The following is a description of the contents of the Introductory Number Theory course. It should be understood that this summary is not cast in stone; depending on time constraints and student interest, some other topics may be covered, while perhaps the one or other topic listed here might be dropped.

We will start with introducing congruences and investigating modular arithmetic: the set $\mathbb{Z}/n\mathbb{Z}$ of “integers modulo $n$” forms a ring. This ring is a field if and only if $n$ is a prime number. A study of the multiplicative structure leads to Fermat’s Little Theorem (for prime $n$) and to the Euler phi function and Euler’s generalization of Fermat’s Theorem. Another basic tool is the Chinese Remainder Theorem.

Building on this basis, we will have a look at modern cryptographic systems. Then we will get back to more classical number theory and deal with quadratic residues and the famous quadratic reciprocity law that was discovered and proved (several times!) by Gauss.

This leads naturally to the study of solutions to equations like

$$ax^2 + by^2 = cz^2$$

or, in more geometric terms, rational points on conics. We will see that the question whether such an equation has a nontrivial solution ($X, Y, Z$ not all zero) in integers is decidable, and a solution can be found reasonably fast. For the proof, we will learn about Minkowski’s Lattice Point Theorem.

We will look at quadratic forms in two variables (like $X^2 + 2Y^2$), for example investigating which integers can be represented by such a form. This is related to “quadratic number rings” like the Gaussian integers $\mathbb{Z}[i]$ (consisting of all complex numbers whose real and imaginary parts are integers). A special case is the (wrongly) so-called Pell Equation $X^2 - dY^2 = \pm 1$ (or $\pm 4$), whose theory is related to another classical topic: continued fractions.

I hope to be able to also cover results about representations of integers as sums of three or four squares.

We will also discuss the basic theory of Elliptic Curves over the rational numbers. They are given by equations of the form

$$y^2 = x^3 + Ax + B$$

with rational numbers $A$ and $B$ (such that $4A^3 + 27B^2 \neq 0$). Their solutions in rational numbers have a natural abelian group structure. If there is enough time, we will give a proof of the Mordell-Weil Theorem in a special case; it says that this group is finitely generated.

In the last part of the course, we will discuss some results on the distribution of prime numbers, namely the Prime Number Theorem, which tells us about how many prime numbers there are up to a given $x > 0$, and Dirichlet’s theorem on primes in arithmetic progressions, which states that an arithmetic progression

$$a, a + d, a + 2d, a + 3d, \ldots$$

contains infinitely many primes unless this is obviously impossible (because $a$ and $d$ have a common divisor). We will not be able to prove these results fully, but I hope I will get across the main ideas behind the proofs.