Intermediate Math Circles
Wednesday November 16 2016
Modular Arithmetic I

Welcome to Math Circles! In this two-part lecture series we will investigate a very computationally useful mathematical tool. Namely, we will explore the concept of modular arithmetic. We will apply our modular arithmetic knowledge to:

- Time calculation problems
- Calendar problems
- Divisibility problems
- Digit calculations
- Fermat's Little Theorem and
- Security problems

1 Basic Number Theory

Recall that the set of integers is denoted by $\mathbb{Z}$ and is defined to be the collection of numbers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

The set of integers has many interesting properties. Notably:

- We can add two integers together and still get an integer!
- We can subtract two integers together and still get an integer!
- We can multiply two integers and still get an integer!
- We can divide two integers and . . . !

This leads us to the definition of divisibility.

Definition 1. *Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say a divides b, written $a \mid b$, if $\frac{b}{a} \in \mathbb{Z}$. If a does NOT divide b we write $a \nmid b$.*

If $a|b$ then we say that a divides b. We also say that b is divisible by a.

Example 1. $2|4$, $3|-18$, $-5|5$, $2 \nmid -3$, $-2 \nmid 51$

Exercise 1.1. *Fill in the blanks.*

1. *If a is a nonzero integer such that a divides every integer then $a =$*_____.
2. *True/False. Zero is divisible by every nonzero integer.* _____
3. *The integers which are divisible by 2 are precisely the* _____*numbers?*

4. *Every integer is divisible by at least* _____ *nonzero integers.*

For any a and b in $\mathbb{Z}$ with $b \neq 0$ there exists $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$ with $0 \leq r < b$ such that

$$a = bq + r.$$

Here, q is called the quotient when a is divided by b and r is the remainder when a is divided by b. Note that b divides a exactly when the remainder when a is divided by b is 0. In fact, q and r are unique (i.e. the only numbers which satisfy this property).

Example 2. *If* $a = 15$ *and* $b = 4$ *then* $15 = a = 3(4) + 3 = 3b + 3$. *Therefore* $q = 3$ *and* $r = 3$.

Example 3. *If* $a = -8$ *and* $b = 3$ *then* $-8 = a = 3(-3) + 1$. *Therefore* $q = -3$ *and* $r = 1$.

Exercise 1.2. *Find the quotient and remainder when* -34 *is divided by* -5. *(i.e.* $a = -34$ *and* $b = -5$*)*

Exercise 1.3. *Find the quotient and remainder when* 4 *is divided by* 99.

Now it is time for our main definition which will allow us to start all the fun stuff!

Definition 2. *Let m be a positive integer. Let a and b be integers. We say that a and b are congruent modulo m, written $a \equiv b \pmod{m}$, if a and b have the same remainder when divided by m.*

So what does it really mean to say $a \equiv b \pmod{m}$? Well, it means that

$$a = mq_1 + r,$$

for some $q_1 \in \mathbb{Z}$ and integer r such that $0 \leq r < m$. Moreover,

$$b = mq_2 + r,$$

for some $q_1 \in \mathbb{Z}$. Note that the q_i's may be different but the r's are the same!!! Basically, a and b are congruent modulo m if they "look the same up to a multiple of m"!

Properties. *Let m be a positive integer and let $a, b, a', b', c \in \mathbb{Z}$. Then*

1. *If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then $a + b \equiv a' + b' \pmod{m}$ and $ab \equiv a'b' \pmod{m}$.*
2. *If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.*
3. *if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.*
4. *$a \equiv a \pmod{m}$ for every $a \in \mathbb{Z}$.*
5. *$a \equiv 0 \pmod{m}$ exactly when m divides a.*
6. *If $a \equiv r \pmod{m}$ with $0 \leq r < m$ then r is actually the remainder when a is divided by m.*

Example 4. *Find an integer $0 \leq r < 5$ such that $117 \equiv r \pmod{5}$. Well, observe that*

$$\begin{aligned} 117 &\equiv 115 + 2 \pmod{5} \\ &\equiv 0 + 2 \pmod{5} \\ &\equiv 2 \pmod{5} \end{aligned}$$

Therefore $r = 2$.

Note that in the above we actually found the REMAINDER when 117 is divided by 5.

Example 5. *Find the remainder when 3^{129} is divided by 8. Observe that*

$$\begin{aligned} 3^{129} &\equiv 3(3^{128}) \pmod{8} \\ &\equiv 3(9^{64}) \pmod{8} \\ &\equiv 3(1^{64}) \pmod{8} \\ &\equiv 3 \pmod{8}. \end{aligned}$$

Therefore the remainder is 3.

Exercise 1.4. *Find the remainder when* 2^{601} *is divided by* 5.