Brief Final Project Descriptions for Undergraduate "Introduction to Number Theory" Course at Duke University

Written by Jonathan Hanke

Here are some suggestions for final projects, grouped according to topic. Each project describes a major theorem or idea in number theory, which is a little beyond what we will cover in the lectures. Hopefully you'll find one that is really interesting to you, and have lots of fun learning about it. If you have a different favorite project you'd like to explore, feel free to let me know and we can try to work something out (though I may not be able to find good references for you).

The numbers in boldface at the end are a rough estimate of how involved the project can be on a scale of 1 through 5. Projects starting with a 4 are challenging, but each project is what you make of it. A few require knowledge of other areas of mathematics, so if you choose this, be sure that you're comfortable with the language and tools of that area.

The project consists of a presentation, and a clearly written paper on your topic (which should probably be no less than 10-12 pages) proving the main results, giving a context, and carefully working out a few examples.

Primes in arithmetic progressions – In class we will show that there are infinitely many prime numbers, and infinitely many of the form $4k+1$ and $4k+3$. By a remarkable analytic method, Dirichlet showed that there are infinitely many primes of the form $ak+b$ so long as the integers a and b are relatively prime. Your paper should explain his idea and proof, and work out a few specific examples of this remarkable theorem in detail. **[3.5-4.5]**

The prime number theorem – In class we will show that there are infinitely many prime numbers, but we won't say anything about how they are distributed among the natural numbers. For example, we might want to know if most numbers are prime, or how often we expect a randomly chosen a number to be prime? One of the main results along these lines is the *prime number theorem*, which gives a good idea about how the primes are distributed. Let's say we look at all of the (natural) numbers less than some fixed number x. Then the prime number theorem says about how many of these numbers we expect to be prime (in terms of x). This proof of result uses analytic techniques, and is closely related to the behavior of the Riemann zeta function $\zeta(s)$. Your paper should explain the prime number theorem and how it is proved, its connection to the zeros of $\zeta(s)$, and possibly what we can say about how primes of the form $4k+1$ and $4k+3$ are distributed. **[4-5] (Requires complex analysis.)**

Class numbers and binary quadratic forms – In class, one of our main goals has been to study primes, and to prove unique prime factorization for $\mathbb{Z}$. However not all number systems we enounter will be as simple, and it may happen that unique prime factorization fails. The *class number* $h \in \mathbb{N}$ is a number which tells us how far we are from having unique prime factorization (with $h = 1$ meaning that unique factorization holds), and so it is important to be able to compute h, and decide when $h = 1$. This question was first addressed by Gauss, who computed these class numbers by studying quadratic forms $ax^2 + 2bxy + cy^2$ for some $a, b, c \in \mathbb{Z}$. Your project should describe this connection, and use it to compute the class number of the integers in any quadratic number field $\mathbb{Q}(\sqrt{D})$, and perhaps for other number systems in $\mathbb{Q}(\sqrt{D})$. **[3-4]**

Pell's equation and the continued fraction of $\sqrt{D}$ – One of the simplest and oldest quadratic equations in number theory are the (slightly misnamed) Pell equations $x^2 - Dy^2 = \pm 1$ for some $D \in \mathbb{Z} > 0$. These solutions (x, y) have close connections to the quadratic number field $\mathbb{Q}(\sqrt{D})$, but are much harder to understand than their positive counterparts $x^2 + Dy^2 = 1$. Some information about them can be found be studying the continued fraction expansion of $\sqrt{D}$, though there is still much left to know. Your project should describe this connection, and use it to understand the solutions of these equations, and what they can tell us about their associated quadratic number fields. **[3-4]**

Dirichlet's class number formula – Because of it's connection to unique prime factorization (described above), it is important to be able to compute the class number h of a number system. By a remarkable analytic method, Dirichlet was able to give an explicit formula for the class number in certain cases using a variant of the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Your project should describe how this is done, and describe how one can use the to compute the class number of the integers in any quadratic number field $\mathbb{Q}(\sqrt{D})$, and perhaps for other number systems in $\mathbb{Q}(\sqrt{D})$. **[3-4]**

