INTRODUCTION TO CONCEPTS OF NUMBER THEORY

In order to understand the basic number theoretic functions, we first must be familiar with large summations. To this end, it will be very useful to be comfortable using "Sigma" notation, written as $\sum$.

When you see a sigma, you should immediately think, "to sum", but you might ask, from what to what? This is what our indices are for and they are placed on the bottom and top of the sigma. Observe,

Example 1

$$\sum_{n=1}^{4} n = 1 + 2 + 3 + 4 = 10$$

We are simply plugging in the first value for n, inserting a plus sign, incrementing n by 1, and repeating until the last value of n plugged in is the upper limit (i.e. the number at the top of the sigma).

Heres one more example:

Example 2

$$\sum_{n=1}^{4} n^2 = 1 + 4 + 9 + 16 = 30$$

Now, we can also change up the notation a little bit if the numbers involved in our sum are not as easy to explain. The restriction we put on the numbers in the sum is often written underneath the sigma. Heres a few examples:

Example 3/4

$$\sum_{5 \leq n \leq 10} n = 5 + 6 + 7 + 8 + 9 + 10 = 45$$

Or we can get even more complicated:

$$\sum_{\substack{n \leq 25 \\ n \equiv 3 \pmod 7}} n = 3 + 10 + 17 + 24 = 54$$

Verify that this makes sense to you.
Now that we are familiar with summation notation lets do some exercises.

1)

$$\sum_{n=0}^{4}(2n+1) =$$

2)

$$\sum_{n=0}^{5}(2n+1) =$$

3)

$$\sum_{n=0}^{6}(2n+1) =$$

Can you make a conjecture about the sum of the first n odd numbers?

4)

$$\sum_{k=1}^{4} k^3 =$$

5) Write the following in summation notation:

$1 + 4 + 9 + \cdots 81$

6)

$$\sum_{n=1}^{5}(n^2 - 2^n) =$$

7)

$$\sum_{d=\text{divisors of } 6} d$$

Now that we are familiar with summations, let's jump into the number theory! In order to do so, let's refresh on simple numerical notation.

Definition 1: The greatest common divisor of two positive integers a and b, written $gcd(a, b)$, is the largest positive integer, d, such that d divides both a and b. Recall that if d divides a we write $d|a$.

Definition 2: Two numbers are relatively prime if they share no common factors. If a and b are relatievely prime, we write $a \perp b$.

If $a \perp b$, then $gcd(a, b) = 1$.

Definition 3: If $a \equiv b \pmod{m}$, this means:

1) m divided by a has a remainder of b.

2) There exists an integer k such that $a = b + mk$, or $a - b = mk$
Make sure you understand both of these definitions, plugging in values for a, b, and m will be helpful.

In order to be number theorists, we must recall, and eventually master, modular arithmetic. Below are some exercises on this new notation, as well as warm-up/challenge exercises on modular arithmetic, which we used a lot in our study of groups. Any time you see the letter p, it is implied that it is a prime.

1) True or False:

$$gcd(986, 100023746532) = 1, \qquad p \perp 123, 456, 789, \qquad 1,000,000,000,007 \equiv 7 \pmod{10}$$

2) List the following set of objects:

All positive integers, d, such that $d|30$.

3. Compute the following:

a) $1492 \equiv$ _____ (mod 4)

b) $1492 \equiv$ _____ (mod 10)

c) $1492 \equiv$ _____ (mod 101)

d)$3^{302} \equiv$ _____ (mod 28)

Challenge Problems (only attempt if you're interested)

4) What is the last digit of 7^{355}?

5) Find the smallest positive integer, n, such that

$$n \equiv 0 \pmod{4}, \quad n+1 \equiv 0 \pmod{9}, \quad \text{and} \quad n+2 \equiv 0 \pmod{25}$$

Hint: use the formula for modular arithmetic in definition 3 part b).

6) Can you find a multiple of 7 that leaves a remainder of 1 when divided by $2, 3, 4, 5,$ and 6?

Now lets introduce some number theoretic functions, also known as arithmetic functions. You do not need to rigorously understand them as this will be the focus of our attention for the first few weeks. You may want to try and understand what the functions do based on their summation notation.

$\tau(n)$, pronounced "tau"

$$\tau(n) = \sum_{d|n} 1$$

$\sigma(n)$, pronounced "sigma"(lowercase)

$$\sigma(n) = \sum_{d|n} d$$

$\phi(n)$, pronounced "phi"

$\phi(n)$ is the number of positive integers relatively prime to n. We could also write it as

$$\phi(n) = \sum_{\substack{d \leq n \\ gcd(d,n)=1}} 1$$

$\mu(n)$, pronounced "mew" but more formally known as the möebius function

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if n contains a power of a prime} \\ (-1)^t & \text{if } n = p_1 p_2 p_3 \dots p_t \end{cases}$$

YES, you are correct. The möebius functions is incredibly strange, and as you will find out, it is surprisingly powerful. In order to understand it better, let's quickly wrap up with finding a numbers' prime factorization.

The algorithm goes as follows:

Start with a given integer, n, and divide it by the smallest prime, 2. If it is not divisible by 2, try and divide it by the next smallest prime, 3, continue this process until you find a prime that divides n. Once you find a prime that divides n, remember that prime, call it p, and add it to the prime factorization of n. Then compute $\frac{n}{p}$, which will be an integer and start the algorithm back at 2 again, but this time with your new integer, $\frac{n}{p}$. Once you find the last prime, p' such that $\frac{n}{p'}$ is itself prime, you are done.

Example 1
Find the prime factorization of 60.

$$\frac{60}{2} = 30, \quad \frac{30}{2} = 15, \quad \frac{15}{3} = 5, \quad \text{which is prime!}$$

Thus the prime factorization of 60 is

$$60 = 2^2 \cdot 3 \cdot 5$$

Try it for yourself.

Find the prime factorizations of 2345 and 45670.