Math 354: Number Theory
Summary of Lectures- Spring 2015.

In this document I will give a summary of what we have covered so far in the course, provide references, and given some idea of where we are headed next. There will be a lot of overlap between the descriptions given here and the introductory comments on each homework assignment.

1 Lecture 1

In the first lecture of the course I gave an overview of some of the types of problems that number theorists are interested in. Number theory is a huge subject so I cannot possibly cover everything. There was definitely a bias towards the type of number theory I like. Some of these problems are the types of things we will cover in this course and others would be covered in a more advanced number theory course.

Here are some examples of the types of problems we discussed. How do you classify rational solutions to $x^2 + y^2 = 1$? Do these ideas extend to classifying solutions to similar types of equations? What if we look at equations of these types modulo n for different values of n? How often can we write n as a sum of two integer squares? How is this related to finding primes in the set of *Gaussian integers* $\mathbb{Z}[i]$ or *Eisenstein integers* $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$? Which positive integers can be written as sums of three squares? What about four squares? Which triangular numbers are also squares? What does this have to do with Pell's equation $x^2 - dy^2 = 1$, and how does this equation relate to continued fractions? We also discussed the distribution of prime numbers and stated the prime number theorem. At the end of this lecture we showed an example of how the computer algebra system Sage can be used to investigate many of these questions.

2 Lecture 2

In this lecture we got started on the actual material of the course by proving unique factorization of integers into primes, closely following Chapter 1 of Ireland and Rosen. We skipped some of the material including unique factorization of polynomials in $k[x]$ and unique factorization in principal ideal domains. We defined the greatest common divisor and introduced the Euclidean algorithm.

3 Lecture 3

We started by reviewing the Euclidean algorithm and gave some examples. We defined finite simple continued fractions and proved a theorem relating the two. This material is not really covered in

detail in Ireland and Rosen, but is contained in the first few sections of Nathanson.

We then transitioned to talking about counting prime numbers, pretty closely following Ireland and Rosen Chapter 2. We gave Euclid's proof of the infinitude of primes and used it to prove a weak lower bound on $\pi(x)$. We gave another proof of the infinitude of primes that involved writing every integer n as ab^2. We gave a better lower bound for $\pi(x)$ by introducing a function that counts the number of integers less than x that only have prime divisors in a finite set S.

4 Lecture 4

We continued our discussion of counting primes following Ireland and Rosen Chapter 2. We proved that the sum of the reciprocals of the prime numbers diverges and proved the Euler product expansion for the Riemann zeta function. We stated several theorems where values of $\zeta(s)$ appear in asymptotic counts for number theoretic questions. We then used properties of the binomial coefficient $\binom{2n}{n}$ to give the upper bound in Chebyshev's theorem.

5 Lecture 5

We proved the lower bound for Chebyshev's theorem by again considering the primes dividing $\binom{2n}{n}$. We stated a number of difficult results involving sets whose sum of reciprocals diverge, including Szemeredi's theorem, the Green-Tao theorem, and the Erdös-Turan conjecture. This involved defining asymptotic/natural density for an infinite set.

We then started the proof of Bertrand's postulate, that there is always a prime between n and $2n$, closely following the presentation in Proofs from the Book (PFTB). This involved more carefully considering the primes dividing $\binom{2n}{n}$.

6 Lecture 6

We started by going over the last details of the proof of Bertrand's postulate. We gave the Euclid style argument that there are infinitely many primes congruent to 3 modulo 4. We proved some of the basic properties of congruences following Chapter 3 of Ireland and Rosen. We showed that $\mathbb{Z}/m\mathbb{Z}$ forms a ring and that $\mathbb{Z}/p\mathbb{Z}$ is a field and reviewed some necessary algebraic background. We discussed counting solutions to congruences modulo n.

7 Lecture 7

We started by considering when a linear congruence is solvable modulo n. We introduced the Euler phi function and reviewed Lagrange's theorem from group theory and some of its basic consequences. We used this to prove Euler's theorem and Fermat's Little Theorem. This all pretty closely follows Ireland and Rosen, although the necessary statements about group theory are contained in Nathanson. As a consequence we gave another proof of the infinitude of primes by considering factors of Mersenne numbers. This is one of the arguments in PFTB. We stated the Chinese Remainder theorem and prove some lemmas to lead up to its proof.

