MATH 152 NOTES

MOOR XU
NOTES FROM A COURSE BY KANNAN SOUNDARARAJAN

Abstract. These notes were taken from math 152 (Elementary Theory of Numbers) taught by Kannan Soundararajan in Fall 2010 at Stanford University. These notes were live-TEXed during the lecture in `vim` and compiled using `latexmk`. Each lecture gets its own section. The notes were not edited afterward, so there may be typos; please email corrections to `moorxu@stanford.edu`.

1. 9/20

Information for the course exists at the website `http://math.stanford.edu/~ksound`.

There is no required book for the course, but some books are on reserve in the library.

30% from homework, 30% from one midterm, 40% from the final.

We have a CA, and he will also have office hours. Sound's office is in 383W. His office hours will be Thursdays, 1-3.

Homeworks will be given Wednesdays and due the following Wednesday.

1.1. **Introduction.** This course is about number theory, which is the study of properties of $\mathbb{N}$ or $\mathbb{Z}$ or $\mathbb{Q}$.

There is some kind of basic theory leading up to quadratic reciprocity. I like to have a big theorem, and we'll end up proving that given any arithmetic progression, it contains an infinite number of primes.

Today we'll start with primes.

1.2. **Primes.** One definition that you can make is the definition of an irreducible. We make a distinction here just for fun.

Definition 1.2.1. A natural number $n > 1$ is called **irreducible** if n cannot be written as $n = ab$ with $1 < a, b < n$.

This is what usually one calls a prime number.

That's actually one way of writing what a prime is; here's one that is more natural. We need the concept of divisibility.

Definition 1.2.2. Given two integers $a \neq 0$ and b; we say that $a|b$ if $b = ac$ for some integer c.

Definition 1.2.3. A natural number $p > 0$ is prime if $p|ab \implies p|a$ or $p|b$.

It's not clear that our two definitions are the same, so we need to prove a theorem.

Theorem 1.2.4. *The primes and irreducibles are the same.*

Proof. It is true that we can write each number as a product of irreducibles. We can prove this by induction. That's the same as factoring a number. We'd like to say that there is only one way of factoring each number. Let's prove this first.

Theorem 1.2.5 (Fundamental Theorem of Arithmetic)**.** *Every number n is a product of primes in a unique way.*

This needs a proof; it is not an obvious fact. Why? Consider an example.

Example 1.2.6. Consider the even numbers $A = \{2, 4, 6, 8, \dots\}$. The irreducibles are 2, 6, 10, 14, 18, 22, etc – the numbers that are not multiples of 4. Not every number can be written uniquely as a product of irreducibles; for example, $60 = 6 \cdot 10 = 2 \cdot 30$. Why is it true that unique factorization doesn't hold here? Why do proofs of FTA fail in this case?

There is the division algorithm:

Proposition 1.2.7 (Division algorithm)**.** *Given n, $a \in \mathbb{N}$, we can find $q, r \in \mathbb{Z}$ with $n = aq + r$, and $0 \leq r < a$.*

Does this hold for our example? If we divide 30 by 2, we would get a remainder that is too large: $30 = 2 \cdot 14 + 2$.

There are other contexts when the division algorithm holds, but it's not always clear.

This suggests that we need to use the division algorithm in our proof. We need to prove something about the greatest common divisor.

Definition 1.2.8. Given two numbers $a, b \in \mathbb{Z}$ (not both 0), we say that $g \in \mathbb{N}$ is the **greatest common divisor** of a and b if $g|a$ and $g|b$, and if it is the largest such number – no number greater than g divides both a and b.

There is a really nice property of the GCD that will help us.

Theorem 1.2.9. *Given a and b, there exists integers x, y such that $g = ax + by$.*

Let's use this to finish proving our Theorem 1.2.4.

First, we need to show that every prime is irreducible. Suppose not; there is a prime p that is not irreducible. Then express $p = cd$ with $1 < c, d < p$. Then $p|cd$, which implies that $p|c$ or $p|d$ (since p is prime), which is a contradiction because $c, d < p$.

Conversely, we show that every irreducible is prime. Given an irreducible n, and that $n|ab$, we want to have that $n|a$ or $n|b$. Suppose n doesn't divide a. The GCD of n and a is 1, so Theorem 1.2.9 tells us that $1 = nx + ay$, so that $b = nbx + aby$. Therefore $n|b$, which is what we wanted to show. This means that n is prime. □

Proof of Theorem 1.2.5. We can now prove Theorem 1.2.5. We need to show uniqueness. Suppose that there are two factorization:

$$n = p_1 \cdots p_r = q_1 \cdots q_s.$$

Now, $p_1|p_1 \cdots p_r$, so $p_1|q_1 \cdots q_s$. Therefore, p_1 divides one of $q_1, \dots q_s$. But $q_1 \dots q_s$ are irreducibles, so p_1 equals one of $q_1, \dots q_s$. We can then cancel p_1 on both sides and continue with p_2. □

Now we turn to the proof of the theorem for the GCD.

Proof of Theorem 1.2.9. Let $S = \{ax + by : x, y \in \mathbb{Z}\}$. Clearly, $0, a, b \in S$. Let's just look at the positive numbers. By the well-ordering property, there is a smallest number; let s be the smallest natural number in S.

We claim that every element of S is a multiple of s. This comes from the division algorithm: for $n \in S$, $n = qs + r$ where $0 \leq r < s$, then $r \in S$. But then $r = 0$ by the minimality of s.

In particular, $s|a$ and $s|b$, so $s = ax + by$ is a common divisor of a and b. We need to show that there are no bigger divisors. Any common divisor of a and b divides s, so $s = \gcd(a, b)$. □

Of course, this could also have been proved using the Euclidean Algorithm. Here, we computed $(312, 968) = 8$, and $8 = 10 \cdot 968 - 31 \cdot 312$.

Now that we know what the primes are, let's talk about properties of primes.

Theorem 1.2.10 (Euclid)**.** *There are infinitely many primes.*

We consider several proofs:

Proof. Suppose not. Then there are only finitely many primes $p_1, \ldots, p_n$ are all the primes. But then $p_1 \cdots p_n + 1$ is a new prime, which is a contradiction. □

Proof. If there are few primes, there must also be few natural numbers. But we know the number of natural numbers. That's the idea; let's make this precise.

Usually, $\pi(x)$ will denote the number of primes up to x. Consider $n \leq x$. Factorize a number $n \leq x$ such that

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}.$$

Assume that there are only k primes.

Every number can be written as $n = ab^2$ where a is square-free. This is of course unique. If there are only k primes, there are only 2^k square-free numbers. Now,

$$\sum_{n \leq x} 1 = \sum_{\substack{ab^2 \leq x \\ a \text{ square-free}}} 1 < \sqrt{x} \sum_{\substack{a \leq x \\ a \text{ square-free}}} 1 \leq 2^k \sqrt{x}.$$

This is a contradiction for $x > 4^k$. □

This also gives a bad bound

$$\pi(x) \geq \frac{\log x}{\log 4}$$

.

We describe the factorization of $n!$. Given a prime p, what is the exact power of p dividing $n!$; this is sometimes denoted $p^\alpha || n!$.

So the power of p dividing $n!$ equals

$$s_p := \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right].$$

Note that this is actually a finite sum. Now,

$$n! = \prod_{p \leq n} p^{s_p}.$$

Proposition 1.2.11. *We have Stirling's Formula:*

$$n! \approx \sqrt{2\pi n} e^{-n} n^n.$$

In number theory, we are often interested in how quickly something can be computed – with a computer program, for example. GCD was fast to compute, while $n!$ is not fast to compute; that's why we care about Stirling's Formula.

Another form of Stirling is

$$\log n! = n \log n - n$$

.

Proof. We have

$$\log n! = \sum_{1 \le m \le n} \log m.$$

Comparing the sum to an integral, we see that

$$n \log n - n + 1 = \int_1^n \log t \, dt \le \log n! \le \int_1^{n+1} \log t \, dt = (n+1)\log(n+1) - n$$

We can write

$$\log(n+1) = \log n + \log(1 + \frac{1}{n})$$

and use a Taylor expansion. So

$$(n+1)\log(n+1) = (n+1)\log n + \frac{n+1}{n} - \dots.$$

□

2. 9/22

Instead of writing down inequalities all the time, we want a more convenient notation to drop insignificant terms.

Definition 2.0.12. $f(x) = O(g(x))$ if there is a constant C such that $|f(x)| \le Cg(x)$ for all large x.

Example 2.0.13. For example, $x = O(e^x)$, $\sqrt{x} = O(x)$, $\sin(x) = O(1)$, $\log x = O(x^{0.01})$.

Our previous inequalities for $\log n!$ can now be written as

$$\log n! = n \log n - n + O(\log n),$$

and Stirling's formula would be

$$\log n! = n \log n - n + \frac{1}{2} \log n + \frac{1}{2} \log 2n + O\left(\frac{1}{n}\right).$$

2.1. **The number of primes.** So why is this useful for studying primes? We had the formula

$$\log n! = \sum_{p \le n} s_p \log p,$$

where

$$s_p = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots$$

Using the fact that $[x] = x + O(1)$, we have $s_p = \frac{n}{p} + O(1) + O(\frac{n}{p^2})$.

Now, we have

$$\sum_{p \le n} \left(\frac{n}{p} + O(1) + O\left(\frac{n}{p^2}\right)\right) \log p = n \sum_{p \le n} \frac{\log p}{p} + O\left(\sum_{p \le n} \log p\right) + O\left(n \sum_{p \le n} \frac{\log p}{p^2}\right)$$

The final term has a sum that converges, so it reduces to $O(n)$. We will prove that the middle term is also $O(n)$. Assuming this, we have

$$n \sum_{p \le n} \frac{\log p}{p} + O(n) = n \log n - n + O(\log n)$$

so that

$$n \sum_{p \le n} \frac{\log p}{p} = n \log n + O(n).$$

Theorem 2.1.1. *As $n \to \infty$,*

$$\sum_{p \le n} \frac{\log p}{p} = \log n + O(1).$$

Note that here, it is no longer important that n is an integer. So we can replace it by a real number x, and the formula would still make sense.

Why do we care? We want to study $\pi(x) = \sum_{p \le x} 1$. The first person to make real progress toward this was Gauss, and he made a conjecture that became the prime number theorem.

Theorem 2.1.2 (Prime Number Theorem, Gauss, 1896)**.**

$$\pi(x) \approx \int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right).$$

Our previous theorem was a weak version of the prime number theorem.

Based on what we know, we can still say something about primes. Here's a weaker result:

Proposition 2.1.3 (Chebyshev)**.**

$$\frac{cx}{\log x} \le \pi(x) \le \frac{Cx}{\log x}$$

for some constants $0 < c < C$ and all large x.

The prime number theorem would state that

$$\lim_{n \to \infty} \frac{\pi(x)}{x/\log x} = 1,$$

so this is clearly a bit weaker.

From the Chebyshev bounds, we get the following nice result about primes that says that prime occurs will some regularity.

Theorem 2.1.4 (Bertrand's Postulate)**.** *For every $n \geq 2$, there is always a prime between n and $2n$.*

2.2. **Proof of a Chebyshev bound.**

Proof of a Chebyshev bound. Here, we will prove one of the Chebyshev bounds.

We will consider the middle binomial coefficient $\binom{2n}{n}$. We want to understand its prime factorization. We have some easy bounds because it is the biggest binomial coefficient:

$$\frac{2^{2n}}{2n+1} \leq \binom{2n}{n} \leq 2^{2n}.$$

This means that

$$2n \log 2 - \log(2n+1) \leq \log \binom{2n}{n} \leq 2n \log 2.$$

What is the power of p dividing $\binom{2n}{n}$? Using the factorial form of the binomial coefficient, we see that this is

$$\sum_{j=1}^{\infty} \left[\frac{2n}{p^j}\right] - 2\sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right] = \sum_{j=1}^{\infty} \left(\left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right] \right).$$

Note that

$$[2x] - 2[x] = \begin{cases} 0 & \{x\} \in [0, \frac{1}{2}) \\ 1 & \{x\} \in [\frac{1}{2}, 1) \end{cases}$$

For the large primes, we only have to consider $j = 1$, which is easy. The smaller primes are messier. We divide into two groups of primes.

For large primes $p > \sqrt{2n}$, the power of p dividing $\binom{2n}{n}$ is either 0 or 1, depending on the fractional part of $\{\frac{n}{p}\}$.

For example, if $n < p \leq 2n$, then the power of p is 1. Of course, this should be obvious from the factorial form.

If $\frac{2n}{3} < p \leq n$, the power of p is 0.

If $\frac{n}{2} < p \leq \frac{2n}{3}$, the power of p is 1.

We can keep extending this.

For the primes $p < \sqrt{2n}$, the exponent of p dividing $\binom{2n}{n}$ is at least 0 and at most $\frac{\log 2n}{\log p}$.

So the binomial coefficient satisfies

$$\prod_{p \leq 2n} p^{\frac{\log 2n}{\log p}} \geq \binom{2n}{n} \geq \prod_{n < p \leq 2n} p$$

This gives us

$$\frac{2^{2n}}{2n+1} \leq \binom{2n}{n} \leq \prod_{p \leq 2n} 2n = (2n)^{\pi(2n)}.$$

This actually tells us that

$$\pi(2n) \geq \frac{\log\left(\frac{2^{2n}}{2n+1}\right)}{\log(2n)} = \frac{2n}{\log 2n} \log 2 - \frac{\log(2n+1)}{\log 2n} \geq \left(\frac{2n}{\log 2n}\right) \log 2 - 2,$$

which gives us a Chebyshev bound. Why did we consider $\binom{2n}{n}$? Ramanujan came up with the proof. □

Example 2.2.1 (Chebyshev)**.**

$$\frac{(30n)!n!}{(15n)!(10n)!(6n)!} \in \mathbb{N}.$$

Corollary 2.2.2.

$$\pi(x) \geq \frac{x}{\log x}(\log 2) + O(1).$$

We also have the following bound:

$$2^{2n} \geq \binom{2n}{n} \geq n^{\pi(2n)-\pi(n)},$$

so that

$$\pi(2n) - \pi(n) \leq \frac{2n \log 2}{\log n}.$$

As before, if we want, we can replace n by a real number x to get

$$\pi(2x) - \pi(x) \leq \frac{x}{\log x}(2 \log 2) + O(1).$$

This also gives an estimate for $\pi(x)$ by summing this formula and dividing by 2 at each step.

$$\pi(x) - \pi(x/2) \leq \frac{x/2}{\log x/2}(2 \log 2) + O(1).$$

This gives

$$\pi(x) \leq \frac{x}{\log x}(2 \log 2) + O(\log x),$$

yielding the other half of the Chebyshev bound. This is enough (with some tweaking) to prove Bertrand's Postulate. This uses the fact that if $\frac{2n}{3} \leq p \leq n$ then p does not divide $\binom{2n}{n}$.

