The following topics are suggestions for the Math 110 WIM project. You may also choose a topic not on this list, but please have your choice approved with Jenny and Jeremy.

You have some freedom in which details you choose to include in your paper, but every project should contain at least one significant mathematical result and its proof.

Contents

1 The Primitive Root Theorem

Suggested references:
Trappe–Washington, Chapter 3.7
Stein, Chapter 2.5

Project description:
The goal of this project is to prove the following theorem:

Theorem 1.1. *If p is a positive prime, then there is at least one primitive root b among the units of $\mathbb{Z}/p\mathbb{Z}$.*

Proofs of Theorem 1.1 typically involve proving the following results:

- Let p be prime. If $f(x)$ is polynomial with coefficients in $\mathbb{Z}/p\mathbb{Z}$, of degree d, then at most d congruence classes modulo p are roots of f.
- If a, b are units in $\mathbb{Z}/p\mathbb{Z}$ such that $\gcd(\mathrm{ord}_p(a), \mathrm{ord}_p(b)) = 1$, then $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a)\ \mathrm{ord}_p(b)$.

There are several ways the proof can proceed by here. One strategy:

- For each prime q dividing $p-1$, show that there a unit a modulo p so that $a^{\frac{p-1}{q}}$ is not congruent to 1 modulo p. Conclude that $a^{\frac{p-1}{q^r}}$ has order q^r for any power q^r dividing $p-1$.
- Construct a unit modulo p with order $p-1$.

Theorem 1.1 is also proven in Chapter 2.5 of Stein, using a slightly different outline. You may read Stein's proof and use the outline presented there, however, if you do closely follow Stein's proof then please additionally include the solution to Exercise 2.28b:

Theorem 1.2. *If p is a positive odd prime, then $(\mathbb{Z}/p^k\mathbb{Z})^\times$ has a primitive root for any $k \geq 1$.*

If you are ambitious, and would be comfortable using some basic field theory and group theory, then you may consider completing this project by proving the following stronger result in place of Theorem 1.1.

Theorem 1.3. *If F is any finite field, then the units of F have a primitive root. In other words, the group of units $F^\times$ is cyclic.*

2 Continued Fractions and applications to cryptography

Suggested references:
Trappe–Washington, Chapter 3.12 and 6.2.1
Koblitz, Chapter V.4
Stein, Chapter 5
Rosen, Elementary number theory and its applications, Chapter 10

Project description:
This paper should serve as an introduction to continued fractions, and describe at least one of their applications to cryptography.

Your introduction should provide a definition, relevant terminology, examples, and mathematical context for continued fractions. You may want to explain the sense in which they give the "best" rational approximations, their connection to the Euclidean algorithm, or other mathematically interesting properties.

You can include facts about continued fraction without proof (with a reference for the proof given). That said, the project should include at least one rigorous proof of a significant mathematical result. For example, you could prove the result:

Theorem 2.1. *For any x with convergents $\frac{p_n}{q_n}$,*

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

You could additionally (optionally) prove the result in Trappe-Washington 3.12:

Theorem 2.2. *If $\left|x - \frac{r}{s}\right| < \frac{1}{2s^2}$ for integers r, s, then $\frac{r}{s}$ is a convergent of x.*

Finally, the paper should include an example of how continued fractions can be used in cryptography. One option is to describe the continued fraction method for low exponents attacks on RSA (see, for example, Trappe-Washington 6.2.1). Another is to describe the "Continued Fraction Factoring Algorithm" (see, for example, Koblitz V.4).

3 Miller-Rabin Primality Test

Suggested references:
Trappe-Washington Chapter 6.3
Koblitz Chapter V.1 and exercises

Project description:
The goal of this paper is to describe and analyze the Miller-Rabin primality test. The paper should include background on history and uses of primality testing, and the significance of Miller-Rabin. The paper should explain the test, and prove that the test returns a false a positive with probability at most 25% for a randomly chosen base a.

You may also wish to include one or more of the following:

- discussion of the time efficiency (number of bit operations) of the test
- comparison to other primality tests (such as Solovay–Strassen)
- discussion of relative advantages of probabilistic tests compared to deterministic ones
- comment on how (assuming the Generalized Riemann Hypothesis) the Miller-Rabin test is deterministic
- discussion of variations on the Miller-Rabin test

4 Zero knowledge proofs

Suggested references:
Trappe–Washington, Chapter 14 and 3.9
Martin Tompa, Zero Knowledge Interactive Proofs of Knowledge
Koblitz, Chapter IV.5

Project description:
The goal of this project is to present a zero knowledge proof that one knows the factorization of a large integer n. We assume that $n = pq$ is a product of two large primes, and it is computationally infeasible for an adversary to factor n. Peggy, the prover, has picked p and q and kept them secret, but told the world that she knows the factorization of n. Victor, the verifier, wants to ask questions to check whether Peggy actually knows the factorization. The protocol should be zero knowledge in the sense that the exchange should not help Victor, or any eavesdropper, actually compute the factorization of n. It should be a proof in the sense that for any $\epsilon > 0$, by asking enough questions Victor should be able to verify that there is at most an ϵ chance that Peggy is lying about knowing the factorization. This protocol can be used to make an identification scheme, for example.

To do this, one uses a simpler zero knowledge proof, that a prover knows a square root of some integer a modulo n. Peggy also needs to be able to compute square roots modulo n, given the prime factors p and q. Together these ingredients can be combined to give a zero knowledge proof for factorization.

You should keep the following questions in mind:

- How do the zero knowledge proofs of knowing a square root of $a \mod n$ and of knowing a factorization of n work?
- Why can the prover successfully answer the questions to convince the verifier?
- If an adversary could successfully answer the questions, why can they factor n (which is assumed to be infeasible)?
- Why are the protocols zero knowledge?
- How does Peggy compute square roots modulo n? It is fine to assume that $p, q \equiv 3 \mod 4$.

You might also want to discuss how this can be used, or discuss a physical example of a zero knowledge proof.