8 Lecture 8

We proved the Chinese Remainder Theorem. We introduced the concept of a numerical semigroup. This is not covered in Ireland and Rosen but is the subject of Section 1.6 of Nathanson. We then returned to Chapter 3 of Ireland and Rosen and gave the isomorphism between $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z}$. This had nice consequences for Euler's phi function, which allowed us to prove some of the results in Chapter 2 that we had originally skipped. We then moved on to prove that a degree d polynomial in $k[x]$ has at most d distinct roots in k.

9 Lecture 9

We started by proving that the multiplicative group of a finite field is cyclic following the argument given in PFTB. We proved Wilson's theorem in two different ways, first by grouping together residues modulo p and then by factoring $x^{p-1} - 1$. We briefly discussed the converse. We showed how Euler's theorem can show that a number is composite but that it can fail in some cases. We defined a pseudoprime base a and a Carmichael number. We showed that there are infinitely many pseudoprimes base a by some clever polynomial arithmetic combined with Euler's theorem. We stated and proved one direction of Korselt's criterion for Carmichael numbers.

Nathanson has a section on pseudoprimes and Carmichael numbers, but unfortunately it does not have the existence of pseudoprimes result from lecture or Korselt's criterion. This first argument is trickier to find (I learned it from a book of Crandall and Pomerance), but Korselt's criterion should be very 'google-able'.

10 Lecture 10

We started by finishing the proof of Korselt's criterion and then stating Giuga's conjecture. We gave a statement of the Miller-Rabin primality testing algorithm but did not discuss the proof

that it works. Stein's book *Elementary Number Theory: A Computational Approach* gives a nice discussion of this and is available for free online.

We then shifted back to talk about primitive roots modulo n and showed that there always exist primitive roots modulo p^e for any odd prime p and any $e \geq 1$. We also characterized the group structure of $(\mathbb{Z}/2^e\mathbb{Z})^*$. This closely follows Chapter 4 of Ireland and Rosen.

11 Lecture 11

We will start by characterizing the set of n such that there exists a primitive root modulo n. We then stated Artin's Primitive Root Conjecture, an important unsolved problem. We briefly discussed solving equations modulo n and mentioned some cases we will consider later on in the course, for example binary quadratic forms and elliptic curves. We then began to talk about n-th power residues following the end of Ireland and Rosen Chapter 4. We stated some results about n-th power residues without proving them. We will discuss Hensel's lemma after the midterm, which is a nice tool for using solutions of equations modulo p to get solutions modulo higher powers of p, and is directly relevant to these types of questions.

12 Lecture 12

We first stated and proved Hensel's lemma, which is Theore 3.18 in Nathanson. We then started to discuss the structure of the set of quadratic residues modulo p, introducing the Legendre symbol and proving some of its basic properties. This closely followed the presentation in the beginning of Chapter 5 of Ireland and Rosen. We showed the -1 is a quadratic residue modulo an odd prime p if and only if $p \equiv 1 \pmod 4$. We used this to show that there are infinitely many primes congruent to 1 modulo 4. We stated Gauss' lemma and used it to determine when 2 is a quadratic residue modulo p. We then used this to show that there are infinitely many primes congruent to 7 modulo 8.

13 Lecture 13

We proved Gauss' Lemma following the argument in Proofs from the Book. We then used it to prove quadratic reciprocity (again from PFTB). This argument involves cleverly dividing up a certain set of lattice points so that the number of lattice points in two special regions correspond to the exponents in Gauss' lemma, and there is a nice involution on the rest of the points.

We then gave the first PFTB proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares. This involved a clever application of the pigeonhole principle. We started (but did not finish) the next

proof, which involves considering the set of integer points solving $4xy + z^2$ where $x, y > 0$, focusing in on two special subsets, and studying a few special involutions on this set. At the end of class I gave out Zagier's one sentence proof of this theorem.

14 Lecture 14

We finished the Heath-Brown proof about sums of two squares and noted that this actually gives us more information, telling us the number of ways of writing $p = (2x)^2 + y^2$ with $x, y > 0$ is odd. In fact, it is unique which we also proved. We also gave a complete characterization of the set of integers n that are the sum of two squares. We stated, but did not prove, the theorem giving the number of ways of writing n as a sum of two squares.