3. 9/27

We will discuss the theory of congruences, leading up to quadratic reciprocity, for the next few lectures.

3.1. **Congruences.**

Definition 3.1.1. $n > 0$, $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n}$ means that $n \mid (a - b)$.

It is easy to see that this forms an equivalence relation. This means that it is satisfies

(1) $a \equiv a \pmod{n}$
(2) $a \equiv b \pmod{n}$ iff $b \equiv a \pmod{n}$
(3) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ means that $a \equiv c \pmod{n}$.

We have more properties:

- $a \equiv b \pmod{n} \implies ax \equiv bx \pmod{n}$
- $c \equiv d \pmod{n} \implies a + c \equiv b + d \pmod{n}$

We cannot always cancel, however. If $ax \equiv bx \pmod{n}$ and $(x, n) = 1$, then $a \equiv b \pmod{n}$.

3.1.1. *Residue classes.* It is natural to think about equivalence classes. Given any n, $\mathbb{Z}$ splits into n equivalence classes. These are called the residues mod(n). The set of residue classes $\pmod n$ forms an additive group, satisfying the standard properties of associativity, existence of identity, and inverses.

We can also multiply residue classes: $a \pmod n \times b \pmod n = ab \pmod n$. In general, this does not form a group, as 0 does not have an inverse. There is a multiplicative identity $1 \pmod n$.

Theorem 3.1.2. *The congruence* $ax \equiv b \pmod n$ *as a unique solution* $\pmod n$ *if* $(a, n) = 1$.

If $(a, n) = g$, then g must divide b for there to be a solution.

Proof. From $(a, n) = 1$, we see that $1 = ax + ny$. This means that we can solve $ax \equiv 1 \pmod n$, so $b = abx + nby$, so we therefore can solve $ax \equiv b \pmod n$.

For uniqueness, suppose that $ax \equiv b \pmod n$ and $ay \equiv b \mod n$. We can subtract these equations and cancel because $(a, n) = 1$. □

So this tells us precisely which residue classes are invertible.

Definition 3.1.3. $a \pmod n$ is a *reduced residue class* if $(a, n) = 1$.

Every reduced residue class is invertible. The set of reduced residue classes (mod(n)) with the operation of multiplication again forms an abelian group. (Check this).

It was clear that the additive group had n elements. It's not so clear for this multiplicative group.

Definition 3.1.4. The Euler phi function $\phi(n)$ is the number of reduced residue classes $\pmod n$.

Note. If p is prime, $\phi(p) = p - 1$, and $\phi(p^2) = p^2 - p$.

If we look at residue classes $\pmod p$, we only need to check distributivity to see that this forms a field with $(+, \times)$.

3.2. **Useful theorems.**

Theorem 3.2.1 (Wilson's Theorem)**.** *If* p *is a prime then* $(p - 1)! \equiv -1 \pmod p$.

Exercise 3.2.2. If $n > 4$ is composite then $(n - 1)! \equiv 0 \pmod n$.

Remark. Someone told Gauss that this would be hard to prove because there are no good ways to write primes, and Gauss said that they needed new notions and not new notations.

Proof of Wilson's Theorem. Consider

$$1 \times 2 \times 3 \times \cdots \times p - 1.$$

If $a \pmod p$, there exists $a^{-1} \pmod p$, and we can cancel the two. This is good as long as $a \not\equiv a^{-1} \pmod p$, but $a \equiv a^{-1} \pmod p$ means that $a^2 \equiv 1 \pmod p$, so we need to consider 1 and -1 as the two that do not cancel. Hence we get that the product is congruent to $-1 \pmod p$. □

From $a \pmod n$, we can compute $a^2 \pmod n$, $a^3 \pmod n$, etc. Since there are a finite number of reduced residue classes, we must come back to something that we had earlier. So $a^k \equiv a^l \pmod n$ for some $k < l$, so that $a^{l-k} \equiv 1 \pmod n$.

Definition 3.2.3. The *order* of the residue class $(\mathrm{mod}\ n)$ is the smallest $g \in \mathbb{N}$ such that $a^g \equiv 0 \pmod{n}$.

Example 3.2.4. The order of 1 is 1, and the order of -1 is 2 (if $n > 2$). Anything else would be hard to compute.

Theorem 3.2.5 (Euler's Theorem)**.** *If $(a, n) = 1$, then order of a divides $\phi(n)$.*

Corollary 3.2.6 (Fermat's Little Theorem)**.** *If p is prime, the order if $a \pmod{p}$ divides $p - 1$. Equivalently, if $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$, or equivalently, $a^p \equiv a \pmod{p}$.*

Proof of Euler's Theorem. Consider the $\phi(n)$ residue classes $1 \pmod{n}, \ldots, (n-1) \pmod{n}$. What happens when we multiply these by $a \mod n$? We get $a \pmod{n}, \ldots, (-a) \pmod{n}$. We claim that these two sets are the same. Each of these is reduced, so it was claimed in the original set. The reverse is also true because $ax \equiv b \pmod{n}$ has a solution, all of these are distinct. So our two sets of residue classes are permutations of each other.

So

$$\prod_{\substack{(b,n)=1 \\ b \pmod{n}}} b \equiv \prod_{\substack{(b,n)=1 \\ b \pmod{n}}} (ab) \pmod{n} \equiv a^{\phi(n)} \prod_{\substack{(b,n)=1 \\ b \pmod{n}}} b \pmod{n}.$$

Hence, $a^{\phi(n)} \equiv 1 \pmod{n}$. □

3.3. **Primality testing.**

Puzzle 3.3.1. Here is a puzzle. Two people meet on the internet, and they decide to get married. They want to send a ring, but the mail isn't secure. Everyone has a big supply of padlocks. How would they be able to send a ring so that at any time, the ring has at least one padlock on it.

Is it true that $a^{n-1} \equiv 1 \pmod{n}$ implies that n is prime? If $(a, n) \equiv 1$? The answer turns out to be no. There is this number $561 = 3 \times 11 \times 17$. But if $(a, 561) = 1$ then $a^{560} \equiv 1 \pmod{561}$.

To show this, observe that

$$\begin{aligned} a^2 \equiv 1 \pmod{3} &\implies a^{560} \equiv 1 \pmod{3} \\ a^{10} \equiv 1 \pmod{11} &\implies a^{560} \equiv 1 \pmod{11} \\ a^{16} \equiv 1 \pmod{17} &\implies a^{560} \equiv 1 \pmod{17}. \end{aligned}$$

Hence, the converse to Fermat's Little Theorem is not true. There are infinitely many numbers like 561; it is a *Carmichael number*.

What if we want to see if a number is prime? Check that $a^{n-1} \equiv 1 \pmod{n}$, and $(a, n) = 1$. If not, n is not prime. If so, we don't know; check with a different a. Eventually, we might have a good chance that this is prime, as Carmichael numbers are rare.

Is this good way to check primality? Is this fast to compute? We can compute $a^{n-1} \pmod{n}$ rapidly by repeated squaring.

Six or seven years ago, there was a jazzed up version of this from Agrawal, Kayal, and Saxena. It was a rapid (polynomial time) algorithm to determine whether a number is prime, answering a question of Gauss.

In contrast, we don't know a good way to factor numbers into primes. If there were a way, the remainder of this lecture would be pointless.

3.3.1. *Diffie-Hellman.* This is a precursor of RSA.

A and B want to have a common code word but while communicating in a pubic channel. Let p be prime and let g be a random complicated number. A thinks of a number x. She posts $g^x \pmod p$. B thinks of a number y and posts $g^y \pmod p$.

At this point, public information is g, p, g^x, and g^y, while x and y are private. Both A and B know g^{xy}, which no one else knows.

Why can't anyone else find g^{xy}? This is the discrete logarithm problem: Given x and g^x, find x. This has no known good solution. People don't know how to nicely do this with more than two people.

4. 9/29

Definition 4.0.2. $\mathbb{Z}/n\mathbb{Z}$ is the additive group of residue classes (mod n). $(\mathbb{Z}/n\mathbb{Z})^\times$ is the multiplicative group of residue classes (mod n), which has size $\phi(n)$.

4.1. **RSA Public Key Cryptography.** This uses Euler's Theorem. Say you're a big company like Amazon, and people want to buy stuff from you. You need to be able to send messages and receive coded messages. Everyone should be able to encode, and only you should be able to decode.

Pick two large primes p and q. These are secret. Compute $pq = n$ and compute the Euler phi function $\phi(n) = (p-1)(q-1) = pq - p - q + 1$. Choose a number c as the coding key, and find a number d such $cd \equiv 1 \pmod{\phi(n)}$. Suppose that $(c, \phi(n)) \equiv 1$. Then we can use the Euclidean algorithm to compute d rapidly.

Public information are c and n, while d is secret.

Anyone can send a message a. They compute $a^c \pmod n$ and send that to you. You can decode this by computing $(a^c)^d \equiv a^{1+k\phi(n)} \equiv a \pmod n$.

Nobody can prove that this is secure. It's easy to show that something is easy, but it hard to show why something should be hard. This is the $P \neq NP$ problem.

4.2. **Structure of group of reduced residues (mod n).** What is the structure of the group of all residues (mod n)? This is a cyclic group of order n generated by $1 \pmod n$. Actually, any a coprime to n also gives a generator $a \pmod n$.

4.2.1. *Chinese Remainder Theorem.* Consider the structure of the multiplicative group.

Theorem 4.2.1 (Chinese Remainder Theorem)**.** *If $(n_1, n_2) = 1$ then there is a natural bijection*

$$\begin{cases} a_1 \pmod{n_1}, & (a_1, n_1) = 1 \\ a_2 \pmod{n_2}, & (a_2, n_2) = 1 \end{cases} \leftrightarrow \begin{cases} a \pmod{n_1 n_2}, & (a, n_1 n_2) = 1. \end{cases}$$

Another way of saying this is that we can find a unique simultaneous solutions to

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$$

Proof. The main thing to use is that $(n_1, n_2) = 1$. This means that we can find k_1 and k_2 such that $n_1 k_1 + n_2 k_2 = 1$.

I want to find some number $a \pmod{n_1 n_2}$. We would like to use something like $a_1 n_2 k_2 + a_2 n_1 k_1$. Note that this is congruent to $a_1 \pmod{n_1}$ and congruent to $a_2 \pmod{n_2}$. $\square$

4.2.2. *Euler ϕ function is multiplicative.* One consequence of this is that the Euler ϕ function is multiplicative, so that if $n = n_1 n_2$ and $(n_1, n_2) = 1$, then $\phi(n) = \phi(n_1)\phi(n_2)$.

Therefore, if $n = \prod p_i^{\alpha_i}$, then

$$\phi(n) = \prod \phi(p_i^{\alpha_i}) = \prod_i \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right).$$

Another way of writing this is $\phi(p^\alpha) = p^\alpha \left(1 - \frac{1}{p}\right)$. Then

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

For reduced residue classes, we have

$$\begin{aligned} a_1 \pmod{n_1}, \quad a_2 \pmod{n_2} &\leftrightarrow a \pmod{n_1 n_2} \\ b_1 \pmod{n_1}, \quad b_2 \pmod{n_2} &\leftrightarrow b \pmod{n_1 n_2}. \end{aligned}$$

Then we see that

$$a_1 b_1 \pmod{n_1}, \quad a_2 b_2 \pmod{n_2} \leftrightarrow ab \pmod{n_1 n_2}.$$

So we've proved that $(\mathbb{Z}/n_1 n_2\mathbb{Z})^\times$ is isomorphic to the group $(\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times$. Therefore, $(\mathbb{Z}/n\mathbb{Z})^\times$ can be understood from the structure of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ for prime powers p^α.

Consider $(\mathbb{Z}/p\mathbb{Z})^\times$. Every element has order dividing $p - 1$. Does there exist an element of order $p - 1$?

4.2.3. *Primitive roots.*

Definition 4.2.2. A primitive root (mod n) is an element of $(\mathbb{Z}/n\mathbb{Z})^\times$ of order $\phi(n)$. This means that it generates $(\mathbb{Z}/n\mathbb{Z})^\times$.

Theorem 4.2.3. *There is a primitive root (mod n) if and only if $n = p^\alpha$ for an odd prime or $n = 2p^\alpha$ or $n = 2$ or $n = 4$.*

Lemma 4.2.4. *$(n_1, n_2) = 1$, g_1 is the order of $a \pmod{n_1}$, and g_2 is the order of $a \pmod{n_2}$, then the order of $a \pmod{n_1 n_2}$ is the lcm of g_1 and g_2.*

Proof. Note that the lcm works. So the order of $a \pmod{n_1 n_2}$ is g that divides $\operatorname{lcm}(g_1, g_2)$. Now, $a^g \equiv 1 \pmod{n_1}$ and $a^g \equiv 1 \pmod{n_2}$, so $g_1 \mid g$ and $g_2 \mid g$, which means that $\operatorname{lcm}(g_1, g_2) \mid g$. □

Proof of Theorem 4.2.3. Notice that $\phi(n)$ is almost always composite, because it is even. If $n_1, n_2 > 2$, then $\phi(n_1)$ and $\phi(n_2)$ are even, and $\operatorname{lcm}(\phi(n_1), \phi(n_2)) \leq \frac{1}{2}\phi(n_1)\phi(n_2)$. There are then no primitive roots (mod n).

Let's take it for granted that if n is a power of 2 larger than 4, then the structure is a little bit different. □

Example 4.2.5. Consider $561 = 3 \times 11 \times 17$. Then

$$\text{order} \mid \operatorname{lcm}(2, 10, 16) = 80,$$

while $80 \mid 560$.

Note that $(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

The plan will be the following:

(1) $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic
(2) "lift" primitive roots (mod p) to (mod p^2), etc.

5. 10/4

If $(n_1, n_2) = 1$, we clearly have that $(\mathbb{Z}/n_1n_2\mathbb{Z})^\times$ is isomorphic to $(\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times$.

5.1. **Primitive roots.**

Theorem 5.1.1 (Primitive roots)**.** *For any prime p, the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. So there is a element $g \pmod p$ with order $p-1$.*

This is an easy to understand group, as

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{g \pmod p, g^2 \pmod p, \cdots, g^{p-1} \pmod p\}.$$

If $p = 2$, this is easy because $(\mathbb{Z}/2\mathbb{Z})^\times$ has only one element. So we can assume that p is odd.