Geometry and Sums of 4 squares (Minkowski's theorem) – One of the most amazing insights into the "geometry" of numbers was offered by a brilliant young mathematician named Hermann Minkowski, who showed that the distribution of lattice points in a symmetric region is related to the area/volume of the region. This theorem is quite easy to state and prove, but has many surprising applications in number theory. One of these is to show that every natural number is a sum of 4 squares. Your project should explain the theorem, and show how it can be used to answer some questions related to which numbers are sums of squares. **[2.5-4]**

Arithmetic and Sums of 4 squares (Quaternion algebras) – In class we will see that the question of which numbers have the form $x^2 + y^2$ has deep connections to certain other number systems. A similar connection exists for the question of which numbers can be written a sum of 4 squares, and it related to a non-commutative number system known as a *quaternion algebra*. The simplest example of this is the quaternions, discovered by Hamiliton in the 1800's, is numbers of the form $a+bi+cj+dk$ where $a, b, c, d \in \mathbb{Z}$, and $i^2 = j^2 = k^2 = -1$. Your project should describe this connection, and use it to answer questions related to which numbers can be written as sums of 4 squares. **[4-5]**

Algebra and Sums of 4 squares (Local-global principle and Class numbers) – In class we describe which numbers can be represented in the form $x^2 + y^2$ or $x^2 + 2y^2$ by using certain other number systems to study them. It happens that in many cases there is no clear connection to a number system, so we must find a different approach. One idea is that we can check whether a number is represented in $\mathbb{Z}/m\mathbb{Z}$ for all numbers m, and if it is, we can conclude something about whether the number is represented. In general, we can't answer our original question without considering a few other related quadratic forms, but in some cases we can. Your project should explain how this works in general, and use it in some examples to find all numbers which are represented by certain quadratic forms. In particular, you can use this to prove that every positive integer is a sum of 4 integer squares. **[3-4]**

Analysis and Sums of 4 squares (Siegel's theorem) – It is a classical fact that every positive integer is a sum of 4 squares, and there are a variety of proofs explaining why. Above, we describe how one can use modular arithmetic and a certain kind of local-global principle to show this. However, it is possible to use a similar idea to also answer the deeper question of *how many ways* can we write any number as a sum of 4 squares? To do this, we need to keep track of the number of ways this can be done mod p for all primes p, and do a little extra work at the prime 2. These local computations mod p are computed using a very interesting sum called a *Gauss sum* and yield very simple formulas for the number of solutions mod p. Then, by multiplying these factors from each prime together, we can find an exact formula for the number of ways of writing any positive integer as a sum of 4 squares. Your project should carry this through, and perhaps find an exact formula for the number of representations of another interesting quadratic form. **[4-5]**

Local-global principle for rational points on conics and p-adic numbers – One approach to finding Pythagorean triples is to use them to make rational points (i.e., points (x, y) where both coordinates are rational numbers) on the unit circle by dividing the triple (x, y, z) by z. One then has to describe all of the rational points on the unit circle. It turns out that there is a general strategy for doing this which comes in 2 parts: First find one rational point, then use it to find all of the others. Your project should describe this procedure, and use it to find all Pythagoran triples and do a few other examples of finding all "generalized" Pythagorean triples in certain interesting cases (say, for example, all integer solutions of the form $x^2 + y^2 = 2z^2$ or $x^2 + y^2 = 3z^2$). It should also describe the "local-global" principle that allows you to

check for the existence of a rational point on a quadratic curve by looking for solutions over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all primes p, and possibly explain how this fails for cubics. **[3-4.5]**

