MATH 4573: COURSE PROJECT LIST

INSTRUCTOR: TYLER GENAO

Project due date: April 19, 2024.
Optional project draft deadline: April 5, 2024.

The following is a list of topics that can be assigned as your class project. Each one has a short summary meant to give you an overview of the topic – you don't have to stick with it when working on your project.

Project Title	Summary
Algebraic curves over finite fields	Equations over a finite field F must always have a finite amount of solutions over F – contrast this to solutions for equations over $\mathbb{Q}$. For example, an elliptic curve $y^2 = x^3 + Ax + B$ over F will have a finite amount of solutions, and the number of solutions will explicitly depend on the the "Frobenius automorphism" of F and a special polynomial over $\mathbb{C}$. This project will explore counting other types of curves and their points modulo p. See e.g. Chapters 10 and 11 of [IR90].
Algebraic integers	Just as $\mathbb{Q}$ is the ring of fractions of $\mathbb{Z}$, for any finite degree extension $F/\mathbb{Q}$ there exists a "ring of integers" $\mathcal{O}_F$ whose ring of fractions is F, and which satisfies a special type of unique factorization for its "ideals" rather than its numbers. Such rings are called *algebraic number rings.* For example, the field $\mathbb{Q}(\sqrt{2})$ has ring of integers $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. This project explores some of the properties of algebraic number rings, as well as how their arithmetic differs from $\mathbb{Z}$. See e.g. Chapter 9 of [NZM91], as well as the bonus exercises in HW 2 and HW 3.
Binary quadratic forms	A *binary quadratic form* is a two-variable polynomial of the form $f(x, y) := ax^2 + bxy + cy^2$, where $a, b, c \in \mathbb{Z}$. Fixing such an f, it is interesting to ask which integers $n \in \mathbb{Z}$ can be "represented" by f, i.e., $f(x_0, y_0) = n$ for some $x_0, y_0 \in \mathbb{Z}$. For example, fixing $f(x, y) := x^2 + y^2$, we've shown that a prime $p \in \mathbb{Z}^+$ is represented by $f(x, y)$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$, see [NZM91, Lemma 2.13]. A more general result is [NZM91, Theorem 2.15]. This project explores the general properties of binary quadratic forms, their connections to matrices, and when they represent an integer $n \in \mathbb{Z}$. See e.g. §3.4 − 3.7 of [NZM91].

Project Title	Summary
the Bunyakovsky conjecture	The Bunyakovsky conjecture asks whether any polynomial $f(x) \in \mathbb{Z}[x]$ satisfying three particular conditions will produce infinitely many primes of the form $f(n)$ where $n \in \mathbb{Z}^+$. When f has degree one, this is a theorem due to Dirichlet on primes in arithmetic progressions. It is open, however, for all degrees ≥ 2. This project explores these three conditions, and their necessity. It also explores what is known about the values $f(n)$ for well-known polynomials such as $f(x) := x^2 + 1$ (see also the bonus exercises in HW 2 and HW 3).
the Chevalley-Warning theorem	Given a finite field F of characteristic $p > 0$ and polynomials $f_1, f_2, \ldots, f_r \in F[x_1, x_2, \ldots, x_n]$ in several variables, it is interesting to ask how many simultaneous solutions there are to $f_1, f_2, \ldots, f_r$ over F. Remarkably, the Chevalley-Warning theorem says that the number of solutions is always a multiple of p if the sum of their degrees is less than the number of variables: i.e., $d := \sum_{i=1}^{r} \deg(f_i) < n$. Thus, for example, having at least one solution implies at least p solutions. This project explores the proof of the Chevalley-Warning theorem, as well as what happens when $d \geq n$; see e.g. this paper.
Cubic reciprocity	Quadratic reciprocity determines precisely when the congruence $x^2 \equiv q \pmod{p}$ has solutions for odd primes $p, q \in \mathbb{Z}^+$. This is connected to the splitting behavior modulo q of a certain quadratic polynomial which depends on p; this itself is connected to the splitting of p in the algebraic number ring $\mathbb{Z}[\sqrt{q*}]$, where $q* \in \{q, -q\}$ is chosen so that $q* \equiv 1 \pmod{4}$. Similarly, there are higher laws of reciprocity. The next simplest case is *cubic reciprocity,* which determines when $x^3 \equiv p \pmod{q}$ has a solution. This is connected to the *ring of Eisenstein integers,* $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. This project will explore the Eisenstein integers and a proof of cubic reciprocity. See e.g. Chapter 9 of [IR90].

