

SUGGESTED PROJECTS, MATH 350, SPRING 2022

The following is a list of possible projects. You can and are encouraged to find interesting topics in number theory yourself. You are supposed to learn something *new*, something you didn't know before (and certainly not something you have learned in past courses). It is important to **make your choice early** and **start working on your project asap**. Of course I will be glad to discuss things with you.

1. Let n be a positive integer. Define a polynomial $f_n(X)$ with coefficients in $\mathbb{Z}/n\mathbb{Z}$ by

$$f_n(X) \equiv \prod_{t \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - t) \pmod{n}.$$

This project is to try to determine this polynomial $f_n(X)$. It is a bit open-ended. For instance you can put constraints on n and determine the polynomial $f_n(X)$ under the constraints imposed on n . You can gather numerical data for many values of n , make plausible guesses for general n , further check your conjecture, then try to prove your conjecture.

Here is a possible approach. You are also encouraged to try your own ideas.

- (a) You can reduce the question for general n to the case when n is a power of a prime number. In other words, for every prime divisor p of n , how to express $f_n(X)$ modulo p^a in terms of $f_{p^a}(X)$, where p^a is the highest power of p dividing n .
- (b) For $n = p^a$, a power of a prime number, try to determine $f_p(X) \pmod{p}$, $f_{p^2}(X) \pmod{p^2}$, $f_{p^3}(X) \pmod{p^3}$. Can you find a pattern. After finding a pattern, try to prove it.
- (c) There is a symmetry about $f_n(X)$:

$$f_n(aX) \equiv f_n(X) \pmod{n} \quad \text{for every } a \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

2. Let p be a prime number. Present a the definition/construction of p -adic integers (\mathbb{Z}_p), the p -adic numbers (\mathbb{Q}_p) and some of their basic properties, including Hensel's lemma. (This project is related to project 1.)

Possible sources: The first few chapters of Serre's book, and also chapter 1 of Hasse's *Number Theory*.

3. Present a proof of Dirichlet's theorem on primes in arithmetic progressions. (This project is related to project 3.)

Possible sources: The books by Hua, Landau and Serre, and also the first few chapters of Davenport's *Multiplicative Number Theory*.

4. **Density of a set of prime numbers** (as a subset of the set of all prime numbers). A weak version of Dirichlet's theorem on primes in arithmetic progression asserts that for every positive integer $n \geq 3$ and every integer a relatively prime to n , there exists infinitely many prime numbers p which are congruent to a modulo n . A stronger version asserts that the subset of all prime numbers p which are congruent to a modulo n is a subset of density $1/\phi(n)$ of the set of all prime numbers, with a suitably defined notion of density.

There are at least two notions of density for a subset S of the set P of all prime numbers.

(a) The limit

$$\lim_{x \rightarrow \infty} \frac{\#\{p \in S \mid p \leq x\}}{\#\{p \in P \mid p \leq x\}},$$

if exists, is called the *natural density* of S .

(b) The limit

$$\lim_{s \rightarrow 1^+} \frac{\sum_{p \in S} p^{-s}}{\sum_{p \in P} p^{-s}}$$

if exists, is called the *analytic density* (or Dirichlet density) of S .

Explain these two notions, and illustrate them with examples (as many as you can find). Try to answer the following question: if a subset S of P has a density in one notion, does it also has a density in the other notion, and whether the two densities are equal.

5. (**Transcendence of e**) Present a proof of the irrationality and the transcendence of e .

6. (**Irrationality and transcendence of π**) Present a proof of the transcendence of π .

Possible sources for projects 4 and 5: Hardy–Wright chapter 11, Hua chapter 17.

7. Study and present at least two (preferably more) proofs of quadratic reciprocity which are *essentially different* from Zolotarev's proof as in Theorem 8.22 in Weissman or Gauss's original proof as explained in class. See margin note 30 on page 219 of Weissman, or <http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html>, for further reference. There are quite a number of articles available on the internet on proofs of quadratic reciprocity. You can certainly look at them, but do not copy any of these.)

