In a nutshell, there are two goals in this course: have fun with what we can do with elementary number theory, and explain what we cannot do. For those we can do, we will introduce a sequence of tools in elementary number theory, and combine them with problem solving skills to tackle various kinds of questions in number theory, mostly equations about integers. Nevertheless, sometime since the middle of the course, we will begin to see the limitation of our methods, we then hope to explain how these limitations are resolved by mathematics in the late nineteenth century and early twentieth, or more precisely in Math 120, Math 121 and Math 116.

This course will begin with the topic of modular arithmetic. Write $n \mid m$ if $n$ divides $m$, i.e. if $m$ is an integral multiple of $n$. We say two integers $a$ and $b$ are congruent modulo $n$ if they have the same residue when divided by $n$. More precisely, this is

**Definition 0.1.** We say $a \equiv b \pmod{n}$, or $a$ is congruent to $b$ modulo $n$, if $n \mid a - b$. We will sometimes also further abbreviate it as $a \equiv b(n)$.

The arithmetic regarding such “mod-something” scenario is called modular arithmetic. As an example, the clocks we use for daily life is a mod 12 system; if a clock is at 9, then it will point to 1 after four hours; $9 + 4 \equiv 1 \pmod{12}$.

We have a simple fun example about mod 7. We have

\[
\begin{align*}
1/7 &= 0.142857142857... \\
2/7 &= 0.285714285714... \\
3/7 &= 0.428571428571... \\
4/7 &= 0.571428571428... \\
5/7 &= 0.714285714285... \\
6/7 &= 0.857142857142...
\end{align*}
\]

How does this happen? Well, note that $10 \equiv 3 \pmod{7}$, $100 \equiv 2 \pmod{7}$, $1000 \equiv 6 \pmod{7}$, $10000 \equiv 4 \pmod{7}$, $100000 \equiv 5 \pmod{7}$ and lastly $1000000 = 10^6 \equiv 1 \pmod{7}$. Thus $7 \mid 10^6 - 1$ and in fact $999999 = 10^6 - 1 = 7 \times 142857$. Beginning with

\[7/7 = 1 = 0.999999 999999 999999 \ldots\]

and divides both sides by 7 gives the first formula. If we multiply both sides by 10, we get

\[10/7 = 1.42857142857\ldots\]

But $10 \equiv 3 \pmod{7}$ gives $10/7 = 1 + 3/7$. Taking the fractional parts of the last equation gives the above formula for $3/7$. All others can be obtained in a similar manner.
We have seen at the core of the above phenomenon is the formula $10^6 \equiv 1 \pmod{7}$. How will this generalize? We will see that if $p$ is a prime number, like 7 is, and $a$ is not divisible by $p$, then we always have $a^{p-1} \equiv 1 \pmod{p}$. This is called the Fermat’s little theorem. This theorem, as well as its generalization and application, will occupy our second to fourth weeks. As an example, note that this provides a way to detect whether a number is a prime number! To be precise, if we can find an $0 < a < p$ such that $a^{p-1} \not\equiv 1 \pmod{p}$, then $p$ is NOT a prime number.

Once we establish some tools in modular arithmetic, we will turn to a series of some oldest problems in mathematics: Diophantine equations, a.k.a. equations of integers. As an example, let us look at the following equation:

$$x^2 + y^2 = n$$

and the question is for which $n$ can find integral solutions $(x, y)$. It will turn out that the case when $n$ is a prime number is an essential case, and we have

**Theorem 0.2.** When $p$ is a prime number, the equation $x^2 + y^2 = p$ has an integral solution if and only if $p = 2$ or $p = 4k+1$, i.e. $p \equiv 1 \pmod{4}$. In general $x^2 + y^2 = n$ has a solution if and only if $n$ is a product of prime numbers of the above forms.

To establish theorem like this, we need a careful study in the mod-$p$ arithmetic, as well as invoking some baby version of the tool of rings in Math 120 (we will go over this, and in fact hope this promotes interests in the topics of Math 120).

After results as in Theorem 0.2, it will then be natural to ask the following questions: How many prime numbers are there, and how many of them are of the form $4k+1$? This will be the third topic of this course, that of analytic number theory. We will give heuristic and prove special cases of the following two results:

**Theorem 0.3.** (Prime Number Theorem) Among $1$ to $n$, roughly $\frac{1}{\log n}$ of the numbers are prime numbers. In precise terms, this says

$$\lim_{n \to +\infty} \frac{\# \{1 \leq p \leq n \mid p \text{ is a prime number} \} \cdot \log n}{n} = 1.$$  

**Theorem 0.4.** (Dirichlet Theorem) Among $1$ to $n$, the number of prime numbers of the form $4k+1$ and the number of those of the form $4k+3$ are roughly equal. That is

$$\lim_{n \to +\infty} \frac{\# \{1 \leq p \leq n \mid p \text{ is a prime number of the form } 4k+1 \}}{\# \{1 \leq p \leq n \mid p \text{ is a prime number of the form } 4k+3 \}} = 1.$$  

Natural proofs of these theorem will require the tool of Complex Analysis (Math 116). We will definitely not go that far, but will Math 155?