15 Lecture 15

We followed the beginning of Chapter 7 of Ireland and Rosen pretty closely. We considered the factorization of $x^q - q$ in $F[x]$ where F is a finite field of size q. We then showed that every finite field has prime power order. We classified the possible subfields of a finite field of size p^n Finally, we showed that $\mathbb{Z}/p\mathbb{Z}[x]/\langle f \rangle$, where f is an irreducible polynomial of degree n, gives a finite field of size p^n.

I do not think that this section of Ireland and Rosen is as clear as it could be. I would recommend the course notes of Sophie Huczynska found here:
`http://www.math.rwth-aachen.de/~Max.Neunhoeffer/Teaching/ff2013/ff2013.pdf`

I think it would be particularly helpful to read through Sections 4 and 5. Chapter 3 is all about finite fields and contains more information than we will cover. I would also recommend reading Section 6.1 of Ireland and Rosen to see how some of the material about algebraic numbers is presented there. Lots of this can be carried over to the finite field setting, which is what I-R means in the comment following Proposition 7.2.2: ?The proof of this proposition is the same as that of Proposition 6.1.8 and its corollary. One replaces Q by k and the complex number alpha by the above alpha?.

Proposition 6.1.7 introduces the notion of the minimal polynomial of a complex number alpha. This is in definition 4.9 in the reference above (for ?algebraic over? see definition 4.7). The result we want to prove is then a version of parts (i) and (ii) Theorem 5.9 here. Part (i) is basically what we did in class and part (ii) is the statement from the end, that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ give a basis of $K(\alpha)$ over K, that is, they span $K(\alpha)$ and are linearly independent.

16 Lecture 16

We now know that an irreducible polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$ of degree n gives a finite field of size p^n. So in order to show that there exists a finite field of every prime power order we need only show that for each prime p and each $n \geq 1$, there is an irreducible polynomial of degree n with coefficients in $\mathbb{Z}/p\mathbb{Z}$. We will show something stronger, using the Möbius inversion formula to count the number of such polynomials.

We first considered the factorization of $x^{p^n} - x$ in $\mathbb{Z}/p\mathbb{Z}[x]$. Comparing degrees gave an expression involving sums of N_d, the number of irreducible polynomials of degree d. The Möbius-Inversion formula then gives an expression for N_d that is clearly at least 1 for each d. We followed the presentation of the ring of arithmetic functions given in Section 6.1 of Nathanson. We gave many examples of arithmetic functions and then focused on the Möbius μ-function. We proved Möbius inversion, which is actually a very simple statement about the Dirichlet convolution of two arithmetic functions. Finally, we showed that the probability as p goes to infinity that a randomly chosen polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$ of degree d is irreducible converges to $1/d$.

The part of Chapter 2 of Ireland and Rosen that we previously skipped is a nice reference for this material as are Sections 6.1 and 6.3 of Nathanson.

17 Lecture 17

We gave a second proof of quadratic reciprocity following Proofs from the Book. This argument involves working in a cyclic subgroup of size p inside a finite field of size q^{p-1}. We consider a certain kind of Gauss sum G, computing G^q in two different ways.

Ireland and Rosen also give an introduction to Gauss sums in Chapter 6, but their point of view is a little different. Their Gauss sums involve sums of powers of complex pth roots of unity. It is a good exercise to read this chapter and see how the argument we presented matches up with the argument of this reference. We briefly discussed the sign of the Gauss sum, Section 6.3 of Ireland and Rosen, but did not give the proof.

We discussed the problem of finding the least quadratic residue modulo p. We stated the Polya-Vinogradov theorem, which shows that the Legendre symbol cannot take too many consecutive values of the same sign. As a consequence we see that the least quadratic residue is always at most $\sqrt{p}\log(p) + 1$. We can do a little better on the least quadratic residue problem. We showed that the least quadratic residue is always prime, and that it is at most $1 + \sqrt{p}$.