5.1.1. *Polynomial Congruences.* We want to consider polynomial congruences. In general, we look at a polynomial with integer coefficients $f(x) \in \mathbb{Z}[x]$, and we want to consider $f(x) \pmod p$. We say that a is a solution to the congruence $f(x) \equiv 0 \pmod p$ if $f(a) \equiv 0 \pmod p$. In fact, we can also consider congruences mod n where n is composite.

So far, we know how to solve one congruence: the linear case $f(x) = ax + b$. Considering this expression modulo p, we see that it has a unique solution if $(a, p) = 1$, and if $p \mid a$, then no solutions if $b \not\equiv 0 \pmod p$ and p solutions if $b \equiv 0 \pmod p$.

5.1.2. *Quadratic congruences.* The natural next step is to consider quadratic congruences. This is already hard.

The equation $x^2 - 1 \pmod p$ has two solutions when p is prime, while the equation $x^2 - 1 \pmod{15}$ has four solutions by the Chinese remainder theorem.

In addition, $x^2 + 1 \pmod 3$ has no solutions, $x^2 + 1 \pmod 5$ has two solutions, and hence $x^2 + 1 \pmod{15}$ has no solutions. This demonstrates that the solutions are not so easy to see.

We'll discuss this in more detail in the next few lectures. Most of the time, looking at a congruence mod p, you never get more solutions than the degree of the polynomial.

5.1.3. *Monic polynomials.* We consider polynomials with coefficient 1 by dividing out by the leading coefficient as long as it were coprime to the modulus. Look at polynomials of the form

$$f(x) = x^n a_{n-1}x^{n-1} + \cdots + a_0.$$

Lemma 5.1.2. *If $f(x)$ is monic of degree n (leading coefficient is coprime to p), then $f(x) \equiv 0 \pmod p$ has at most n solutions.*

Proof. If $n = 1$ then we're done. We will prove this by induction on n. Assume the induction hypothesis is that the lemma is true for degrees up to $n-1$. We need to prove this in degree n.

Suppose that $f(x)$ has $n+1$ solutions, so that $f(b_1), \ldots, f(b_{n+1}) \equiv 0 \pmod p$, where $b_1, \ldots, b_{n+1}$ are distinct residue classes.

Consider the polynomial of degree n $g(x) = (x - b_1) \ldots (x - b_n)$. This means that $g(x) = f(x)q(x) + r(x)$, where the remainder has degree less than n. Note that this means that $r(x)$

has solutions $b_1, \ldots, b_n$, but $r(b_{n+1}) \not\equiv 0 \pmod{p}$. This contradicts the induction hypothesis, so $f(x)$ must have at most n solutions and we're done. $\square$

5.1.4. *Back to primitive roots.* We go back to looking for primitive roots. If p is a prime, write $p-1 = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_r^{\alpha_r}$ where $q_1, \ldots, q_r$ are distinct primes.

Lemma 5.1.3. *There is an element $g \pmod{p}$ whose order is $q_j^{\alpha_j}$.*

Proof. Suppose that there is no element of order $q_j^{\alpha_j}$. Take any number $a \pmod{p}$ of order $g = q_1^{\beta_1} \ldots q_j^{\beta_j}$ dividing $p-1$, so $a^g \equiv 1 \pmod{p}$. Note that

$$\left(a^{\frac{p-1}{q_j^{\alpha_j}}} \right)^{q_j^{\beta_j}} \equiv 1 \pmod{p}.$$

If $q_j^{\beta_j}$ is the order of $a^{\frac{p-1}{q_j^{\alpha_j}}}$, but if the order if even smaller, you won't have enough powers of the q_j. This was a messy proof.

If there is no element of order $q_j^{\alpha_j}$, then for every $a \pmod{p}$, we have $a^{\frac{p-1}{q^{\alpha_j}}} \equiv 1 \pmod{p}$.

If g is the order of $a \pmod{p}$ and $q_j^{\alpha_j - 1} \mid g$ then $\beta_j < \alpha_j$ and this is true. But if $\beta_j = \alpha_j$, then by the preceding argument we have produced an element of order $q_j^{\alpha_j}$.

Consider $f(x) = x^{\frac{p-1}{q_j}} - 1$ has at most $\frac{p-1}{q_j}$ solutions. But we know that it is zero for every $(x, p) \equiv 1$, and that's a contradiction.

The notation is messy, but the idea is simple. Remove all of the j's and things will look better. $\square$

Lemma 5.1.4. *If a has order m and b has order n and $(m,n) = 1$, then ab has order mn.*

Proof. If $a^m \equiv 1 \pmod{p}$ then $a^{mn} \equiv 1 \pmod{p}$, and a similar argument holds for b to get $b^{mn} \equiv 1 \pmod{p}$, so $(ab)^{mn} \equiv 1 \pmod{p}$. So if g is the order of ab, then g divides mn. We want to show that $m \mid g$ and $n \mid g$.

We know that $(ab)^g \equiv 1 \pmod{1}$, so $(ab)^{gn} \equiv 1 \pmod{p}$, which means that $a^{gn} \equiv 1 \pmod{p}$, so $m \mid gn$ and hence $m \mid g$. The same holds for b. $\square$

There is therefore a primitive root $\pmod{p}$. We've proved that $(\mathbb{Z}/p\mathbb{Z})^\times$ has a generator $g \pmod{p}$.

What is the order of an element g^a? g^a is also a primitive root if $(a, p-1) = 1$. If $(a, p-1) \neq 1$, then the order is $\frac{p-1}{(a,p-1)}$.

What we've proved is that $(\mathbb{Z}/p\mathbb{Z})^\times$ is isomorphic to $(\mathbb{Z}/(p-1)\mathbb{Z})$. The number of primitive roots $\pmod{p}$ is $\phi(p-1)$.

If $d \mid p-1$, how many elements of order d are there? The elements of order d are of the form $g^{(\frac{p-1}{d})l}$ where $(d, l) = 1$. There are $\phi(d)$ elements with this order.

This also means that

$$\sum_{d \mid p-1} \phi(d) = p - 1.$$

In fact,

$$\sum_{d \mid n} \phi(d) = n.$$

To see this, write down the fractions $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$, and reduce each to lowest terms. The possible denominators are divisors of n, provides another representation to the previous sum.

Theorem 5.1.5. *If p is odd, there is a primitive root (mod p^α).*

Proof. First, we go from p to p^2. Take $g \pmod p$ to be a primitive root. We want to construct a primitive root (mod p^2). If we have an element $a \pmod{p^2}$, then $a_0 + a_1 p$ where $0 \le a_0, a_1 \le p-1$.

Starting with $g + kp \pmod{p^2}$, $0 \le k \le p-1$, we compute the order of $g + kp \pmod{p^2}$. If the order is r, then $(g+kp)^r \equiv 1 \pmod{p^2}$. $r \mid p(p-1)$, and $g^r \equiv 1 \pmod p$, but also $p-1 \mid r$. So $r = p-1$ or $r = p(p-1)$. Can it actually be equal to $p-1$?

We'll prove next time that for exactly one value of k, $g+kp$ will have order $p-1 \pmod{p^2}$, and for the remaining $p-1$ values, $g+kp$ will be a primitive root $\pmod{p^2}$.

□

6. 10/6

Midterm in two weeks: Wednesday week after next: October 20.

We have a polynomial $f(x) \in \mathbb{Z}[x]$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. We're interested in solutions to $f(x) \equiv 0 \pmod p$. We're really interested in the coefficients (mod p).

We proved:

Theorem 6.0.6. *If $(a_n, p) = 1$, then $f(x) \equiv 0 \pmod p$ has at most n solutions.*

Proof. Suppose not, then $b_1, \ldots, b_n$ are distinct solutions (mod p). Then $f(x) = a_n(a - b_1)(x-b_2)\ldots(x-b_n) = g(x)$ where $g(x)$ has degree $< n$. Then $g(b_1), \ldots, g(b_n) \equiv 0 \pmod p$. Contradiction unless all coefficients of g are $0 \pmod p$. But plug in $x = b_{m_1}$. □

Last time, this was drowned in notation.

Lemma 6.0.7. *If $q^\alpha \mid\mid p-1$ then there is an element $a \pmod p$ of order q^α.*

Proof. Suppose there is an element $b \pmod p$ of order $q^\alpha r$. Then b^r has order q^α. There is no element of order a multiple of q^α. So every element has order dividing $\frac{p-1}{q}$.

So $x^{\frac{p-1}{q}} \equiv 1 \pmod p$ has $p-1$ solutions. This is a contradiction. □

If $p - 1 = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_l^{\alpha_l}$, Then we get $a_i \pmod p$ of order $q_i^{\alpha_i}$. We multiply these together to get that $a_1 \ldots a_l$ has order $p-1$.

We have therefore proved that

Theorem 6.0.8. *$(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, and there is a primitive root (mod p).*

6.1. **Lifting.**

6.1.1. *Lift from p to p^2.* We will lift primitive roots (mod p) to primitive roots (mod p^2). We began this last time.

Consider a primitive root $g \pmod p$. There are p of them (mod p^2): $g + kp \pmod{p^2}$ where $0 \le k \le p-1$. These are the only candidates for a primitive root (mod p^2).

Exercise 6.1.1. If $g \pmod{p^2}$ is a primitive root, then $g \pmod p$ is a primitive root.

Solution. If $g^r \equiv 1 \pmod{p}$, then $g^r = 1 + ap$. Then $g^{rp} = (1+ap)^p \equiv 1 \pmod{p^2}$. The order of $g \pmod{p^2}$ is a multiple of r that divides rp.

The order of $g \pmod{p}$ is $p-1$, and the order of $g + kp \pmod{p}$ is $p-1$, so the order of $g \pmod{p^2}$ is a multiple of $p-1$ and a divisor of $p(p-1)$. So there are in fact only two choices: it could be $p-1$ or $p(p-1)$.

If $g^{p-1} \equiv 1 + ap$, then consider $(g+kp)^{p-1}$. We want to check if this is $1 \pmod{p^2}$. We can expand this using the binomial theorem:

$$\begin{aligned}(g+kp)^{p-1} &= g^{p-1} + \binom{p-1}{1}(kp)g^{p-2} + \binom{p-2}{2}(kp)^2 g^{p-3} + \cdots \\ &\equiv g^{p-1} + (p-1)kpg^{p-2} \equiv 1 + ap - kpg^{p-2} \pmod{p^2}.\end{aligned}$$

So we want to see if $a \equiv kg^{p-2} \pmod{p}$, or equivalently, $k \equiv ag \pmod{p}$.

Therefore, the order of $g \pmod{p^2}$ is $p-1$ for one value of k and it is $p(p-1)$ for $p-1$ values of k. So every primitive root $\pmod{p}$ gives $p-1$ primitive roots $\pmod{p^2}$. So we get at least $(p-1)\phi(p-1) = \phi(\phi(p^2))$ primitive roots.

6.1.2. *Lift from p^2 to p^3.* Suppose $g \pmod{p^2}$ is a primitive root and $g + kp^2 \pmod{p^3}$. The possible orders are $p^2(p-1)$ or $p(p-1)$. Now write $g^{p(p-1)} = 1 + bp^2$, and we want to understand $(g+kp^2)^{p(p-1)} \pmod{p^3}$. This comes from the binomial theorem:

$$(g+kp)^{p(p-1)} = g^{p(p-1)} + \binom{p(p-1)}{1} kp^2 g^{p(p-1)-1} \equiv g^{p(p-1)} \pmod{p^3}.$$

Could $g^{p(p-1)}$ have been $1 \pmod{p^3}$? Could b have been a multiple of p? We can write $g^{p-1} = 1 + ap$ and $p \nmid a$. Then

$$(g^{p-1})^p = 1 + \binom{p}{1}(ap) + \binom{p}{2}(ap)^2 + \cdots \equiv 1 + ap^2 \pmod{p^3}.$$

That means that $b \equiv a \pmod{p}$ is not a multiple of p.

So if $g \pmod{p^2}$ is a primitive root $\pmod{p^2}$, then $g + kp^2 \pmod{p^3}$ is a primitive root $\pmod{p^3}$ for every $0 \le k \le p-1$.

There are therefore $p(p-1)\phi(p-1) = \phi(\phi(p^3))$ primitive roots.

Hence, if p is an odd prime, there are $\phi(\phi(p^\alpha))$ primitive roots $\pmod{p^\alpha}$.

6.1.3. *Structure of $(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times$.* This is the same as the structure of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ by the Chinese Remainder Theorem.

Why did we have to assume that p is an odd prime? $(\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3 \pmod{4}\}$ is generated by 3. However, for $(\mathbb{Z}/8\mathbb{Z})^\times$, every element has order 1 or 2. This means that it is the Klein four group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. What is different in the proof?

If $\alpha \ge 3$, then $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ has size $2^{\alpha-1}$. Then 5 has order $2^{\alpha-2}$. Also include -1, and we can prove that $a \pmod{2}^\alpha$ is $\pm 5^j$ for some $1 \le j \le 2^{\alpha-2}$.

6.2. **Quadratic Congruences.** Consider $ax^2+bx+c \equiv 0 \pmod{p}$, where p is odd. There's not much to do for $p = 2$. We can also assume that $(a, p) = 1$. First, we complete the square:

$$\begin{aligned} 4a^2(ax^2 + bx + c) &\equiv 0 \pmod{p} \\ (2ax)^2 + 2(2a)bx + 4ac &\equiv 0 \pmod{p} \\ (2ax + b)^2 &\equiv b^2 - 4ac \pmod{p}. \end{aligned}$$

Therefore, it is sufficient to solve $y^2 \equiv d \pmod{p}$, where d is the discriminant $b^2 - 4ac$.

Definition 6.2.1. A residue class $a \pmod{p}$ is a called a *quadratic residue* if there are 2 solutions to $x^2 \equiv a \pmod{p}$ and a *nonresidue* if there are no solutions to the congruence. If $a \equiv 0 \pmod{p}$, then there is only one solution.

Definition 6.2.2. The *Legendre symbol* is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \pmod{p} \\ -1 & \text{if } a \text{ is a quadratic nonresidue} \pmod{p} \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

7. 10/11

We want to understand quadratic congruences (mod n), and it is sufficient to understand them (mod p); from that, simply use the Chinese Remainder Theorem.

We considered $ax^2 + bx + c \equiv 0 \pmod{p}$, p is odd, and $(a, p) = 1$. This reduced to solving $y^2 \equiv d \pmod{p}$, which led to the definitions of quadratic residue and Legendre symbol.