Algebra and analysis in the p-adic numbers – A feeling one gets when studying number theory is that prime numbers figure prominently in the answers to most questions, and in particular it is important to understand what is going on in $\mathbb{Z}_{p^n}$ for all $n \in \mathbb{N}$. There is a beautiful construction which allows one to actually make a complete space (meaning that all Cauchy sequesces converge) containing $\mathbb{Q}$ associated to every prime $p \in \mathbb{N}$ known as the p-adic numbers. These p-adic spaces $\mathbb{Q}_p$ should be thought of as equally important as the more familiar real numbers $\mathbb{R}$, and it is interesting to see how the "analysis" on $\mathbb{Q}_p$ is related to the algebra on $\mathbb{Q}$ and $\mathbb{Z}$. Your project should explore this connection by defining $\mathbb{Q}_p$, describing its connection to $\mathbb{Q}$ and $\mathbb{Z}$, and exploring analogues of "standard" functions like $n!$, e^x, $\ln(x)$, and possibly $\Gamma(s)$ and the p-adic zeta function $\zeta_p(s)$. **[4-5]**

Public key cryptography, and its relationship to $\mathbb{Z}_{pq}$, finite fields, and elliptic curves – One of the most important applications of number theory (and some would say its only application) is to the art of keeping secrets. Because of the popularity of the internet to send private information (e.g. credit card numbers when buying something online), keeping this information private has become a very important issue. It is surprising how simple the mathematics is behind the most popular (and secure?) encryption schemes, and how the age of modern cryptography was born from a few clever applications of these simple ideas. Your project should explain how some of the most popular encryption schemes work, and analyze their security (both in terms of general time estimates, and special situations/keys to avoid). This will lead you to think about the problems of factoring numbers, finding logarithms mod p, and the basics of elliptic curves. **[3-5]**

Factoring and Primality Testing – The problem of finding large prime numbers has always been an interesting pastime, but with the recent advent of public-key cryptography and its implications for data-security and privacy, it has become a very serious endeavor. In the last 30 years, many algorithms have been developed to help answer the questions: "Is a given number m prime?" and if not, "What is its prime factorization?". Answering these questions efficiently involves many of the structures we have considered in class (Z_p, continued fractions, quadratic number fields), as well as some ideas which are a bit deeper (Elliptic curves, complex multiplication, general number fields), and it is interesting to see how much better they allow us do. The prime numbers one can generate at present routinely have hundreds of decimal digits, and in some special cases they can be quite a bit larger. (The largest known prime as of today has 7,235,733 decimal digits!) Your project should explain the answers to these questions, explaining both why these varied methods work, and how efficient they are. It will also be fun to apply them to some large examples to see how practical they are! **[3.5-5]**

Elliptic Curve Cryptography – The modern phenomenon of public-key cryptography and the role of number theory in designing (hypothetically) secure cryptosystems has given new importance to classical questions like "How can we tell is a number is prime?" and "How can we factor a given number quickly?". The efficiency of the answers determine the "security" of certain modern cryptosystems, which are widely used today. The bad news is that since we don't actually know the best possible answers to these questions, we can't actually guarantee that these commonly used systems are secure. This has driven the search for a variety of different cryptosystems, each of which may have different vulnerabilities and strengths. One recent favorite is to use the points on certain "Elliptic curves" $E : y^2 = x^3 + Ax + B$ for given $A, B \in \mathbb{Z}$ to encrypt information and factor numbers. Your project should describe the basic properties of these curves, explain how they can be useful for encryption and factoring, and do a few examples to illustrate this. **[4-5]**

The group law on elliptic curves, and finding rational and integral points. – In class we will briefly study the integer and rational solutions of the Diophantine equations $y^2 = f(x)$ where $f(x)$ is some cubic polynomial. This solutions of such equations are called elliptic curves, and understanding them is a very rich area of number theory. (For example, they were used to prove Fermat's Last Theorem!) It is an amazing fact that you can use lines to define an addition operation on the rational points on an elliptic curve, which helps us to answer questions like: "How many rational points are there on an elliptic curve?" and "What do they look like?". For a given elliptic curve, one can use this (and other) ideas to try to find all of of its

rational (and integral) points. Your project should describe the addition law for elliptic curves, and some techniques for finding and understanding their integral and rational points. Using these methods, you should compute the rational an integral points for a few different examples. Along the way, you will also be able to use a simple version of this idea to find all rational points on any conic (circle, ellipse, or hyperbola). **[4-5]**