8. Let a be a quadratic residue modulo p . Produce and explain an algorithm which is polynomial-time in the bit length of p , for solving the congruence equation

$$x^2 \equiv a \pmod{p}$$

9. **Jacobi symbol, Kronecker symbol and the Hilbert symbol.** The Jacobi symbol is defined on page 221 of Weissman's book in an exercise. They generalize Legendre symbols, and can be computed quickly (polynomial in the input bit length), because the Jacobi symbol satisfies a quadratic reciprocity law similar to Legendre symbols. In particular Legendre

symbols can also be computed quickly. However there is more mathematics hidden under the Jacobi symbol and the reciprocity law. For instance $\left(\frac{d}{a}\right)$ with d a fixed *fundamental determinant* while b varies, can be thought of as a Dirichlet character attached to a quadratic field. Also the Jacobi symbol is closely related to the *Hilbert symbol*. Possible reference: chapter 5 of Hasse's *Number Theory*.

10. Give a presentation of the **quadratic sieve** method used for factoring composite numbers.

11. **The number field sieve.** This is considered the best known method for factoring generic composite numbers. Give a presentation of this method.

Projects 10 and 11 together can be presented by two people as a team. Possible sources for projects 10 and 11: *Prime Numbers* by Crandall and Pomerance. The bibliography for chapter 2 of Ribenboim's *The Little Book of Prime Numbers* contains many books and expository articles on factoring.

12. (von Staudt) The Bernoulli numbers are defined by

$$\frac{x}{e^x - 1} = 1 - \frac{1}{2}x + \sum_{k=1}^{\infty} \frac{(-1)^k B_k}{(2k)!} x^{2k}$$

Von Staudt's theorem states that

$$(-1)^k B_k - \sum_{(p-1)|2k} \frac{1}{p} \in \mathbb{Z},$$

where p runs through all prime numbers such that $p - 1|2k$. Give a presentation about this result.

13. We can write every real number x , $0 \leq x \leq 1$ in its decimal expansion

$$x = \sum_{i=1}^{\infty} a_i(x) 10^{-i}$$

where each $a_i(x)$ is an integer between 0 and 9. A real number x between 0 and 1 is said to be decimally *normal* if

$$\lim_{n \rightarrow \infty} \frac{1}{n} \# \{i \leq n \mid a_i(x) = r\} = \frac{1}{10}$$

for $r = 0, 1, 2, \dots, 9$. If we use base a positive integer $n \geq 2$ instead of 10 as the base, we arrive at a similar notion of *n-adically normal numbers*. Give a presentation of (a) the fact that for almost all real numbers x between 0 and 1 are decimally regular and (b) whether there exist a real number which is *n-adically regular* for every $n \geq 2$. (Here "almost all" means that, the set of all real numbers between 0 and 1 which are not decimally regular has *measure zero*. A part of this project is to find and understand the definition of sets of measure zero.)

Note: This topic is often used as an example in probability or measure theory. See for instance chapter 1 of Billingsley's *Probability Theory*.

14. The identity

$$\prod_{m=1}^{\infty} (1 - x^m) = \sum_{n=-\infty}^{\infty} (-1)^n x^{\frac{1}{2}n(3n+1)}$$

is known as Euler's identity. It can be interpreted as a formula for $E(n) - U(n)$, where $E(n)$ is the number of ways to partition n into an even number of unequal parts, and $U(n)$ is the the number of ways to partition n into an odd number of unequal parts. Given a presentation of this topic.

Possible source: Chapter 19 of Hardy–Wright, chapter 14 of *Introduction to Analytic Number Theory* by Apostol, or search the internet with keywords: generating functions, partitions, Jacobi identity.

