Suggested Projects, Math 350, Spring 2005

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

1. (a) Formulate Hensel's Lemma over $\mathbb{Z}_p$, including a version that does not require the derivative at an approximate solution to be non-congruent to 0 modulo p, in such a way that the statement of Theorem 4.14 in Rosen's book becomes a corollary of your formulation.

(b) Formulate (and prove) Hensel's Lemma for a system of polynomial equations in several variables, with the number of equations equal to the number of variables, either for $\mathbb{Z}/p^m\mathbb{Z}$ or for $\mathbb{Z}_p$.

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

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

Determine $f_n(X)$. (Notice that this is equivalent to determining $f_n(X)$ modulo p^a, for prime divisors p of n, and p^a is the highest power of p dividing n.)

3. Prove Chebyshev's theorem. (This is weaker than the prime number theorem. In Rosen's book you can find exercises leading to a proof. You can also consult other books in number theory.)

4. Prove Bertrand's hypothesis. (In Rosen's book you can find exercises leading to a proof. You can also consult other books in number theory.)

5. Study and present some proofs of quadratic reciprocity not seen in class or from the textbook. (You can find some references in Rosen's book.)

6. (a) Suppose that p is an odd prime number. Write $p - 1 = 2^r \cdot s$, where s is an odd number, $r \geq 1$. Give a probabilistic algorithm, polynomial in the bit length of p, for finding an element $b \pmod{p}$ of order 2^r. (In other words, $b^{2^r} \equiv 1 \pmod{p}$, and $b^{2^{r-1}} \not\equiv 1 \pmod{p}$.)

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

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

7. The numbers $\Phi = \frac{\sqrt{5}+1}{2}$ and $\phi = \frac{\sqrt{5}-1}{2}$ determine the *golden ratios*. They are closely related to Fibonacci sequences; see Chap. 1, section 4 of Rosen's book. These numbers occur often in architecture, arts, and nature. See page 599 of Rosen's book for a URL about the Fibonacci numbers. Give a presentation about them. (This project is especially suitable for a power-point-like show. You can grow artificial sun flowers, for instance.)

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

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

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

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

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

13. (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 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.)

14. 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.)