What is Number Theory About?
Pre-class activity, Week 1

Number theory studies the properties of natural numbers, or more generally integers. In the first class, we will see a brief introduction to a few of the different topics that we will focus on in this course. This pre-class activity is designed to help you refresh some of the background material related to these topics that you would have seen in a proofs course, or Discrete Math, or Modern Algebra course.

Divisibility and Primes

We officially say that a non-zero integer a **divides** an integer b if $b = ak$ for some integer k. For example, 3 divides 6 and 15, while 3 does not divide 11 or 20. If a divides b, we also say that a is a **divisor** (or factor) of b, and that b is a **multiple** of a. The notation for a divides b is $a|b$ (which might be a bit confusing especially compared with the notation of a fraction, so please be careful with this notation; one trick I use it to read the whole $a|b$ in words in your head as a divides b, replacing the | with divides, and to think of "divides" as "goes into").

1. Find all positive divisors of 30.

1, 2, 3, 5, 6, 10, 15, 30

The reason why we officially define such obvious words is these definitions give us something to work with when we define more complicated words, or when we try to explain why something always works, or when we try to decide whether a specific case is an example which the word applies to. Here are two examples.

2. Suppose $a \neq 0$ is an (unknown) integer. Does $a|0$? Does $a|a$? Does $0|a$? Does $1|a$? Justify each briefly.

yes yes no yes

3. Does 0 divide 0?

yes

A **prime number** is a non-zero natural number that has no natural number divisors besides 1 and itself. A non-prime (natural) number greater than 1 is called a **composite** number.

4. For each of the following numbers, determine whether they are prime or not. Justify briefly.

a. 23 **b.** 91 **c.** 101

yes No yes

$13 \cdot 7 = 91$

We will see later (if time allows) different methods for testing whether a number is prime or not. This is an important problem due to the use of large prime numbers in certain encryption methods.

Recursively defined sequences

Recursively defined sequences play an important role in number theory. One such famous sequence is the Fibonacci numbers. Here's how we create the Fibonacci numbers recursively: The first two numbers are both 1. We denote these by $f_0 = 0$ and $f_1 = 1$. To get the next number we add the two last numbers we have: $f_2 = 0 + 1 = 1$. Continuing this way, we can get an infinite sequence of numbers.

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

1. Find the first 16 Fibonacci numbers (i.e. up to f_{15}).

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610

2. Find the values of the sums of the first 2, 3, 4, 5, 6, 7, 8, Fibonacci numbers. In other words, find $f_0 + f_1$, $f_0 + f_1 + f_2$, $f_0 + f_1 + f_2 + f_3$, etc. (Note: You shouldn't need to add all the way from the start every time.) Do you notice something special about these numbers? Do they look like something else?

1, 2, 4, 7, 12, 20, 33

$$\sum_{i=0}^{n} f_n = f_{n+2} - 1$$

Congruences

Congruences are an equivalent way of thinking about remainders in long division. We officially define it as follows: Given a non-zero natural number n, if $n|(a-b)$ (i.e. n divides $a-b$), then we say that a is *congruent* to b modulo n and write $a \equiv b \pmod{n}$. For example, $7 \equiv 2 \pmod{5}$ because $5|(7-2)$ (i.e. 5 divides $7-2=5$). Similarly, $1 \equiv 13 \pmod{3}$ because $3|(1-13)$. But $2 \equiv 4 \pmod{3}$ because $3 \not| (2-4)$ (i.e. 3 does not divide $2-4$).

1. Determine whether the following congruences are true:

a. $23 \equiv 2 \pmod{7}$ yes

b. $2 \equiv 23 \pmod{7}$ yes

c. $2 \equiv -2 \pmod{5}$ no

d. $-1 \equiv 9 \pmod{5}$ yes

e. $-3 \equiv -8 \pmod{5}$ yes

2. Find three-four valid congruences of your own.

$5 \equiv 14 \pmod{3}$ $16 \equiv 0 \pmod{4}$ $3 \equiv -3 \pmod{6}$

3. Congruences modulo 3:

a. Determine which of the following numbers are congruent modulo 3: $0, 1, 2, 3, 4, 5, 7, 9, 12, 20, 21, 22, 100, -1, -2, -3, -4, -5$.

0, 3, 9, 12 | 1, 7, 7, 22 | 2, 5, 20
21, -3 | 100, -2, -5 | -1, -4

b. Given a number n, we can partition all the integers into groups where the integers in the same group are congruent to each other. This follows from the reflexive, symmetry and transitivity properties of congruence. For example, for $n=3$, the numbers $0, -3, 24, 15$ are all in the same group. These groups are officially called the *residue classes* modulo n.

How many residue classes are there modulo 3? If you were to choose representatives from each group (residue class), what would be a good choice of representatives?

3 residue classes

0, 1, 2 work nicely as representatives