Project Title	Summary
the discrete logarithm problem	For any prime $p \in \mathbb{Z}^+$, we know that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, i.e., there exists a primitive root mod p. Therefore, there exists $[g] \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that any element $[a] \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a power of $[g]$, i.e., $a \equiv g^e \pmod{p}$ for some $0 \leq e < p-1$. Computing powers of g is rather straightforward. However, given $[a] \in (\mathbb{Z}/p\mathbb{Z})^\times$, it can be difficult to determine the unique $0 \leq e < p-1$ for which $g^e \equiv a \pmod{p}$; such an e is the *discrete logarithm of a modulo p with respect to base g.* In this project, you will explore how the discrete log problem is used in modern cryptography, and when certain choices of p create security vulnerabilities.
Elliptic curves	Elliptic curves over a field F are (almost always) defined by an equation of the form $y^2 = x^3 + Ax + B$, where $A, B \in F$. Elliptic curves have applications in number theory, algebraic geometry and cryptography; they are particularly special algebraic curves, in that the set $E(F)$ of their solutions with F-rational coordinates forms a group under the "chord-and-tangent" method. As it turns out, when $F = \mathbb{Q}$ the group $E(\mathbb{Q})$ is a *finitely generated abelian group,* which implies it is isomorphic to a group of the form $\mathbb{Z}^r \times T$, where $r \geq 0$ and $\#T < \infty$. This project explores r (the *rank* of the elliptic curve) and/or the finite group T (the *torsion subgroup* of the elliptic curve). See e.g. [LR11].
Fermat's last theorem	One of the most important mathematical theorems of the 20'th century is Fermat's last theorem, which states that for all $n \geq 3$ the Diophantine equation $x^n + y^n = z^n$ has no solutions $x_0, y_0, z_0 \in \mathbb{Z}^+$. Stated as a theorem in 1637 with no proof, it has since been proven more than 300 years later using deep results in elliptic curves and modular forms. In this project, you will prove the first two cases of Fermat's last theorem: that $x^3 + y^3 = z^3$ and $x^4 + y^4 = z^4$ have no positive integer solutions. These two cases only require elementary techniques to prove.

Project Title	Summary
Finite fields	Generally speaking, doing arithmetic over a field is easier than over a general ring, since all nonzero elements are invertible. However, fields come in many shapes and sizes: for example, the ring $\mathbb{Q}$ of rational numbers is a field, as well as $\mathbb{Z}/p\mathbb{Z}$ for all primes $p \in \mathbb{Z}^+$. However, $\#\mathbb{Q} = \infty$, whereas $\#\mathbb{Z}/p\mathbb{Z} = p$. This project will study *finite* fields, including their construction, uniqueness, elements and arithmetic. See e.g. Chapter 7 of [IR90].
p-adic numbers	The ring of p-adic integers, denoted $\mathbb{Z}_p$, is a generalization of the usual integers $\mathbb{Z}$ through an "inverse limit" process: a p-adic integer is an infinite tuple of integers $(a_1, a_2, a_3, \ldots)$ where $a_{i+1} \equiv a_i \pmod{p^i}$ for all $i \geq 1$. In this way, p-adic integers are like "infinite lifts" of a system of congruences modulo powers p^k. One can study p-adic solutions to Diophantine equations as is done in §2.6 and §2.7. As it turns out, such solutions encode important information about rational solutions. Just as $\mathbb{Z}$ has $\mathbb{Q}$ for its set of fractions, $\mathbb{Z}_p$ has the *p-adic numbers* $\mathbb{Q}_p$. This project explores the rings $\mathbb{Z}_p$ and $\mathbb{Q}_p$ and their construction, as well as their differences from $\mathbb{Z}$ and $\mathbb{Q}$. See e.g. [Gou20].
the prime number theorem	The prime number theorem states that the number of primes p up to a number $x \geq 0$ is asymptotically $\frac{x}{\log(x)}$. Differently stated, we have $\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log(x)}} = 1$, where $\pi(x)\colon \mathbb{R}_{\geq 0} \to \mathbb{Z}^+$ counts the number of primes up to x. This project explores the history of the prime number theorem and the functions number theorists use to approximate $\pi(x)$. If you'd like to try, find and understand an elementary proof of the prime number theorem. See e.g. Chapter 8 of [NZM91], as well as the bonus exercises in HW 2.

Project Title	Summary
Primes in arithmetic progressions	Given any coprime integers $a, m \in \mathbb{Z}^+$, there are infinitely many primes in the congruence class of a modulo m, i.e., there are infinitely many primes $p \in \mathbb{Z}^+$ with $p \equiv a \pmod{m}$. This result is often called Dirichlet's theorem on primes in arithmetic progressions. We've proven the infinitude of the primes $p \equiv 3 \pmod{4}$ in HW 2. This project will study other elementary proofs for the infinitude of primes $p \equiv a \mod m$, for varying coprime a and m. See also the bonus exercises in HW 2.
the ring of arithmetic functions	Given two arithmetic functions $f, g\colon \mathbb{Z}^+ \to \mathbb{C}$, it is not hard to see that their pointwise sum $f + g\colon \mathbb{Z}^+ \to \mathbb{C}$ is also an arithmetic function. As it turns out, there also exists a "multiplication" operation on any two arithmetic functions f and g, called the *convolution;* this is denoted as $f * g$. The set $\mathcal{A}$ of arithmetic functions has the structure of a ring under these two operations; it is called the Dirichlet ring. This project explores the algebraic structure of the Dirichlet ring $(\mathcal{A}, +, *)$ and its ring-theoretic properties.
RSA cryptography	RSA is a public key cryptosystem: it uses a public key to encrypt data, and a private key to decrypt it. RSA exploits the general difficulty of factoring the product pq of two large prime numbers to keep encryption secure. Encryption and decryption is done via exponentiation modulo pq. This project explores the RSA algorithm. If you have programming experience, you can also implement the algorithm.

The following references are good sources for expository material on several of these projects:

References

[Gou20] F.Q. Gouvêa, *p-adic numbers*, 3rd ed., Springer (2020).

[IR90] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Springer-Verlag, New York (1990).

[LR11] Á. Lozano-Robledo, *Elliptic curves, modular forms, and their L-functions*, American Mathematical Society, Providence, RI; Institute for Advanced Study (IAS), Princeton, NJ (2011).

[NZM91] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers*, 5th ed., John Wiley & Sons, Inc., New York (1991).