7.1. **Quadratic residues.** There are primitive roots $g \pmod{p}$, so for every $(n, p) = 1$, then $n \equiv g^a \pmod{p}$ for some a. From this, we see that if a is even, then n is a quadratic residue because $n \equiv (g^{a/2})^2 \pmod{p}$. If a is odd, then n is a quadratic nonresidue, since otherwise $g = (n^b)^2 \pmod{p}$.

From this, we see that the Legendre symbol is (completely) multiplicative, which means that $\left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{mn}{p}\right)$.

Proposition 7.1.1 (Euler's Criterion)**.** *If* $(n, p) = 1$ *then*

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p}.$$

Proof. Write $n \equiv g^k \pmod{p}$. If n is even, the left hand side is 1, which is congruent to the right hand side.

If n is odd, the LHS is -1, so we have

$$-1 \equiv g^{(2l+1)\frac{p-1}{2}} \equiv g^{(p-1)/2} \equiv -1 \pmod{p}.$$

□

Corollary 7.1.2.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{4}} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

This makes it easy to determine whether a number is a quadratic residue $\pmod p$.

We can produce a primality test. We want to see if n is prime. Pick any $a < n$, and check if $a^{n-1} \equiv 1 \pmod n$. If this $\not\equiv 1$, then n is composite. If $\equiv 1$, then we look at $a^{\frac{n-1}{2}} \equiv \pm 1$. If it is -1, we stop. If it is $+1$, see if $\frac{n-1}{2}$ is even and check if $a^{\frac{n-1}{4}} \equiv \pm 1$.

If a number n passes this test for any value of a, it is called a strong pseudoprime. Try a different a with this procedure. This is a very rapid process.

If the Generalized Riemann Hypothesis is true, then this algorithm works efficiently.

Theorem 7.1.3 (Gauss's Law of Quadratic Reciprocity)**.** *Given two primes p and q (different and odd), then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} 1 & \text{if either } p \text{ or } q \text{ is } 1 \pmod 4 \\ -1 & \text{if both } p \text{ and } q \text{ are } 3 \pmod 4. \end{cases}$$

This is a result that is theoretically interesting. It is not yet clear why it is an interesting or important fact. People are still looking for similar reciprocity laws in other cases. You'll have to trust me that it is interesting. It is not a useful computational tool.

The Legendre symbol $\pmod p$ has some properties:

(1) is periodic $\pmod p$
(2) is completely multiplicative

This is rather surprising, as it is not clear why such a function should exist. We'll later find all such functions that are periodic and multiplicative. This will be the crucial thing to prove Dirichlet's Theorem on producing primes in arithmetic progressions.

Example 7.1.4.

$$\begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \\ -1 & \text{if } n \equiv 3 \pmod 4 \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

Proof of Quadratic Reciprocity. Consider the reduced residue classes $1, 2, \ldots, \frac{p-1}{2}$, and multiply each of them by a to get the classes $a, 2a, \ldots, a\frac{p-1}{2}$. Suppose $1 \le j \le \frac{p-1}{2}$. We can make $aj \pmod p$ lie in the interval $[-\frac{p-1}{2}, \frac{p-1}{2}]$. There are now two cases.

$$aj = b_j \text{ or } -b_j \text{ with } 1 \le b_j \le \frac{p-1}{2}.$$

Now, consider $1 \le j \ne k \le \frac{p-1}{2}$. Can $b_j = b_k$? No, because $aj \not\equiv ak \pmod p$ and $aj \not\equiv -ak \pmod p$. So the b_j form a permutation of $[1, \frac{p-1}{2}]$.

Lemma 7.1.5.

$$a^{\frac{p-1}{2}} \equiv (-1)^{\#\text{ times we get } -b_j}$$

Proof.

$$\prod_{j=1}^{(p-1)/2} j = a^{(p-1)/2} \prod_{j=1}^{(p-1)/2} j \equiv \prod_{j=1}^{(p-1)/2} \pm b_j.$$

□

Note that the number of times we get $-b_j$ is equal to the number of times that $aj \pmod p$ lies in $[\frac{p+1}{2}, p-1]$. We don't really care about this number; just whether it's even or odd.

Now,

$$aj = \left\lfloor \frac{aj}{p} \right\rfloor + r.$$

There are two cases: $r = b_j$ or $r = p - b_j$. If it is $+b_j$, then it has the same parity as b_j; if it is $-b_j$, then it has the opposite parity as b_j.

We can now compute

$$\begin{aligned}\sum_{j=1}^{\frac{p-1}{2}} a_j &= \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{aj}{p} \right\rfloor + \sum_{j=1}^{\frac{p-1}{2}} r_j = p\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{aj}{p} \right\rfloor + (\#\text{ of } -b_j \text{ terms}) + \sum_{j=1}^{\frac{p-1}{2}} j \\ &\equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{aj}{p} \right\rfloor + \sum_{j=1}^{\frac{p-1}{2}} j + (\#\text{ of } -b_j \text{ terms}) \pmod 2.\end{aligned}$$

Now,

$$(\#\text{ of } -b_j \text{ terms}) \equiv a\frac{\frac{p-1}{2}\frac{p+1}{2}}{2} - \frac{\frac{p-1}{2}\frac{p+1}{2}}{2} + \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{aj}{p} \right\rfloor = \frac{p^2-1}{8}(a-1) + \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{aj}{p} \right\rfloor \pmod 2.$$

Corollary 7.1.6.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv -1 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases}$$

Proof. Take $a = 2$ above, and we get that

$$(\#\text{ of } -b_j \text{ terms}) = \frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{2j}{p} \right\rfloor = \frac{p^2-1}{8}.$$

□

Now,

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p^2-1}{8}(q-1) + \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor} = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor}.$$

Similarly,

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{pk}{q} \right\rfloor},$$

so their product is

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = h(-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{pk}{q} \right\rfloor}.$$

We need one final trick. Consider all numbers of the form $qj - pk$ where $1 \le j \le \frac{p-1}{2}$ and $1 \le k \le \frac{q-1}{2}$.

There are $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ nonzero integers. Some are positive and some are negative. How many positive numbers are there? For it to be positive, we need $qj > pk$. Given j, there are $\left\lfloor \frac{qj}{p} \right\rfloor$ such values of k. The total positive values are therefore

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor.$$

The negative values come from $qj < pk$. Given k, the number of j is $\left\lfloor \frac{pk}{q} \right\rfloor$, so the total negative values is

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{pk}{q} \right\rfloor.$$

So

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{pk}{q} \right\rfloor}. = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

□

Remark. This was not the most intuitive proof, but it doesn't require much machinery to set up. There are more intuitive proofs. For example, we want to work with congruences of things other than integers. Here,

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

might hold for algebraic integers a and b, i.e. where a and b are solutions to monic polynomial equations with integer coefficients.

There are nice algebraic integers that you can construct; these are called Gauss sums:

$$\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e^{\frac{2\pi i n}{p}}.$$

These are also algebraic integers. Now we can do ingenious things:

$$\left(\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e^{\frac{2\pi i n}{p}}\right)^q \equiv \sum \left(\frac{n}{p}\right)^q = \left(\frac{q}{p}\right) \sum \left(\frac{nq}{p}\right) e^{\frac{2\pi i n q}{p}} = \left(\frac{q}{p}\right) \left(\sum \left(\frac{m}{p}\right) e^{\frac{2\pi i n q}{p}}\right).$$

Therefore,

$$\left(\frac{q}{p}\right) \equiv (\text{Gauss sum})^{q-1} \pmod{p}.$$

8. 10/13

We now know how to solve any quadratic congruence $ax^2 + bx + c \pmod{p}$. This leads to computing $\left(\frac{d}{p}\right)$, $d = b^2 - 4ac$.

We know a variety of facts about the Legendre symbol. In particular, it gives statements of the form

$$\left(\frac{d}{p}\right) = \begin{cases} 1 & \text{if } p \text{ lies in some residue classes } (\text{mod } 4|d|) \\ -1 & \text{if } p \text{ lies in some other residue classes } (\text{mod } 4|d|) \end{cases}$$

Example 8.0.7.

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 4 \pmod 5) \\ -1 & \text{if } p \equiv 2, 3 \pmod 5) \end{cases}$$

$$\left(\frac{7}{p}\right) = \begin{cases} \left(\frac{p}{7}\right) & \text{if } p \equiv 1 \pmod 4) \\ -\left(\frac{p}{7}\right) & \text{if } p \equiv 3 \pmod 4), \end{cases}$$

which leads to conditions on $p \pmod{28}$.

Figure out what happens when $d = 35$.

8.1. **Absolute Values in $\mathbb{Q}$.** We'll talk about some pretty theorems. There's a completely different way where primes appear. This has to do in some way with analysis. If you think about real analysis, it is based on the notion of distance between two numbers, which is based on absolute value. This has some nice properties: $|xy| = |x||y|$ and $|x + y| \leq |x| + |y|$.

The questions that we want to think about involve the field $\mathbb{Q}$ of rational numbers.

Definition 8.1.1. An absolute value on $\mathbb{Q}$ is a function $f : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ with the following properties:

(1) $f(x) = 0$ iff $x = 0$
(2) $f(xy) = f(x)f(y)$ for all $x, y \in \mathbb{Q}$
(3) $f(x + y) \leq f(x) + f(y)$ (triangle inequality).

Example 8.1.2. The trivial absolute value: $f(0) = 0$, $f(x) = 1$ for all $x \neq 0$.

Example 8.1.3. $f(x) = |x|$ satisfies these properties. $f(x) = |x|^\alpha$ does too when $0 < \alpha \leq 1$. The conditions on α come from the triangle inequality. We want to check that

$$x^\alpha + y^\alpha \geq (x + y)^\alpha.$$

If we take $x = y$ then we want $2 > 2^\alpha$, so clearly $\alpha < 1$. To show our condition, divide both sides by y^α to reduce the inequality to $t^\alpha + 1 \geq (t+1)^\alpha$, which is a problem in single variable calculus.

There are another class of examples that come from primes.

Example 8.1.4. p-adic absolute value. Let p be a prime. Consider $n \in \mathbb{N}$, and write $n = p^\alpha b$. Here, $p^\alpha || n$, so $p \nmid b$, $\alpha \geq 0$.

Define the p-adic absolute value as

$$|n|_p = p^{-\alpha},$$

and additionally, define $|-1|_p = 1$.

If we have a rational number $\frac{m}{n}$, define

$$\left|\frac{m}{n}\right|_p = \frac{|m|_p}{|n|_p}.$$

Multiplicativity is obvious. We need to check the triangle inequality. For simplicity, we do this for the integers. Suppose that $n_1 = p^{\alpha_1} b_1$, $n_2 = p^{\alpha_2} b_2$. We want to show that

$$|n_1 + n_2|_p \leq |n_1|_p + |n_2|_p.$$

Note that $|n_1|_p = p^{-\alpha_1}$, $|n_2|_p = p^{-\alpha_2}$, and $|n_1 + n_2|_p \leq p^{-\min(\alpha_1,\alpha_2)} = \max(p^{-\alpha_1}, p^{-\alpha_2})$. So the triangle inequality is true, and indeed, we've shown something stronger:

$$|n_1 + n_2|_p \leq \max(|n_1|_p, |n_2|_p).$$

To check the triangle inequality for rational numbers, we can extend the previous argument by clearing denominators.

We needed p to be prime, because otherwise the multiplicativity fails.

With the normal absolute value, the absolute value of the rational numbers form a dense set in $\mathbb{R}$. In this case, however, the image is $|\mathbb{Q}|_p = \{p^n : n \in \mathbb{Z}\}$.

Strangely, $p, p^2, p^3, \ldots$ is small while $\frac{1}{p}, \frac{1}{p^2}, \ldots$ are large.

Example 8.1.5. As in the case of the usual absolute value, we can raise this to a power $|x|_p^\alpha$. With our new triangle inequality, we see that the triangle inequality is satisfied whenever $\alpha > 0$.

Theorem 8.1.6 (Ostrowski)**.** *These are all of the absolute values on $\mathbb{Q}$.*

Proof. Let f be an absolute value on $\mathbb{Q}$. Note that multiplicativity implies that $f(1) = 1$. Then $f(n) \leq n$ by the triangle inequality.

If we consider values of $f(n)$, $n \in \mathbb{N}$, there are two cases: all are ≥ 1, or at least one of them is < 1. We want to show that they come from the normal absolute value and the p-adic absolute value respectively.

Case 1: Pick the smallest $n \in \mathbb{N}$ with $f(n) < 1$. Then by minimality, $n = p$ is prime.

Consider $r \in \mathbb{N}$, and take its base p expansion

$$r = b_0 + b_1 p + b_2 p^2 + \cdots + b_s p^s,$$

$0 \leq b_j \leq p - 1$. Then

$$f(r) \leq f(b_0) + f(b_1) + \cdots + f(b_s) \leq (p-1)(s+1) \leq (p-1)\left(\frac{\log r}{\log p} + 1\right).$$

Now,

$$f(r^k) = f(r)^k \leq (p-1)\left(\frac{k \log r}{\log p} + 1\right),$$

so

$$f(r) \leq (p-1)^{1/k}\left(\frac{k \log r}{\log p} + 1\right)^{1/k}.$$

As $k \to \infty$, we conclude that $f(r) \leq 1$.

We want to show that if $(r, p) = 1$ then $f(r) = 1$. If $(r, p) = 1$, then $(r^k, p^k) = 1$. By the Euclidean algorithm, we can write $1 = r^k x + p^k y$. This means that $1 \leq f(r^k x) + f(p^k y) \leq f(r)^k + f(p)^k$. Let $k \to \infty$. If $f(r) < 1$ then the right hand side goes to 0 as $k \to \infty$, a contradiction.

We now know that p is a prime for which $f(p) < 1$, and $f(n) = 1$ if $(n, p) = 1$. But this tells us everything. Take any $n = p^a b$. Then

$$f(n) = f(p)^a f(b) = f(p)^a.$$

Write $f(p) = p^{-\alpha}$, $\alpha > 0$. Then $f(p) = |p|_p^\alpha$, and we get that $f(n) = |n|_p^\alpha$.

Case 2: Now, we consider the case when $f(n) \geq 1$ for all $n \in \mathbb{N}$. Pick two numbers $m, n \in \mathbb{N}$, $m, n > 1$. Write m in base n:

$$m = b_0 + b_1 n + b_2 n^2 + \cdots + b_s n^s.$$

Then $f(m) \leq (f(b_0) + f(b_1) + \cdots + f(s)) f(n)^s < (s+1)(n-1) f(n)^s$, where $s \approx \frac{\log m}{\log n}$.

