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
- Fivisibility problems
- Figit 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 $a = 1$ or $a = -1$.*
2. *True/False. Zero is divisible by every nonzero integer. TRUE.*
3. *The integers which are divisible by 2 are precisely the even numbers!*

4. *Every integer is divisible by at least 2 nonzero integers. Namely, if a is a nonzero integer then a is divisible by 1 and -1.*

For any a and b in $\mathbb{Z}$ with $b > 0$ 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 $b = 5$)*

Begin by noting that

$$-34 = (5)(-7) + 1.$$

Therefore $q = 7$ and $r = 1$.

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

This may seem tricky because $99 > 4$. However, sticking to our definitions of quotient and remainder we see that

$$4 = (99)(0) + 4,$$

so that $q = 0$ and $r = 4$.

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.

In this problem, the trick is to notice that $2^{601} = 2(4^{300})$ and that $4 \equiv -1 \pmod 5$. With that being said we see that

$$\begin{aligned} 2^{601} &\equiv 2(4^{300}) \pmod 5 \\ &\equiv 2((-1)^{300}) \pmod 5 \\ &\equiv 2 \pmod 5. \end{aligned}$$

Therefore the remainder is $r = 2$.

2 Applications

Exercise 2.1. *Today is a Wednesday! In 240 days, what day of the week will it be?*

Since the day of the week is the same every seven days, we work modulo 7. Observe that

$$\begin{aligned} 240 &\equiv 210 + 30 \pmod 7 \\ &\equiv 0 + 30 \pmod 7 \\ &\equiv 30 \pmod 7 \\ &\equiv 28 + 2 \pmod 7 \\ &\equiv 2 \pmod 7. \end{aligned}$$

Therefore in 240 days it will be a "Wednesday plus 2", which we normally call a Friday!

Exercise 2.2. *It's November! In 24 145 months, what month will it be? What year will it be?*

As there are 12 months in a year, we work modulo 12. Observe that

$$\begin{aligned} 24145 &\equiv 24000 + 145 \pmod{12} \\ &\equiv 0 + 145 \pmod{12} \\ &\equiv 145 \pmod{12} \\ &\equiv 144 + 1 \pmod{12} \\ &\equiv 1 \pmod{12}. \end{aligned}$$

Therefore it will be December. Now, as $r = 1$ we see that $24145 = (12)q+1$. A simple calculation shows that $q = 2012$. Therefore the year will be $2016 + 2012 = 4028$.

Exercise 2.3. *Today is November 16, 2016. We already know it is a Wednesday! What day of the week will November 16, 2017 be on?*

Observe that

$$\begin{aligned} 365 &\equiv 350 + 15 \pmod 7 \\ &\equiv 0 + 15 \pmod 7 \\ &\equiv 15 \pmod 7 \\ &\equiv 14 + 1 \pmod 7 \\ &\equiv 1 \pmod 7. \end{aligned}$$

Therefore it will be a Thursday!

Exercise 2.4. *What day of the week was it on November 16, 2015?*

Now, we need to remember that this year was a leap year! Therefore November 16, 2015 was 366 days ago! With that being said,

$$\begin{aligned} -366 &\equiv -365 - 1 \pmod 7 \\ &\equiv -1 - 1 \pmod 7 \\ &\equiv -2 \pmod 7 \\ &\equiv 5 \pmod 7, \end{aligned}$$

and so it was a Monday!

Exercise 2.5. *Suppose it is currently 7:01 PM. What time will it be in 269 hours?*

Working modulo 24 we see that

$$\begin{aligned} 269 &\equiv 240 + 29 \pmod{24} \\ &\equiv 0 + 29 \pmod{24} \\ &\equiv 29 \pmod{24} \\ &\equiv 5 \pmod{24}, \end{aligned}$$

Therefore it will be 12:01 AM.

Exercise 2.6. *What is the ones digit of* $9 \times 9 \times 9 \times 9 \times 9 \times 9 \times 9 \times 12$*?*

Notice that to capture the ones digit (i.e. the last digit) of a number, we need only know what the remainder is when the number is divided by 10. Working modulo 10 we see that

$$\begin{aligned} 9^7 \times 12 &\equiv (-1)^7 \times 2 \pmod{10} \\ &\equiv -2 \pmod{10} \\ &\equiv 8 \pmod{10}. \end{aligned}$$

Therefore the ones digit is 8.

Exercise 2.7. *Show that for any positive integer n, $2^n 3^{2n} - 1$ is always divisible by 17.*

Notice that for any n,

$$\begin{aligned} 2^n 3^{2n} - 1 &\equiv 2^n 9^n - 1 \pmod{17} \\ &\equiv 18^n - 1 \pmod{17} \\ &\equiv 1^n - 1 \pmod{17} \\ &\equiv 0 \pmod{17}, \end{aligned}$$

Therefore 17 divides $2^n 3^{2n} - 1$.

Exercise 2.8. *TRUE or FALSE. Throughout let a, b and c be positive integers.*

1. *If $a|(bc)$ then $a|b$ or $a|c$.*
   F

2. *If $a|b$ and $b|a$ then $a = b$ or $a = -b$.*
   T

3. *If $a \equiv 4 \pmod{14}$ then $a \equiv 4 \pmod{7}$.*
   T

4. *The ones digit of $11^{1000000}$ is 1.*
   T

5. *52 cards can be dealt evenly to 3 players?*
   F