exercise 3. Find the value(s) for x that make the equation true.

(a) $x + 6 = 2 \mod (7)$

(b) $x + 117 = 73 \mod (125)$

5. Multiplication

Lemma 3. *Let* $r_1 = a \mod (n)$ *and* $r_2 = b \mod (n)$*,*
then $r_1 r_2 \mod (n) = ab \mod (n)$

There is a large difference between multiplication in the integers and multiplication $mod(n)$.
You may not be able to divide by a number in $mod(n)$.
This is because division in any number set is multiplication by the multiplicative inverse.
Let me explain, if you see $2x = 5$, and I ask you how to "solve" the equation, you would "divide" both sides by 2.
Really, what you are doing is multiplying both sides by $\frac{1}{2}$ because $2\frac{1}{2} = 1$, which means that

$$\frac{1}{2}2x = \frac{1}{2}5$$
$$x = \frac{5}{2}$$

Therefore, to "divide" by a number, it has to have a multiplicative inverse.
What is the multiplicative inverse of $2mod(10)$?
Try it. I'll wait.

What? You didn't find one?
That's weird.

The reason for this is because $2(5) = 0mod(10)$ which means 2 is a zero divisor in $\mathbb{Z}_{10}$.
That's right! $xy = 0$ no longer implies that $x = 0$ or $y = 0$.
You can kiss all that you know and love about the real numbers goodbye.
In fact, all numbers which are not relatively prime to 10 will be zero divisors. For example, $2, 4, 5, 6, 8, 0$ are not relatively prime to 10, and are, therefore, are zero divisors.
Also, $1, 3, 7, 9$ are relatively prime, and so are multiplicative invertible.

6. Exercises

For each of the numbers below, find the multiplicative inverse in the indicated modulus.
If it does not have a multiplicative inverse, then find the factor which makes it a zero divisor.

(A) 5 modulo 24
(B) 4 modulo 7
(C) 3 modulo 9
(D) 2 modulo 6
(E) 6 modulo 14