Now,

$$f(m^k) \leq \left(1 + \frac{k \log m}{\log n}\right)(n-1) f(n)^{\frac{\log m}{\log n}}.$$

Take k-th roots, and let $k \to \infty$. Then

$$f(m) \leq f(n)^{\frac{\log m}{\log n}},$$

so what we've shown is that

$$f(m)^{\frac{1}{\log m}} \leq f(n)^{\frac{1}{\log n}}.$$

If we swap m and n, we see that

$$f(m)^{\frac{1}{\log m}} = f(n)^{\frac{1}{\log n}}.$$

If we write $f(2) = 2^\alpha$, then $f(2)^{\frac{1}{\log 2}} = f(n)^{\frac{1}{\log n}}$, and we get $f(n) = n^\alpha$. The triangle inequality forces $0 < \alpha \leq 1$. □

Remark. From the rational numbers, we can take the completion: we can obtain $\sqrt{2}$ as the limit of rational numbers, but it is not a rational number itself. So we can extend this absolute value continuously from the rational numbers to the real numbers. We can now do the same thing with this p-adic absolute value. Think of taking sequences of rational numbers and consider convergence in the p-adic absolute value.

Example 8.1.7. $1, 1+7, 1+7+7^2, 1+7+7^2+7^3, \ldots$ is a sequence of integers. Does this sequence converge? No for the usual absolute value, but it does converge for $|\cdot|_7$. It forms a Cauchy sequence, and it converges to $\frac{1}{1-7} = -\frac{1}{6} = 1 + 7 + 7^2 + 7^3 + \cdots$.

In fact, we can even consider $\sqrt{-1}$ in the 5-adics. We want to find a sequence $x_1, x_2, \ldots$ of natural numbers with $|x_n^2 + 1|_5 \to 0$.

Since $2^2 + 1 \equiv 0 \pmod 5$, we have $|2^2 + 1|_5$. We can lift 2 to $2 + k \cdot 5$, and get congruences $\pmod{p^2}$, $\pmod{p^3}$, etc, yielding a converging sequence.

9. 10/18

9.1. **Sum of Two Squares.** We'll try to describe all numbers that can be written as the sum of two squares, and we'll give two or three proofs of this.

Given a number n, we want to write $n = x^2 + y^2$, $x, y \in \mathbb{Z}$. We want a characterization of all such n. Here's the main theorem:

Theorem 9.1.1. *$n = x^2 + y^2$ if and only if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ such that if $p_j = 3 \pmod 4$ then α_j is even.*

Let's try to see why this condition is necessary. It is more difficult to show that it is sufficient.

Proof. First, we show that the condition is *necessary*:

Suppose that n is not of this form and n is the sum of two squares. So $p^{2\beta+1}||n$, $p = 3 \pmod 4$. Then $x^2 + y^2 \equiv 0 \pmod p$ and hence $x^2 = -y^2 \pmod p$, and if $(y, p) = 1$, this means that $(x/y)^2 = -1 \pmod p$, but -1 is a quadratic nonresidue (mod p).

So y is a multiple of p and x is a multiple of p, so $x^2 + y^2$ is a multiple of p^2; cancel p^2 and repeat.

Now, we show that the condition is *sufficient*:

First, if $m = x_1^2 + y_1^2$ is the sum of two squares and $n = x_2^2 + y_2^2$ is the sum of two squares then mn is the sum of two squares. Here,

$$m = (x_1 + iy_1)(x_1 - iy_1) \quad n = (x_2 + iy_2)(x_2 - iy_2)$$

so that

$$mn = (x_1x_2 - y_1y_2 + i(x_1y_2 + x_2y_1))(x_1x_2 - y_1y_2 - i(x_1y_2 + x_2y_1)).$$

If $p \equiv 3 \pmod 4$, we showed that it isn't the sum of two squares. But $p^2 = p^2 + 0^2$ is the sum of two squares, which means that all even powers of p is the sum of two squares. So the main fact that we want to show is the following theorem:

Theorem 9.1.2 (Fermat)**.** *If $p \equiv 1 \pmod 4$, then $p = x^2 + y^2$.*

Proof 1. If $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = 1$. This means that $p^2+1 \equiv 0 \pmod p$. So if we look at the set of all sums of two squares, it contains multiples of p smaller than p^2. If $l^2 + 1 \equiv 0 \pmod p$, we can take $|l| < \frac{p-1}{2}$, so hence $l^2 + 1^2 \leq (\frac{p-1}{2})^2 + 1 < p^2$.

Suppose that pm is the smallest multiple of p which is the sum of two squares, and we can assume that $m < p$. Then $pm = x^2+y^2$. Suppose that $x \equiv \overline{x} \pmod m$ and $y \equiv \overline{y} \pmod m$, where $|\overline{x}|, |\overline{y}| \leq \frac{m}{2}$. Then $\overline{x}^2 + \overline{y}^2 \equiv mn$ and $n < \frac{m}{2}$.

Now, $mn = \overline{x}^2 + \overline{y}^2$ and $pm = x^2 + y^2$, so $pm \cdot mn = pm^2n$ is the sum of two squares. With the identity from the beginning of our proof, this means that

$$pm \cdot mn = pm^2n = (x\overline{x} + y\overline{y})^2 + (x\overline{y} - \overline{x}y)^2.$$

Since the second term is $0 \pmod m$, we see that the first term is also $0 \pmod m$. This means that we can cancel m^2 everywhere, so pn is the sum of two squares, contradicting the minimality assumption for m. □

Proof 2. As before, we get $l^2+1 \equiv 0 \pmod p$, $|l| \leq \frac{p-1}{2}$. Consider $p = x^2+y^2$. If $x^2+y^2 \equiv 0 \pmod p$, take $y = xl \pmod p$, so we get $x^2 + l^2x^2 \equiv 0 \pmod p$.

Search numbers of the form $x^2 + (lx)^2$. We are interested in $(x \pmod p, (lx) \pmod p)$. What we want is $x \pmod p$ is smaller than $\sqrt{p}$, and $lx \pmod p$ smaller than $\sqrt{p}$. This is enough: Then $x^2 + (lx)^2 < 2p$ and it is a multiple of p, so it is equal to p.

Now, for each of $1 \leq x \leq \sqrt{p}$, we want that $|lx - kp| < \sqrt{p}$, so we want

$$\left|\frac{l}{p} - \frac{k}{x}\right| < \frac{1}{\sqrt{p}x}.$$

This is a problem that we can solve with the pigeonhole principle; it is guaranteed by Dirichlet's Theorem.

Theorem 9.1.3 (Dirichlet's Theorem on Diophantine Approximation)**.** *Given a real number θ, find a rational number $\frac{a}{q}$ which approximates θ, with $q \leq Q$ and*

$$\left|\theta - \frac{a}{q}\right| < \frac{1}{qQ}.$$

Proof. Look at $0, \theta, 2\theta, \ldots, Q\theta \pmod 1$, i.e. subtract out the integer part and just keep the fractional part. There are $Q+1$ numbers here. Look at the Q boxes

$$\left[0, \frac{1}{Q}\right), \left[\frac{1}{Q}, \frac{2}{Q}\right), \cdots, \left[\frac{Q-1}{Q}, 1\right).$$

By the pigeonhole principle, there exist $0 \leq j < k \leq Q$ with the two numbers $j\theta$ and $k\theta$ lying in the same box.

This means that $j\theta - k\theta$ has fractional part less than $\frac{1}{Q}$. Then

$$\theta = \frac{\text{integer}}{j-k} + \text{error}, \quad |\text{error}| \leq \frac{1}{Q(j-k)}.$$

□

Remark. If you are given an irrational number θ, there are infinitely many q with

$$\left|\theta - \frac{a}{q}\right| \leq \frac{1}{q^2}.$$

□

□

9.2. $\mathbb{Z}[i]$**.** We will do arithmetic in the Gaussian ring of integers $\mathbb{Z}[i]$. Here,

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

This is nice, but we can't divide. Allowing division, we obtain

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}.$$

Units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$. One thing that clarifies a lot of stuff is the norm. Define the norm as

$$N(a+bi) = a^2 + b^2 = (a+bi)(a-bi).$$

This has various nice properties. For example, $N(a+bi)$ is a positive rational number, and if $a + bi \in \mathbb{Z}[i]$ then the norm is an integer. Furthermore,

$$N((a+bi)(c+di)) = N(a+bi)N(c+di).$$

If $u \in \mathbb{Z}[i]$ and $\frac{1}{u} \in \mathbb{Z}[i]$, then u is called a unit. This means that $N(u) = 1$, so $u = \pm 1, \pm i$ are the only units.

If π is a prime, $\pi \mid \alpha\beta$ implies that $\pi \mid \alpha$ or $\pi \mid \beta$. Here, $\alpha \mid \beta$ if $\beta = \alpha\gamma$ with $\gamma \in \mathbb{Z}[i]$.

α is irreducible if $\alpha = \beta\gamma$ implies one of β or γ is a unit. This means that α is irreducible if it can't be written as a product of two numbers with smaller norm. Suppose $N(\alpha) = p$, then α is irreducible.

Example 9.2.1. $2 + i$ is irreducible. 7 is irreducible because if $7 = \alpha\beta$, then $N(7) = 49 = N(\alpha)N(\beta)$, which means that $N(\alpha) = 7$, which is impossible because 7 is not the sum of the two squares.

The question we want to ask is: Is there a division algorithm? If we want to divide, we want to write as a quotient plus some remainder. Here,

$$\frac{a+bi}{c+di} = \rho + \sigma i,$$

with $\rho, \sigma \in \mathbb{Q}$. Pick r and s to be the closest integers to ρ and σ. Then the quotient is $r+si$. We need to show that the remainder has smaller norm than the number I divide by. This isn't too hard to do.

10. 10/25

Recall the theorem of Fermat that $p \equiv 1 \pmod 4$ means that p can be written by the sum of two squares. We already gave two proofs of this. The first was by looking at minimal multiples of p as the sum of two squares, and the second was by Dirichlet's theorem on Diophantine approximation. We started looking at a third proof: The arithmetic of $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$, which sits naturally in the field $\mathbb{Q}(i) = \{a+bi : a, b \in \mathbb{Q}\}$.

10.1. $\mathbb{Z}[i]$**.** Here, the norm of $a+bi \in \mathbb{Q}(i)$ is $N(\alpha) = a^2+b^2 = \alpha\overline{\alpha}$. Note that $N(\alpha\beta) = N(\alpha)N(\beta)$.

$\alpha \in ZZ[i]$ is a unit if $\frac{1}{\alpha} \in \mathbb{Z}[i]$. If $\alpha \in \mathbb{Z}[i]$, then $N(\alpha) \in \mathbb{N}$ (could be zero if $\alpha = 0$), so if α is a unit, $N(\alpha) = 1$, and the only units are $\alpha = \pm 1, \pm i$.

$\alpha \mid \beta$ if $\beta = \alpha\gamma$ for some $\gamma \in \mathbb{Z}[i]$. $\alpha \in \mathbb{Z}[i]$ is irreducible if $\alpha = \beta\gamma$ for $\beta, \gamma \in \mathbb{Z}[i]$ implies that β or γ is a unit. Equivalently, $\alpha \neq \beta\gamma$ with $1 < N(\beta), N(\gamma) < N(\alpha)$.

If $N(\alpha) = p$ (i.e. α is a rational prime) then α is irreducible. For example, $1+2i \in \mathbb{Z}[i]$ is irreducible, as are $1-2i$, $1+i$, $3+2i$. But there are other irreducibles too. If $p \equiv 3 \pmod 4$, then p is irreducible in $\mathbb{Z}[i]$.

Proof. Suppose that p is irreducible, and $p = \alpha\beta$, so $N(\alpha)N(\beta) = p^2$, and so $N(\alpha) = N(\beta) = p$. But then $p = a^2+b^2$, contradicting $p \equiv 3 \pmod 4$. □

Note that $5 = (1+2i)(1-2i)$ and $2 = (1+i)(1-i) = (1+i)^2(-i)$, so these are not irreducible.

Our aim is to show that if $p \equiv 1 \pmod 4$ then $p = \pi\overline{\pi}$ where $N(\pi) = p$ and π is irreducible.

π is prime means that if $\pi \mid \alpha\beta$ then $\pi \mid \alpha$ or $\pi \mid \beta$. What we would like to prove is

Theorem 10.1.1. *In $\mathbb{Z}[i]$, every irreducible is prime and conversely.*

Proof. In the case of the integers, we used the division algorithm. We want to do something similar here.

Note that the converse is easy: If π is prime and $\pi = \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$. Then $N(\alpha) \geq N(\pi)$ or $N(\beta) \geq N(\pi)$. This implies that $N(\alpha) = N(\pi)$ and $N(\beta) = 1$, or the other way around, so π is irreducible.

10.1.1. *Division algorithm.* Given $\alpha, \beta \in \mathbb{Z}[i]$, we can write $\alpha = \beta\gamma + \delta$, where γ is the quotient and δ is the remainder. We want to be able to do this with $0 \leq N(\delta) \leq N(\beta)$.

Proof. Take $\frac{\alpha}{\beta} = \rho + \sigma i$, $\rho, \sigma \in \mathbb{Q}$. Take r and s to be integers with $-\frac{1}{2} < \rho - r < \frac{1}{2}$ and $-\frac{1}{2} < \sigma - s < \frac{1}{2}$.

Then take $\gamma = r + si$. Then $\delta = ((\rho - r) + (\sigma - s)i)\beta$. Then

$$N(\delta) = N(\beta)((\rho - r)^2 + (\sigma - s)^2) < \frac{1}{2}N(\beta).$$

□

10.1.2. *Euclidean algorithm.* Our aim is to understand the common factors of α and β. Then write $\alpha = \beta\gamma + \delta$ and $\beta = (\cdots)\delta + (\cdots)$. This is nice because it always terminates because of the division algorithm.

We can express the "greatest common divisor" of α and β as a linear combination $\alpha x + \beta y$ where $x, y \in \mathbb{Z}[i]$.

10.1.3. *Finishing the proof.* We can now show that if π is irreducible, $\pi \mid \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$. Suppose that $\pi \nmid \alpha$. Then the only common factors of π and α are units $\pm 1, \pm i$. By the Euclidean algorithm, we can therefore write $1 = \alpha x + \pi y$. Then $\beta = \alpha\beta x + \beta\pi y$. Therefore, $\pi \mid \beta$. □

Theorem 10.1.2. *$p \equiv 1 \pmod 4$ then $p = x^2 + y^2$ is the sum of two squares.*

Proof. We want to show that p is reducible, as then we could write $p = \pi\overline{\pi}$, and then $N(\pi) = N(\overline{\pi}) = x^2 + y^2 = p$.