Congruence and Hasse-Weil Zeta functions – Many of the most important questions in number theory are connected to questions about "Zeta functions" associated to various interesting objects. In class we will see how the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ helps us to understand many deep questions about the prime numbers. It turns out that we can construct zeta functions associated to any curve (for example, the unit circle $x^2 + y^2 = 1$ or an elliptic curve $y^3 = x^3 + x$), and this helps us to understand the rational points on that curve. This Hasse-Weil zeta function is assembled by looking at the points of our curve over certain finite fields associated with each prime number (of which $\mathbb{Z}/p\mathbb{Z}$ is an example), and then multiplying these pieces together. These computations involve really interesting calculations with Gauss sums, and the resulting zeta functions are connected with current unanswered questions of number theory today. Your project should describe how to construct these zeta functions, compute a few examples simple examples, and describe their relevance to understanding the rational points on elliptic curves. **[3.5-5]**

Solving $x^3 + y^3 = z^3$ and $x^4 + y^4 = z^4$ – While there are infinitely many integer solutions to the equation $x^2 + y^2 = z^2$, there are no solutions of the equation $x^n + y^n = z^n$ for any integer power $n > 2$ where one of x, y, z are not zero. This is called Fermat's Last theorem, even though his supposed proof has never been found. Very recently, a proof of this has been found using elliptic curves and modular forms. However, Fermat was able to prove the cases $n = 3$ and $n = 4$ by his method of "infinite descent". Your project should explain Fermat's proof for $n = 3$ and 4, and its relationship to descent on elliptic curves. **[3.5-5]**

Cubic and Biquadratic reciprocity – In class we will be interested in exploring the question "When is α a square in $\mathbb{Z}_p$?" The answer is intimately connected to the famous theorem of *quadratic reciprocity*, originally proved by Gauss (in many different ways). Your project should explain how one can answer the question of "When is α a cube (or 4^{th} power) in $\mathbb{Z}_p$?", and prove the associated 'higher' reciprocity law(s) of cubic (and biquadratic) reciprocity. **[4-5]**

Cyclotomic numbers and Fermat's last theorem – In class we have discussed the ring $\mathbb{Z}[i]$ where $i = \sqrt{-1}$. One can also study more general number systems involving roots of 1 called the *cyclotomic integers*, which look like $\mathbb{Z}[\zeta_p]$ where ζ_p is a p^{th} root of 1 (and p is an odd prime). These number systems play a central role in much of number theory, and their arithmetic was used to prove many cases of Fermat's last theorem. Your project should describe the cyclotomic integers, and explain the proof of Fermat's last theorem in the case where the $\mathbb{Z}(\zeta_p)$ has unique prime factorization. **[4-5]**

Special values of $\zeta(s)$ – The Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ is a function which encodes lots of information about the integers $\mathbb{Z}$. In particular, features of $\zeta(s)$ can be used to prove the existence of infinitely many primes (using its pole at $s = 1$) and the prime number theorem (which says roughly how the primes are distributed in the integers, by understanding its complex zeros). Because of these connections, it is important to try to understand as much about $\zeta(s)$, and its values, as possible. Along these lines, it is natural to ask for a formula for the values of $\zeta(s)$ when s is a natural number. Unfortunately, the exact values are not known in general (though there are conjectures), except when $s = 2k$ is an even integer. In this case, there are deep connections between this value and the arithmetic of the cyclotomic integers $\mathbb{Z}[\zeta_p]$ (defined above), which helps to prove many cases of Fermat's last theorem. Your project should prove an explicit formula for these special values $\zeta(2k)$, and describe this connection to $\mathbb{Z}[\zeta_p]$. **[3-5]**

Constructability of regular polygons – At the tender age of 18, Gauss solved the 2,000 year old question of "Which regular polygons can be constructed with only a compass (which makes arcs) and a straightedge (which makes lines)?". His proof is connected to the cyclotomic fields $\mathbb{Q}(\zeta_m)$, and the structure of their quadratic subfields $\mathbb{Q}(\sqrt{D})$. Your project should prove Gauss's theorem, and use it to give explicit (algebraic and geometric) constructions of a few of these 'constructible' regular polygons. **[3-4] (Requires Galois theory.)**
