Suggested Projects, Math 350, Fall 2015

The following is a list of possible projects. You are encouraged to find interesting topics in number theory yourself.

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: try to determine $f_n(X)$. A possible approach:

(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 $f_{p^n}(X)$, 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 $f_p(X) \bmod p$, $f_{p^2}(X) \bmod p^2$, $f_{p^3}(X) \bmod p^3$. 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. Find the statement of Chebyshev's theorem on prime numbers, and present a coherent proof. (The statement is weaker than the prime number theorem.)

3. Find the statement of Bertrand's hypothesis/postulate, and present a coherent proof.

4. Study and present one or two proofs of quadratic reciprocity which is *essentially different* from the proof in Silverman's book.

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

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

6. The numbers $\Phi = \frac{\sqrt{5}+1}{2}$ and $\phi = \frac{\sqrt{5}-1}{2}$ determine the *golden ratios*; see p. 258 of Silverman's book. They are closely related to Fibonacci sequences. These numbers occur often in architecture, arts, and nature. Give a presentation about them. (This project is especially suitable for a power-point-like show. You can grow artificial sun flowers, for instance.)

7. Penrose tiling is also related to the golden ratios. Give a presentation of Penrose tiling and its many aspects.

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

9. Give a presentation on pseudorandom numbers generators. (Computer illustration in class are welcome.)

10. Give a presentation about quantum computing: how to use a quantum computer to factor composite numbers in polynomial time.

11. Give a presentation on efficient algorithms for multiplication and division, and/or fast Fourier transform.

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. Present a version of Hensel's Lemma over $\mathbb{Z}/p^n\mathbb{Z}$ (or $\mathbb{Z}_p$), for a system of n polynomial equations in n variables over $\mathbb{Z}/p^n\mathbb{Z}$ (or $\mathbb{Z}_p$), analogous to the inverse function theorem.

14. 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 regular" (non-standard terminology) if

$$\lim_{n\to\infty} \frac{1}{n} \#\left\{i \leq n \,|\, a_i(x) = r\right\} = \frac{1}{10}$$

for $r = 0, 1, 2, \ldots, 9$. Give a presentation of the fact that for almost all real numbers x between 0 and 1 are decimally regular. (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.)

15. The identity

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

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. (Keywords: generating functions, partitions, Jacobi identity.)

16. Explain how to use the discrete logarithm as the basis of a public key crypto system.

[Project 16 is related to project 17 below, and can be combined with it.]

17. 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.]

18. 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.]

19. 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