So suppose that p is irreducible, which is equivalent to saying that p is prime. We know that there is l such that $l^2 + 1 \equiv 0 \pmod p$. This is simply the fact that -1 is a quadratic residue (mod p). This means that $p \mid (l+i)(l-i)$, so $p \mid l+i$ or $p \mid l-i$. But these are both impossible, i.e. $l + i = p(a + bi)$ means that $l = pa$ and $1 = pb$ is impossible. So $p = \pi\overline{\pi}$ is in fact reducible, and we're done. (Note that π and $\overline{\pi}$ are primes in $\mathbb{Z}[i]$ because they have norm p. □

10.2. **Arithmetic of $\mathbb{Z}[i]$.** There is unique factorization into primes (up to units and ordering of the primes). This is the same proof as in the case of the integers (cancel them).

The primes in $\mathbb{Z}[i]$ are rational primes $p \equiv 3 \pmod 4$. If $p \equiv 1 \pmod 4$, then $p = \pi\overline{\pi}$ splits as the product of two primes, and $2 = (1+i)^2(-i)$. Here, 2 is special because $1 - i = -i(1+i)$, so $1 - i$ and $1 + i$ are actually the same prime.

Instead of $\mathbb{Z}[i]$, we could try to do the same thing in $\mathbb{Q}(\sqrt{-5})$, where we consider $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. Here, $N(a + b\sqrt{-5}) = a^2 + 5b^2$, and we're hopeful that we can repeat what we did earlier. Here, the units are ± 1, and 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all irreducible, but $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, and there is no unique factorization.

Here, the division algorithm fails because the remainder is too big. This means that the Euclidean algorithm may not terminate.

In $\mathbb{Q}(\sqrt{14})$, there is unique factorization, but there is no Euclidean algorithm.

There are imaginary quadratic fields $\mathbb{Q}(-\sqrt{d})$, $d > 0$. There are exactly 9 values of d where one gets unique factorization into irreducibles. The largest example is $\mathbb{Q}(-\sqrt{163})$. This is connected to the fact observed by Euler that $n^2 + n + 41$ is prime when $n = 0, 1, 2, \ldots, 39$, and the discriminant of this is -163. There is no better quadratic.

In the integers,

$$\{ax + by\} = \{gx : x \in \mathbb{Z}\}$$

where $g = \gcd(a, b)$. Something similar is true in $\mathbb{Z}[i]$:

$$\{\alpha x + \beta y\} = \{\gamma x\}.$$

This relates to the idea of an ideal, which corresponds to what is sounds like: ideal integers. If $\alpha, \beta \in I$, then $\alpha x + \beta y \in I$t for all $x, y \in R$. For example, in $\mathbb{Z}$, (7) is an ideal. In some sets, every ideal is generated by one number; in other sets, this is not true. For example, in $\mathbb{Z}[\sqrt{-5}]$, $(2x + (1 + \sqrt{-5})y)$ is an ideal that is not principal.

11. 10/27

We will move on to the big theorem that we will prove in the rest of the course.

Theorem 11.0.1 (Dirichlet's Theorem on Primes in Arithmetic Progressions)**.** *If* $(a, p) = 1$*, then any arithmetic progression* $a \pmod q$ *contains infinitely many primes.*

This is a very simple sounding statement, but the proof is not so simple. This will take around three weeks for us to prove. We'll build up a proof and do this case by case.

Before we consider the main idea of the proof, let's look at a case you've already handled. We can prove that there are infinitely many primes $\equiv 1 \pmod 4$ and infinitely many primes $\equiv 3 \pmod 4$. The case of $1 \pmod 4$ was on the homework, using our knowledge about sum of two squares.

For the case of $3 \pmod 4$, we have primes $p_1, p_2, \ldots, p_n$. Then $4p_1p_2 \ldots p_n - 1$ must be divisible by a new prime $\equiv 3 \pmod 4$.

Similarly, in the spirit of Euclid, we can prove that there are infinitely many primes that are $\equiv 1 \pmod 3$ and $\equiv -1 \pmod 3$. This will be on the next problem set.

This trick fails for $-1 \pmod 5$, however, as $5p_1p_2 \ldots p_n - 1$ could be pq with $p \equiv q \equiv 2 \pmod 5$.

11.1. **Euler's proof of the infinitude of primes.** This is based on the fact that $\sum \frac{1}{p}$ diverges. This can be seen from $\sum \frac{1}{p^\sigma}$ for $\sigma > 1$. This converges, but we'd like to say that this tends to infinity as $\sigma \to 1^+$.

A nice way to think about this is to consider the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

For example, if s is real, $s > 1$, this series converges absolutely. If we think of $s = \sigma + it$ as a complex number, we have

$$\frac{1}{n^s} = \frac{1}{n^\sigma} \frac{1}{n^{it}}$$

The final term has absolute value 1, so

$$\left| \frac{1}{n^s} \right| = \frac{1}{n^\sigma}.$$

So $\zeta(s)$, $s = \sigma + it$, converges absolutely for $\sigma > 1$.

The Riemann zeta function has a very natural connection with prime numbers. For every natural number, we can factor it into primes in an unique way. Then

$$\prod_p \left(1 + \frac{1}{p^\sigma} + \frac{1}{p^{2\sigma}} + \frac{1}{p^{3\sigma}} + \cdots \right) = \sum_{n=1}^{\infty} \zeta(s).$$

This identity is due to Euler, and it is a form of unique factorization.

It isn't obvious what it means for a product to converge. Suppose we have

$$\prod_{n=1}^{\infty}(1+a_n).$$

If a_n is small, then $1+a_n \approx e^{a_n}$. Then $\prod(1+a_n) \approx e^{\sum a_n}$, so for the product to converge, we might want the sum of a_n to converge. We make this more formal.

Definition 11.1.1.

$$\prod_{n=1}^{\infty}(1+a_n)$$

converges absolutely if

$$\sum_{n=1}^{\infty}|a_n|$$

converges.

We can certainly say that $1+a_n = \exp(a_n + O(a_n)^2)$. If we assume that $\sum a_n$ converges, then the product makes sense.

Suppose that we take

$$\prod_{n=2}^{\infty}\left(1-\frac{1}{n}\right).$$

The partial products are $\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{3}{4}\cdots\frac{N-1}{N} = \frac{1}{N} \to 0$ as $n \to \infty$, but the product does not converge absolutely. If a product converges absolutely, then it is not zero unless one of the terms in the product is zero.

Let's look back to the product in the zeta function. This product does converge absolutely because $\sum \frac{1}{p^\sigma}$ converges. Then

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_p\left(1+\frac{1}{p^s}+\frac{1}{p^{2\sigma}}+\cdots\right) = \prod_p \frac{1}{1-\frac{1}{p^s}} = \prod_p\left(1-\frac{1}{p^s}\right)^{-1}.$$

This product converges absolutely if $s > 1$, or $\Re s > 1$, and converges is this range to a nonzero value.

Why does this prove that there are infinitely many primes? Suppose that there are finitely many primes. Then the right hand side remains bounded as $\sigma \to 1^+$. However, as $\sigma \to 1^+$,

$$\zeta(\sigma) = \sum_{n=1}^{\infty}\frac{1}{n^\sigma} \geq \int_1^2 \frac{dt}{t^\sigma} + \int_2^3 \frac{dt}{t^\sigma} = \int_1^\infty \frac{dt}{t^\sigma} = \frac{1}{\sigma-1}.$$

On the other hand,

$$\zeta(\sigma) \leq 1 + \int_1^2 \frac{dt}{t^\sigma} + \int_2^3 \frac{dt}{t^\sigma} + \cdots \leq \frac{1}{\sigma-1} + 1.$$

Proposition 11.1.2. *For $\sigma > 1$,*

$$\zeta(\sigma) = \frac{1}{\sigma-1} + O(1)\left[= \frac{1}{\sigma-1} + \gamma + c_1(\sigma-1) + \cdots\right]$$

We can then write

$$\log \zeta(\sigma) = -\sum_p \log\left(1 - \frac{1}{p^\sigma}\right).$$

Using

$$-\log(1-x) = \sum_{k=1}^{\infty} \frac{x^k}{k},$$

we have

$$\log \zeta(\sigma) = \sum_p \sum_{k=1}^{\infty} \frac{1}{kp^{k\sigma}} = \sum_p \left(\frac{1}{p^\sigma} + O\left(\frac{1}{p^{2\sigma}}\right)\right).$$

Now,

$$\sum_{k=2}^{\infty} \frac{1}{kp^{k\sigma}} \leq \sum_{k=2}^{\infty} \frac{1}{2p^{k\sigma}} = \frac{1}{2p^{2\sigma}} \frac{1}{1 - \frac{1}{p^\sigma}} = O\left(\frac{1}{p^{2\sigma}}\right).$$

Therefore, we have

Proposition 11.1.3.

$$\log \zeta(\sigma) = \sum_p \sum_{k=1}^{\infty} \frac{1}{kp^{k\sigma}} = \frac{1}{p^\sigma} + O(1).$$

Corollary 11.1.4.

$$\sum_p \frac{1}{p^\sigma} = \log \frac{1}{\sigma - 1} + O(1).$$

This proves that there are infinitely many primes.

11.2. **Dirichlet's theorem for** 1 (mod 4) **and** 3 (mod 4)**.** The proof will be a generalization of Euler's proof of the infinitude of primes, but we need to construct one more function since we are splitting the primes into two groups. This is called the Dirichlet L-function, which we will denote by $L(s, \chi_{-4})$.

Definition 11.2.1.

$$\chi_{-4}(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \\ -1 & \text{if } n \equiv 3 \pmod 4 \\ 0 & \text{if } n \text{ is even} \end{cases}$$

This is periodic with period 4: $\chi_{-4}(n) = \chi_{-4}(n+4)$. It is also multiplicative: $\chi_{-4}(mn) = \chi_{-4}(m)\chi_{-4}(n)$.

Definition 11.2.2.

$$L(s, \chi_{-4}) = \sum_{n=1}^{\infty} \frac{\chi_{-4}(n)}{n^s} = \frac{1}{1^s} - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \cdots = \prod_p \left(1 + \frac{\chi_{-4}(p)}{p^s} + \frac{\chi_{-4}(p^2)}{p^{2s}}\right).$$

This last equality again follows from unique factorization and the fact that χ_{-4} is completely multiplicative. This is

$$= \prod_p \sum_{k=0}^{\infty} \frac{\chi_{-4}(p)^k}{p^{ks}} = \prod_p \left(1 - \frac{\chi_{-4}(p)}{p^s}\right)^{-1}.$$

When $\Re s > 1$, the product converges absolutely, and it converges to something nonzero. Therefore, $L(s, \chi_{-4}) \neq 0$ if $\Re s > 1$.

Where does the series converge? This is an alternating series, and we can using the alternating series test to see that this converges for $s > 0$. This doesn't say anything about the product, however.

Now, consider

$$\log L(\sigma, \chi_{-4}) = \sum_p -\log\left(1 - \frac{\chi_{-4}(p)}{p^\sigma}\right) = \sum_p \sum_{k=1}^{\infty} \frac{\chi_{-4}(p)^k}{p^{k\sigma}} = \sum_p \frac{\chi_{-4}(p)}{p^\sigma} + O(1).$$

We also know that

$$\log \zeta(\sigma) = \sum_p \frac{1}{p^\sigma} + O(1).$$

Therefore,

$$\log \zeta(\sigma) + \log L(\sigma, \chi_{-4}) = \sum_{p \equiv 1 \pmod 4} \frac{2}{p^\sigma} + O(1)$$

$$\log \zeta(\sigma) - \log L(\sigma, \chi_{-4}) = \sum_{p \equiv 3 \pmod 4} \frac{2}{p^\sigma} + O(1)$$

Let $\sigma \to 1^+$. Then

$$\sum_{p \equiv 1 \pmod 4} \frac{2}{p^\sigma} + O(1) = \log \zeta(\sigma) + \log L(\sigma, \chi_{-4}).$$

Since $\log \zeta(\sigma) \to \infty$, we are done if we can show $\log L(\sigma, \chi_{-4})$ does not go to $-\infty$. In fact, this actually converges to a $\log L(1, \chi_{-4})$. So we want to show that $L(1, \chi_{-4}) \neq 0$. In this case,

$$L(1, \chi_{-4}) = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \frac{\pi}{4},$$

and hence there are infinitely many primes $\equiv 1 \pmod 4$. The other case is similar, so

$$\sum_{p \equiv 1 \pmod 4} \frac{1}{p^\sigma} \approx \sum_{p \equiv 3 \pmod 4} \frac{1}{p^\sigma} \approx \frac{1}{2} \log \frac{1}{\sigma - 1} + O(1).$$

12. 11/1

We are building toward a proof that there are infinitely many $p \equiv a \pmod q$ when $(a, q) = 1$. We are adding to Euler's proof of the infinitude of primes.

12.1. **Review.** Recall

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Then

$$\log \zeta(s) = \sum_p \sum_{k=1}^{\infty} \frac{1}{k p^{ks}},$$

and

$$\log \zeta(\sigma) = \sum \frac{1}{p^\sigma} + O(1).$$

We also proved

$$\zeta(\sigma) = \frac{1}{\sigma - 1} + O(1).$$

We introduced

$$L(s, \chi_{-4}) = \frac{1}{1^s} - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \cdots = \prod_p \left(1 - \frac{\chi_{-4}(p)}{p^s}\right)^{-1}$$

where χ_{-4} is completely multiplicative and periodic. This series converges absolutely if $\Re s > 1$ and converges conditionally if $s > 0$. The product converges absolutely if $s > 1$.

Now,

$$\log L(\sigma, \chi_{-4}) = \sum_p \sum_{k=1}^{\infty} \frac{\chi_{-4}(p)^k}{k p^{k\sigma}} = \sum_p \frac{\chi_{-4}(p)}{p^\sigma} + O(1).$$

Then

$$\frac{1}{2}(\log \zeta(\sigma) + \log L(\sigma, \chi_{-4}) = \sum_{p \equiv 1 \pmod 4} \frac{1}{p^\sigma} + O(1)$$

$$\frac{1}{2}(\log \zeta(\sigma) - \log L(\sigma, \chi_{-4}) = \sum_{p \equiv 3 \pmod 4} \frac{1}{p^\sigma} + O(1).$$

Let $\sigma \to 1^+$, $L(\sigma, \chi_{-4}) \to L(1, \chi_{-4}) \neq \infty \neq 0$ because $L(1, \chi_{-4}) = \frac{\pi}{4}$.