18 Lecture 18

We gave the proof of Polya-Vinogradov, which is probably the most difficult argument we have given so far. This proof is basically what is written here:
http://planetmath.org/polyavinogradovinequality

I mentioned that this result can be improved. The Burgess bound is a more difficult result about 'short character sums'. This involves analytic number theory tools that we have not seen yet so do not worry if you cannot follow the argument. An exposition is given here:
http://www.math.harvard.edu/~elkies/M259.06/burgess.pdf

We then started to talk about cyclotomic polynomials the monic polynomials whose roots are the primitive nth roots of unity. We proved some of their basic properties and introduced some problem about their coefficients. This is not covered in either of our textbooks. The best reference is these notes of Abhinav Kumar's MIT number theory course:
http://ocw.mit.edu/courses/mathematics/18-781-theory-of-numbers-spring-2012/lecture-notes/MIT18_781S12_lec12.pdf

19 Lecture 19

We began by considering roots of cyclotomic polynomials modulo p. We then adapted the argument that we used to show that there are infinitely many primes congruent to 1 modulo 4, using $\Phi_n(x)$ to show that there are infinitely many primes congruent to 1 modulo n. I mentioned that there is also an elementary argument that shows that there are infinitely many primes congruent to -1 modulo n, but it is much harder. For details, see this paper:
http://www.jstor.org/discover/10.4169/amer.math.monthly.122.01.48?uid=3739832&uid=2&uid=4&uid=3739256&sid=21106424517013

In general, the infinitude of primes in arithmetic progressions is given by Dirichlet's Theorem which involves complex analysis. Proofs are given in Serre's book *A Course in Arithmetic* or in Stein and Shakarchi's *Fourier Analysis*. I stated the prime number theorem for primes in progressions, which combines Dirichlet's theorem with the prime number theorem. For a proof of the prime number theorem, see Stein and Shakarchi's *Complex Analysis* (or a number of other references).

We then switched gears and began discussing Lagrange's theorem on sums of four squares. We first showed that by Euler's identity it is enough to show this for odd primes p. We shows that there is some m satisfying $1 \leq m < p$ such that mp is a sum of four squares. Our goal is then to show that the minimal such m is 1.

For this topic we closely follow the presentation of Lalín:
http://www.dms.umontreal.ca/~mlalin/Lagrange.pdf

20 Lecture 20

We completed the proof of Lagrange's theorem. We then talked about sums of higher powers, giving an overview of what is known about Waring's problem.

Our next main goal is to prove Fermat's Last Theorem for $n = 4$. We first gave a careful statement of this theorem. We then focused in on Pythagorean triples, giving two different ways to understand the classification of them, one algebraic and one more geometric. The best reference for this material is Kumar's notes:
`http://ocw.mit.edu/courses/mathematics/18-781-theory-of-numbers-spring-2012/lecture-notes/MIT18_781S12_lec23.pdf`

21 Coming Up

We have four remaining lectures: Tuesday April 14th, Thursday April 16th, then the exam on April 21st, lecture on April 23rd, and a final lecture during reading period on April 28th.

Our first goal is to prove Fermat's last theorem for $n = 4$. We will then discuss other instances of the 'method of infinite descent' and connections to the congruent number problem on areas of right triangles with rational sides.

We will discuss the Chevalley-Warning theorem, which is the subject of Section 10.2 of Ireland and Rosen. This has to do with zeros of equations over finite fields. We will also talk a little more about the geometry of finite fields and low-degree curves.

22 References

At this point we have covered most of Ireland and Rosen up through Chapter 7 except that we presented a different take on the material of Chapter 6. We have also covered some topics that are not covered in Ireland and Rosen, but are discussed in Nathanson. We have covered everything in Nathanson up through the end of Chapter 2 except Section 2.7. We have also covered Sections 3.1 and 3.2, and Sections 6.1 and 6.3. We followed the proof of Chebyshev's theorem in Ireland and Rosen, but Nathanson gives a similar proof in Section 8.1.

We gave some arguments not contained in either of these books. For example, we gave five of the six proofs of infinitude of primes given in PFTB and closely followed the proof of Bertrand's postulate given there. We also gave the argument that the multiplicative group of a finite field is cyclic given on page 28 there. We also gave the two proofs about sums of two squares, the proof of Gauss' lemma, and the both proofs of quadratic reciprocity from this text.

There are also some additional topics not covered in these references. Links to where you can read about them are given in the relevant section of the notes above. If you are having a hard time finding a reference for anything please let me know and I can update this document.