15. (**Explicit formula for the number of solutions** in a few examples of Waring's problem.) There are explicit formulas which expresses the number of solutions of Diophantine equations

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2 \tag{a}$$

$$4n = x_1^2 + x_2^2 + x_3^2 + x_4^2 \tag{b}$$

in terms of the function $\sigma(n) := \sum_{d|n} d$. Give a presentation of these formulas.

Possible sources: Hardy–Wright chapter 20, Landau Part three chapter 4. There is also a more powerful approach using modular forms.

16. Explain how to compute/generate a primitive root of 1 in $(\mathbb{Z}/p\mathbb{Z})^\times$ when you are handed a large prime number p .

[Theoretically, all you need to do is to factor $p - 1$. However this is not a feasible when p is large—factoring is exponential in the length of $p - 1$. So one needs a better way “produce” primitive roots, an algorithm which is polynomial in the length of p , with a high degree of probability for success. Note that being able to compute a primitive root of 1 in $(\mathbb{Z}/p\mathbb{Z})^\times$ is the first step in implementing a discrete logarithm crypto system based on modular arithmetic.]

17. Give a presentation on the existence of *undecidable problems*.

[This is a theoretical limit which even quantum computers cannot break. Quantum computers can be modeled by Turing machines in exponential time, i.e. what you gain with quantum computing is time. These undecidable problems are those which cannot be solved even you have infinite time.]

18. Elliptic curves. This is a big subject; we can have several people doing it. There are many directions, such as

- What are elliptic curves and what they are good for.
- Geometric, analytic and arithmetic of elliptic curves.
- How to find solutions of these cubic equations, including
 - rational solutions
 - solutions in $\mathbb{Z}/p\mathbb{Z}$
- elliptic curve crypto systems

19. Smooth numbers and Hardy-Ramanujan theorem. The theorem asserts roughly that “almost all” positive integer n , the number of prime factors of n is $\log \log n$.

Reference: Hardy–Wright chapter 22 §11.

20. The Prime Number Theorem.

Reference: D. Zagier, Newman’s short proof of the prime number theorem, *The American Mathematical Monthly* **104** (1997), 705–708. See also the paper by P. Bateman and H. Diamond, A hundred years of prime numbers, *The American Mathematical Monthly* **103** (1996), 729–741.

21. Continued fractions.

A century ago, this topic was often taught in high school, because it is useful in computation. (They give very efficient numerical approximations.) Theoretically they are also useful for approximating irrational numbers by rational number (diophantine approximation).

Possible sources: There is a nice think book *Continued Fractions* by Khinchin. Continued fractions are discussed in the books by Davenport, Hardy–Wright and Hua.

22. Find/explain ways to *compute* a solution of a quadratic congruence equation

$$x^2 \equiv a \pmod{p}$$

for a (large) given odd prime number p and an integer a . (You don’t want to do it by trial-and-error: if p has more than 100 decimal digits, it takes longer than one’s lifetime to try $n \bmod p$ for $n = 1, 2, \dots, (p - 1)/2$.)

Note: Use Jacobi symbols, one can quickly determine whether the above congruence equation has a solution. Finding a method (which can be implemented as an algorithm) to compute a solution modulo p is a different matter. Known methods include the Cipolla algorithm and the Tonelli–Shanks algorithm. Both algorithms make random choices and are probabilistic in some sense.

23. Applications of Number Theory

Many number theorists a century ago (e.g. Hardy) took pride that their treasured subject “had no conceivable application” in the earthly world. The opposite is true now. This project is quite open ended: present an interesting application of number theory in science and communication.

You can find a number of possibilities in Schroeder’s *Number Theory in Science and Communication*. However please do not present things you already learned in some other course. (We use an “honor system” in math 350.) For instance, computer science majors are likely to have taken seen various cryptographic protocols such as Diffie-Hellman, RSA. The general idea is that you want to choose a topic which interests you, and you want to learn something new, understand it, and present a concise version in your own words to your friends.