Theorem 12.1.1. *As $\sigma \to 1^+$,*

$$\sum_{p \equiv 1 \pmod 4} \frac{1}{p^\sigma} = \frac{1}{2}\zeta(\sigma) + O(1) = \sum_{p \equiv 3 \pmod 4} \frac{1}{p^\sigma}.$$

Here is a pretty fact:

$$\frac{1}{1 + t^2} = 1 - t^2 + t^4 - t^6 + \cdots$$

Then

$$\int_0^1 \frac{dt}{1 + t^2} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \arctan(1) - \arctan(0) = \frac{\pi}{4}.$$

Now, the plan will be to generalize this whole proof for every modulus. We'll need to construct functions analogous to χ_{-4} and to write down functions like $L(s, \chi_{-4})$. The functions that we write down will need to converge and be positive, which in general is very hard. Then we'll have analogs of the theorem. Evaluating at 1 will be interesting and is called the class number formula.

12.2. $q = 3$. Now, let $q = 3$. There were two reduced residue classes $\pmod 4$, so we needed two functions. You'd think that the same would be true here. One of them is the zeta function, so we need another function.

We want to find χ_{-3} that is periodic with period 3 and that is completely multiplicative and not identically zero.

We want to set $\chi_{-3}(n) = 0$ if $3 \mid n$. Periodic with period 3 means that $\chi_{-3} : (\mathbb{Z}/3\mathbb{Z})^\times \to \mathbb{C}$. Also, if m, n are reduced residue classes (mod 3), we want $\chi_{-3}(mn) = \chi_{-3}(m)\chi_{-3}(n)$. So we have to define $\chi_{-3}(1 \pmod 3) = 1$, and $\chi_{-3}(2 \pmod 3) = \pm 1$. If we chose $+1$, we would get the zeta function, so we'll actually take $\chi_{-3}(2 \pmod 3) = -1$. Then

$$\chi_{-3}(p) = \begin{cases} 1 & p \equiv 1 \pmod 3 \\ -1 & p \equiv 2 \pmod 3 \\ 0 & p = 3. \end{cases}$$

which extends to

$$\chi_{-3}(n) = \begin{cases} 1 & n \equiv 1 \pmod 3 \\ -1 & n \equiv 2 \pmod 3 \\ 0 & n = 3 \end{cases} = \left(\frac{n}{3}\right).$$

We said before that the Legendre symbol is completely multiplicative, so we're looking for generalizations of Legendre symbols.

Now, define

$$L(\sigma, \chi_{-3}) = \sum_{n=1}^{\infty} \frac{\chi_{-3}(\sigma)}{n^\sigma} = \prod_p \left(1 - \frac{x_{-3}}{p^\sigma}\right)^{-1},$$

and

$$\log L(\sigma, \chi_{-3}) = \sum_p \frac{\chi_{-3}}{p^\sigma} + O(1)$$

if $\sigma > 1$. Then

$$\frac{1}{2}(\log \zeta(\sigma) + \log L(\sigma, \chi_{-3}) = \sum_{p \equiv 1 \pmod 3} \frac{1}{p^\sigma} + O(1)$$

$$\frac{1}{2}(\log \zeta(\sigma) - \log L(\sigma, \chi_{-3}) = \sum_{p \equiv 2 \pmod 3} \frac{1}{p^\sigma} + O(1).$$

Let $\sigma \to 1^+$, $L(\sigma, \chi_{-3}) \to L(1, \chi_{-3}) \neq \infty \neq 0$. We know that this does not go to infinity because of the conditional convergence from the alternating series test. It does not go to zero because we can sum the series.

$$\begin{aligned} L(1, \chi_{-3}) &= \int_0^1 (1 - t + t^3 - t^4 + t^6 - t^7 + \cdots)\, dtT = \int_0^1 \frac{1-t}{1-t^3}\, dt = \int_0^1 \frac{dt}{1+t+t^2}\, dt \\ &= \int_0^1 \frac{dt}{(t+1/2)^2 + 3/4} = \int_{1/2}^{3/2} \frac{dy}{y^2 + 3/4} = \int_{1/\sqrt{3}}^{\sqrt{3}} \frac{\sqrt{3}}{2} \frac{dz}{z^2+1} \frac{4}{3} \\ &= \frac{2}{\sqrt{3}} \left(\arctan(\sqrt{3}) - \arctan(1/\sqrt{3})\right) = \frac{\pi}{3\sqrt{3}}. \end{aligned}$$

We have therefore proved an analogous theorem to what we got before:

Theorem 12.2.1. *As $\sigma \to 1^+$,*

$$\sum_{p \equiv 1 \pmod 3} \frac{1}{p^\sigma} = \frac{1}{2}\zeta(\sigma) + O(1) = \sum_{p \equiv 2 \pmod 3} \frac{1}{p^\sigma}.$$

12.3. $q = 8$**.** We want to consider $1, 3, 5, 7 \pmod 8$. To distinguish these four possibilities, we should look for four functions. We have the zeta function as before, which we will give a new name:

$$\chi_0(n) = \begin{cases} 1 & (n,8) = 1 \\ 0 & (n,8) > 1. \end{cases}$$

Then

$$L(\sigma, \chi_0) = \sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^\sigma} = \prod_p \left(1 - \frac{1}{p^\sigma}\right)^{-1}.$$

So $\chi_0 : (\mathbb{Z}/8\mathbb{Z})^\times \to \mathbb{C}$, and it takes the value 1 on all reduced residue classes. We want three more functions that are periodic mod 8. They shall be zero on the even numbers. We want $\chi : (\mathbb{Z}/8\mathbb{Z})^\times \to \mathbb{C}$ not identically zero. They also must satisfy $\chi(mn) = \chi(m)\chi(n)$ for any two residue classes $m, n \pmod 8$. Another way of saying this is that we want a group homomorphism from $(\mathbb{Z}/8\mathbb{Z})^\times$ to $\mathbb{C}$.

As before, we must have $\chi(1) = 1$. Note that $(\mathbb{Z}/8\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. There are two possibilities: $\chi(3) = \pm 1$.

If $\chi(3) = 1$, then $\chi(5) = \pm 1$. If $\chi(5) = 1$ then $\chi(7) = 1$. If $\chi(5) = -1$ then $\chi(7) = -1$.

If $\chi(3) = -1$, then $\chi(5) = \pm 1$. If $\chi(5) = 1$ then $\chi(7) = -1$. If $\chi(5) = -1$ then $\chi(7) = 1$.

These are all of them: there are precisely four of them.

	1	3	5	7
χ_0	1	1	1	1
χ_{-4}	1	-1	1	-1
χ_8	1	-1	-1	1
χ_{-8}	1	1	-1	-1

Currently, this is just numerology. Call these functions characters. We'll generalize this in the next lecture or so.

In each of these four characters, we can look at

$$L(s, \chi) = \sum \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

The series and product converge absolutely when $s > 1$.

What are we hoping to do? In the case $1 \pmod 8$, we want

$$\frac{1}{4}(\chi_0(n) + \chi_{-4}(n) + \chi_{-8}(n) + \chi_{-4}(n))$$

In the case $3 \pmod 8$, we want

$$\frac{1}{4}(\chi_0(n) - \chi_{-4}(n) - \chi_{-8}(n) + \chi_{-4}(n))$$

In the case $5 \pmod 8$, we want

$$\frac{1}{4}(\chi_0(n) + \chi_{-4}(n) - \chi_{-8}(n) - \chi_{-4}(n))$$

In the case 7 (mod 8), we want

$$\frac{1}{4}(\chi_0(n) - \chi_{-4}(n) + \chi_{-8}(n) - \chi_{-4}(n))$$

When $\chi = \chi_0$, we want

$$L(s, \chi_0) = \zeta(s)\left(1 - \frac{1}{2^s}\right).$$

If $\sigma > 1$,

$$\log L(\sigma, \chi_0) = \log \zeta(\sigma) + O(1).$$

We already know that $L(s, \chi_{-4})$ converges conditionally for $s > 0$. Additionally,

$$L(s, \chi_8) = \frac{1}{1^s} - \frac{1}{3^s} - \frac{1}{5^s} + \frac{1}{7^s} + \cdots$$

$$L(s, \chi_{-8}) = \frac{1}{1^s} + \frac{1}{3^s} - \frac{1}{5^s} - \frac{1}{7^s} + \cdots$$

Here, we can combine adjacent terms to get alternating series that converge conditionally for $s > 0$ provided we work out some generalization of the alternating series test.

For all of these characters, $\sigma > 1$, and

$$\log L(\sigma, \chi) = \sum \frac{\chi(p)}{p^\sigma} + O(1).$$

Now,

$$\sum_{1 \pmod 8} \frac{1}{p^\sigma} = \frac{1}{4}(\log L(\sigma, \chi_0) + \log L(\sigma, \chi_4) + \log L(\sigma, \chi_{-8}) + \log L(\sigma, \chi_8)) + O(1),$$

and there are three more of these. The alternating series test says that none of these is zero. The last step is to show that none of these is zero; this step is left as an exercise.

12.4. $q = 5$**.** Here, we want to consider $\chi : (\mathbb{Z}/5\mathbb{Z})^\times \to \mathbb{C}$, where $\chi(mn) = \chi(m)\chi(n)$, χ is not identically zero.

As before $\chi(1) = 1$, and the group $(\mathbb{Z}/5\mathbb{Z})^\times$ is cyclic. It is generated by 2. We just need to know $\chi(2)$. Since $\chi(2)^4 = \chi(16) = \chi(1) = 1$, we get four possibilities: $\chi(2) = \pm 1, \pm i$.

We can again write down the character table:

	1	2	3	4	
χ_0	1	1	1	1	trivial or principal character
χ_5	1	-1	-1	1	
ψ	1	i	-i	-1	
$\overline{\psi}$	1	-i	i	-1	

We can use these to identify each progression (mod 5). For example, for 2 (mod 5), we have

$$\frac{1}{4}(\chi_0 - x_5 - i\psi + i\overline{\psi}).$$

This is kind of like taking the dot product.

We again define

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum \frac{\chi(n)}{n^s}.$$

These converge absolutely when $s > 1$. When $\chi = \chi_0$, we have

$$L(s, \chi_0) = \zeta(s)\left(1 - \frac{1}{5^s}\right).$$

Here,

$$\log L(\sigma, \chi_0) = \log \zeta(\sigma) + O(1).$$

For $\chi \neq \chi_0$, we need an alternating series test that will tell us that they converge conditionally for $s > 0$. We also need to know that $L(1, \chi) \neq 0$ for these characters. The complex ones aren't too hard; the real one was done at the Putnam seminar a few weeks ago.

13. 11/3

We were trying to define Dirichlet characters for every modulus to separate out every reduced residue class.

In the case of $q = 5$, we saw that $\chi : (\mathbb{Z}/5\mathbb{Z})^\times \to \mathbb{C}$. 2 is a primitive root $\pmod 5$, so $\chi(2)^4 = 1$, and we computed a character table.

We defined

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1},$$

which converges for $s > 1$.

If $\chi = \chi_0$, we have $L(s, \chi_0) = \zeta(s)\left(1 - \frac{1}{5^s}\right)$. Then

$$L(s, \chi_0) = 1 - \frac{1}{2^s} - \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

converges conditionally for $s > 0$, and

$$L(s, \psi) = 1 + \frac{1}{2^s} - \frac{1}{3^s} - \frac{1}{4^s} + \cdots$$

converges conditionally for $s > 0$.

Now,

$$\log L(s, \chi) = \sum_p -\log\left(1 - \frac{\chi(p)}{p^s}\right) = \sum_p \sum_{k=1}^{\infty} \frac{\chi(p)^k}{k p^{ks}}.$$

Recall that log of complex numbers is dangerous, because it is not single valued; adding multiples of $2\pi i$ does not change log. When $s > 1$, we have

$$= \sum_p \frac{\chi(p)}{p^s} + O(1).$$

Then,

$$\sum_{p \equiv 1 \pmod 5} \frac{1}{p^s} = \frac{1}{4}\left(\log L(s, \chi_0) + \log L(s, \chi_5) + \log L(s, \psi) + \log L(s, \overline{\psi})\right) + O(1).$$

We want $L(1, \chi_5)$, $L(1, \psi)$, $L(1, \overline{\psi})$ to be not infinity or zero. For $L(s, \psi)$ and $L(s, \overline{\psi})$, we can look at the imaginary part, i.e.

$$\Im L(1, \psi) = \frac{1}{2} - \frac{1}{3} + \frac{1}{5} - \frac{1}{8} + \cdots > 0.$$

We can do this trick of writing it as an integral:

$$L(1,\chi_5) = \int_0^1 \left(1 - t - t^2 + t^3 + t^5 - t^6 - t^7 + t^8 + \cdots\right)\, dt = \int_0^1 \frac{1 - t - t^2 + t^3}{1 - t^5}\, dt,$$

and this is left to you as an exercise. Recall from calculus that any rational function can be integrated. This will have some nice answer in terms of logs of the golden ratio.

We can do the same thing for every progression (mod 5) to see that there are infinitely many primes in every progression, and in fact, a quarter in each progression.

We need to prove orthogonality relations for the character table to make sure that we can produce every arithmetic progression, and we need to find a more general form of the alternating series test. Then we will have a way to isolate the primes in every progression, so when we let $s \to 1^+$, we will need to show that the L-functions are not infinity or zero.

13.1. **Dirichlet characters (mod q).**

Definition 13.1.1. A Dirichlet character $\chi(q)$ is a function $\chi : \mathbb{Z} \to \mathbb{C}$ with the properties

(1) $\chi(n) = 0$ if and only if $(n, q) > 1$.
(2) $\chi(n + q) = \chi(n)$
(3) $\chi(mn) = \chi(m)\chi(n)$ for all m, n.

Therefore, we have $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ is a group homomorphism.

How do we figure out what these functions are? We know that $\chi(1) = 1$ because $\chi(n) = \chi(n)\chi(1)$ for all n. Now, if $(a, q) = 1$,

$$\chi(a)^{\phi(q)} = \chi\left(a^{\phi(q)}\right) = \chi(1) = 1,$$

so each $\chi(a)$ is a $\phi(q)$-th root of unity.

