Math 322: Number Theory
Fall 2019

Jay Daigle

No Additional Background Required

- **Continued Fractions**

  A continued fraction is an expression of the form

  $$a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

  Every rational number can be expressed as a finite continued fraction. Every irrational number can be expressed uniquely as an infinite continued fraction.

  Reference: Rosen chapter 10, PMF chapter 14, Stein chapter 5,

- **The sum of prime reciprocals** The Wikipedia page is actually a good start: `https://en.wikipedia.org/wiki/Divergence_of_the_sum_of_the_reciprocals_of_the_primes`

  More citeable: `http://www.math.toronto.edu/rosent/Mat246Y/Euler.pdf` `http://alpha.math.uga.edu/~pollack/eulerprime.pdf` `http://www.daniellitt.com/s/primes1mod4.pdf`

- **Sieve theory**

  `http://math.uga.edu/~lyall/Analysis/brunsieve.pdf`

  `http://iml.univ-mrs.fr/~ramare/Maths/LecturesEasyChennai.pdf`

- **Fermat's Last Theorem**

  Fermat's last theorem (proven by Wiles in 1996) famously states that $x^n + y^n = z^n$ has no nontrivial integer solutions of $n > 2$. Proving the entire theorem is (very far) beyond the scope of this course, but some results are much easier. For instance, roving it for all n divisible by four is quite doable for a paper for this course.

  Reference: include PMF chapter 15, Rosen 13.2,
  `http://fermatslasttheorem.blogspot.com/2005/05/fermats-last-theorem-n-4.html`,
  and `http://math.uga.edu/~pete/4400flt4.pdf`

- **Gaussian integers**

  We often want to extend our studies to larger "integer-like" sets. The simplest is the so-called "Gaussian integers" $\mathbb{Z}[i]$ first studied by Gauss in order to prove biquadratic reciprocity. Many of the same results that hold over the integers hold as well in the Gaussians (in particular they are a "Euclidean domain", which means an analogue of the Division Algorithm applies). A paper could explore some of the results we have proven in class and extend them to the Gaussian integers.

  Reference: PMF chapter 13

- **p-adic numbers**

- **The Quadratic Sieve**

- **Systems of Linear Congruences** (requires Linear Algebra)

  See Rosen 3.4

- **Partitions** (see Rosen 7.5)
- **Cyclotomic Polynomials** (See e.g. Rosen 7.4.33-36)
- **Pseudoprimes**

  See Rosen 5.2
- **Perpetual Calendar** and other applications of congruences

  See Rosen Chapter 4

Complex Numbers and Analysis

- **Exponential Sums**

  A number of important number-theoretic functions, such as the Möbius function, can be viewed as sums of the form $\sum_{i=1}^{n} e^{im_n}$–that is, sums of complex roots of unity.

Groups

- **Elliptic Curves**

  An elliptic curve is a curve with equation $y^2 = x^3 + ax + b$ for $a, b \in \mathbb{Z}$. Many number theorists study the set of rational points on these curves; they are particularly interesting because the set of rational points forms a group under an idiosyncratic addition law. A paper could explain the group law on elliptic curves, and state and possibly prove some basic results about elliptic curves. (There are a number of choices here; also, some interesting cryptographical systems rely on elliptic curves).

  References: Stein Chapter 6.
- **Characters**

  A *character* of a group G is a homomorphism from G into $\mathbb{C} \setminus \{0\}$ interpreted as a group under multiplication. (In practice this turns out to be a group homomorphism into $\mathbb{Z}/n\mathbb{Z}$). Many of the multiplicative functions we study–and many we do not–can be viewed as group characters. The set of characters of a finite group themselves form a group.

  A paper could explain the basics of character theory and relate this to various important number-theoretic functions such as the Legendre symbol.

  References: Ireland and Rosen Chapter 8, most undergraduate algebra textbooks
- **Non-unique factorization**

  While some "integer-like" sets have number theory much like the integers, others do not. In particular some easy to describe sets such as $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ do not have the property of "unique factorization": while the concept of a "prime number" still exists, many numbers have more than one factorization into prime numbers.

  Reference: any undergraduate algebra textbook

Probability and Statistics

`https://terrytao.files.wordpress.com/2009/09/primes_paper.pdf`
`http://math.hawaii.edu/~xander/Fa06/Billingsley--Prime_Numbers.pdf`

- arithmetic statistics
- Random prime models (Cramér, Hardy-Littlewood)

Computer Science

- Cryptography algorithms [Not allowed if you're in my Cryptology class]
  - RSA depends on prime factorization
  - Diffie-Hellman and El-Gamal depend on the discrete logarithm
- Pollard ρ and other factorization algorithms.
- Prime testing algorithms

Analysis

- Prime Number Theorem
- Ramanujan Sums
- Riemann zeta function