We always have the principal character

$$\chi_0(n) = \begin{cases} 1 & (n, q) = 1 \\ 0 & (n, q) > 1. \end{cases}$$

How many characters are there? There are only finitely many reduced residue classes and finitely many choices for $\chi(a)$, so there are only finitely many characters. (We expect there to be $\phi(q)$ characters based on the examples computed earlier.)

If $q = p^\alpha$ where p is an odd prime, then there exists a primitive root g (mod q). Then we only need to specify $\chi(g)$, so there are exactly $\phi(q)$ characters here. So we can take

$$\chi(g) = e^{\frac{2\pi i l}{\phi(q)}}, \quad 0 \le l \le \phi(q) - 1.$$

What if $q = 2^\alpha$? The case of $\alpha = 1$ is trivial, and we've done $\alpha = 2$ and $\alpha = 3$. To specify χ, we need to specify $\chi(-1)$ and $\chi(5)$. The choices are $\chi(-1) = \pm 1$ and $\chi(5)$ is a $2^{\alpha-2}$-th root of unity. So there are $2^{\alpha-1}$ characters here.

If p is an odd prime and g is a primitive root. Then $\chi(g) = -1$ and x are Legendre symbols. So these characters are generalizations of the Legendre symbols.

The characters form a group. Suppose that χ_1 and χ_2 are characters (mod q). Define $\chi_1\chi_2(n) = \chi_1(n)\chi_2(n)$. This is still a character because it is periodic and completely multiplicative, and it is not identically zero. The identity element is χ_0. The inverse of χ is the complex conjugate $\overline{\chi}$. The Legendre symbol is its own inverse.

For example, in the case $q = 5$, recall the character table

	1	2	3	4
χ_0	1	1	1	1
χ_5	1	-1	-1	1
ψ	1	i	-i	-1
$\overline{\psi}$	1	-i	i	-1

The characters here form a cyclic group ψ, $\psi^2 = \chi_5$, $\psi^3 = \overline{\psi}$, and $\psi^4 = \chi_0$.

13.2. **Orthogonality relations.** Now, we need to show the orthogonality relations. Let G be the group of all characters $x \pmod q$. At the moment, we only know that G is a finite group.

13.2.1. *Orthogonality of rows.*

Proposition 13.2.1. *If $\chi \in G$, consider the row sums*

$$\sum_{n \pmod q} \chi(n) = \begin{cases} \phi(q) & \chi = \chi_0 \\ 0 & \chi \neq \chi_0. \end{cases}$$

In fact,

$$\sum_{n \pmod q} \chi(n)\overline{\psi}(n) = \begin{cases} \phi(q) & \chi = \psi \\ 0 & \chi \neq \psi. \end{cases}$$

Proof. The second statement follows from the first statement for $\chi\overline{\psi}$. ($\chi\overline{\psi} = \chi_0 \Leftrightarrow \chi = \psi$). So we only have to prove the first statement.

Define

$$S(\chi) = \sum_{n \pmod q} \chi(n)$$

Take a number c so that $(c, q) = 1$, and multiply both sides by $\chi(c)$. So

$$\chi(c)S(\chi) = \sum_{n \pmod q} \chi(c)\chi(n) = \sum_{n \pmod q} \chi(cn) = \sum_{m \pmod q} \chi(m) = S(\chi).$$

This means that either $S(\chi) = 0$ or $\chi(c) = 1$. If $S(\chi) \neq 0$ then $\chi(c) = 1$ for all $(c, q) = 1$, so that $\chi = \chi_0$, which is what we wanted to prove. □

13.2.2. *Characters for composite moduli.* Next, we want to show the orthogonality of columns and we want to know what all of the characters are. We want to show how to construct characters for composite moduli.

Consider characters $\chi_1 \pmod{q_1}$ and $\chi_2 \pmod{q_2}$, $(q_1, q_2) = 1$. We can define $x_1x_2(n) = x_1(n)x_2(n)$. We claim that $\chi_1\chi_2$ is a character $\pmod{q_1q_2}$. This is periodic by the Chinese Remainder Theorem. This is also completely multiplicative, so it is a character.

So if $q = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, we have characters $\chi_1 \pmod{p_1^{\alpha_1}}$, $\chi_2 \pmod{p_1^{\alpha_2}}$, $\cdots$ $\chi_k \pmod{p_1^{\alpha_k}}$, we can multiply these to get a character $\chi \pmod q = \chi_1\chi_2\cdots\chi_k$.

Remark. If we take another choice $\psi_1 \pmod{p_1^{\alpha_1}}, \psi_2 \pmod{p_2^{\alpha_2}}, \cdots, \psi_k \pmod{p_k^{\alpha_k}}$, we can construct $\psi \pmod q$.

Say $\chi_1 \neq \psi_1$. Then we want to say that $\chi \neq \psi$.

Proof. Say $\chi_1(n) \neq \psi_1(n)$. Choose $m \equiv n \pmod{p_1^{\alpha_1}}$, $m \equiv 1 \pmod{p_j^{\alpha_j}}$ for all $j > 1$. Then $\chi(m) = \chi_1(n)$ and $\psi(m) = \psi_1(n)$ □

This tells us that we have at least $\phi(q)$ distinct characters $\pmod q$. Consider $\chi\psi \pmod q$. This corresponds to $\chi_1\psi_1 \pmod{p_1^{\alpha_1}}$, $\chi_2\psi_2 \pmod{p_2^{\alpha_2}}$, $\cdots$, $\chi_k\psi_k \pmod{p_k^{\alpha_k}}$.

Let H denote the group of characters that we obtain by multiplying characters $\pmod{p_j^{\alpha_j}}$. We would like to show that $H = G$.

13.2.3. *Orthogonality of columns.*

Proposition 13.2.2. *Let $(n, q) = 1$. Then*

$$\sum_{\chi\in H} \chi(n) = \begin{cases} \phi(q) & n \equiv 1 \pmod q \\ 0 & n \not\equiv 1 \pmod q \end{cases}$$

Given this, we can generalize slightly to get

$$\sum_{\chi\in H} \chi(n)\overline{\chi}(a) = \begin{cases} \phi(q) & n \equiv a \pmod q \\ 0 & n \not\equiv a \pmod q \end{cases}$$

Proof. Note that statement 2 follows from statement 1 Since $aa^{-1} \equiv 1 \pmod q$, we have $\chi(a)\chi(a^{-1}) = 1$, so $\overline{\chi}(a) = \chi(a^{-1})$, and then

$$\sum_{\chi\in H} \chi(n)\overline{\chi}(a) = \sum_{\chi\in H} \chi(na^{-1}).$$

Define $S(n) = \sum_{\chi\in H} \chi(n)$. Take $\psi \in H$. Then

$$\psi(n)S(n) - \sum_{\chi\in H} \psi(n)S(n) = \sum_{\chi\in H} (\psi\chi)(n) = \sum_{\rho\in H} \rho(n) = S(n).$$

Therefore, either $S(n) = 0$ or $\psi(n) = 1$ for all $\psi \in H$. If $\psi(n) \equiv 1$ for all $\psi \in H$, then $n \equiv 1 \pmod q$.

Check this: Prove it for $q = p^\alpha$. □

14. 11/8

14.1. **Review.** We are interested in Dirichlet characters $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$, and in fact, they always have values that lie on the unit circle. The values of χ are $\phi(q)$-th roots of unity.

The characters χ form a group, where χ_0 is the principal character is the identity, and $\chi^{-1} = \overline{x}$ is the complex conjugate and inverse. If χ, ψ are characters, then $\chi\psi(n) = \chi(n)\psi(n)$ is a character.

Let the group of characters $\pmod q$ be G. This is a finite abelian group.

We proved the first orthogonality relation:

$$\sum_{n \pmod q} \chi(n) = \begin{cases} \phi(q) & \chi = \chi_0 \\ 0 & \chi \neq \chi_0 \end{cases}.$$

The proof was reasonably easy. Similarly, we saw that

$$\sum_{n \pmod q} \chi(n)\overline{\psi}(n) = \begin{cases} \phi(q) & \chi = \psi \\ 0 & \chi \neq \psi \end{cases}.$$

We discussed the case $q = p^\alpha$, p is odd. Here, $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic, so it is easy to see what the characters are. We can pick a generator g. Then $\chi(g)$ determines $\chi(g^k)$ for all k, and

so χ is determined for all reduced residue classes. Note that we can have $\chi(g) = e^{\frac{2\pi il}{\phi(q)}}$ for $0 \leq l \leq \phi(q) - 1$. Therefore, for $q = p^\alpha$, we explicitly described $\phi(q)$ characters (mod q).

Now, we describe what happens for a composite modulus. Suppose $q = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Consider characters

$$\chi_1 \pmod{p_1}^{\alpha_1}, \quad \chi_2 \pmod{p_2}^{\alpha_2}, \quad \cdots, \quad \chi_k \pmod{p_k}^{\alpha_k}.$$

Then, define $\chi \pmod q$ via $\chi(n) = \chi_1(n)\chi_2(n)\cdots\chi_k(n)$. Different choices for $(\chi_1, \cdots, \chi_k)$ give different choices of $\chi \pmod q$. We have therefore constructed $\phi(q)$ characters $\chi \pmod q$ in this fashion. The characters we have constructed in this way also form a group. Call this group H. We want to show that $G = H$; all of the characters arise this way. To find characters for a composite modulus, multiply characters for prime power modulus.

To do this, we proved another orthogonality relation. Given $(n, q) = 1$,

$$\sum_{\chi \in H} \chi(n) = \begin{cases} \phi(q) & n \equiv 1 \pmod q \\ 0 & n \not\equiv 1 \pmod q \end{cases}.$$

This is the same as saying that if $(n, q) = 1$, $(a, q) = 1$, then

$$\sum_{\chi \in H} \chi(n)\overline{\chi(a)} = \begin{cases} \phi(q) & n \equiv a \pmod q \\ 0 & n \not\equiv a \pmod q \end{cases}.$$

Proof. Let

$$S(n) = \sum_{\chi \in H} \chi(n).$$

Take any character $\psi \in H$. Then

$$\psi(n)S(n) = \sum_{\chi \in H} \chi\psi(n) = \sum_{\chi \in H} \chi(n) = S(n),$$

so either $S(n) = 0$ or $\psi(n) = 1$ for all characters $\psi \in H$. The only way the latter condition can hold is when $n \equiv 1 \pmod q$. The proof is to pick $\chi_2, \cdots, \chi_k$ to all be the trivial character, and only vary χ_1. Since χ_1 comes from a root of unity, we have $n = g^k$, and therefore $\chi(n) = e^{\frac{2\pi ikl}{\phi(q)}}$, which is only possible for $k = 0$ and hence $n = 1$. The same argument holds for the other characters $\chi_2, \cdots, \chi_k$, and so we're done. □

We get for free that $G = H$ are there are no more characters (mod q). Suppose that X is some character (mod q) which is in G but not H. By the first orthogonality relation, if we take any $\psi \in H$,

$$\sum_{n \pmod q} X(n)\overline{\psi}(n) = 0.$$

Now take any $(c, q) = 1$ and multiply both sides by $\psi(c)$. Then

$$\sum_{n \pmod q} X(n)\overline{\psi}(n)\psi(c) = 0.$$

Since this is true for all $\psi \in H$, we can sum over them:

$$\sum_{n \pmod q} X(n) \sum_{\psi \in H} \overline{\psi}(n)\psi(c) = 0.$$

By the second orthogonality relation, this gives

$$\phi(q) \cdot X(c) = 0,$$

so therefore $X(c) = 0$ for all $(c, q) = 1$, so $X(\cdot)$ is identically zero and therefore $G = H$.

Here is another way to think about the previous discussion. We are interested in the space of all functions $(\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}$. This is a vector space over $\mathbb{C}$ of dimension $\phi(q)$. There are some vectors in this space that we like. A nice basis for the space would be (for $(a, q) = 1$):

$$f_a(n) = \begin{cases} 1 & n \equiv a \pmod{q} \\ 0 & n \not\equiv a \pmod{q} \end{cases}.$$

These form an orthonormal basis with the usual inner product:

$$< f, g >= \sum_{n \pmod{q}} f(n)\overline{g(n)}.$$

We've written down another basis for the space. This is not as simple as the previous basis, but it has another very important property: Our new basis consists of group homomorphisms. These are the characters $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}$, and they respect the group structure. There are exactly $\phi(q)$ of these, and they also form an orthogonal basis by the first orthogonality relation. The second orthogonality relation is simply a change of basis relation between our two bases.

Remark. This is actually an important principle. Given some arbitrary group, we can write down bases of the space of maps from the group to some set. If the group is abelian, life is wonderful. If not, that's the realm of representation theory.

Dirichlet did this before the idea of abstract groups, so he was the first person to deal with these characters. These ideas predate the idea of groups.

14.2. **Plan of proof of Dirichlet's Theorem.** We now know that there are $\phi(q)$ characters $\chi(q)$. For each, form

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \cdots\right) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

If $\Re(s) > 0$, both the series and the product converge absolutely, and $L(s, \chi) \neq 0$ if $\Re(s) > 1$.

Recall that if $\chi = \chi_0$, we have

$$L(s, \chi_0) = \zeta(s) \prod_{p|q} \left(1 - \frac{1}{p^s}\right) = \prod_{p \nmid q} \left(1 - \frac{1}{p^s}\right)^{-1}$$

As $s \to 1^+$, $\prod_{p|q} \left(1 - \frac{1}{p^s}\right) \to \frac{\phi(q)}{q}$ and $\zeta(s) \to \infty$. For $s > 1$,

$$\log L(s, \chi) = \sum_p \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}} = \sum_p \frac{\chi(p)}{p^s} + O(1).$$

Now, given a residue class $a \pmod q$, $(a,q)=1$, we have

$$\begin{aligned}\sum_{p\equiv a \pmod q} \frac{1}{p^s} &= \sum_p \frac{1}{p^s}\left(\frac{1}{\phi(q)}\sum_{\chi \pmod q} \chi(p)\overline{\chi(a)}\right)\\ &= \frac{1}{\phi(q)}\sum_{\chi \pmod q}\overline{\chi(a)}\left(\sum_p \frac{\chi(p)}{p^s}\right)\\ &= \frac{1}{\phi(q)}\sum_{\chi \pmod q}\overline{\chi(a)}\left(\log L(s,\chi)+O(1)\right)\\ &= \frac{1}{\phi(q)}\sum_{\chi \pmod q}\overline{\chi(a)}\log L(s,\chi)+O(1).\end{aligned}$$

We want this to diverge because that would give infinitely many primes $\equiv a \pmod q$. Now, for $\chi=\chi_0$, we have $\log L(s,\chi_0)=\log\zeta(s)+O(1)\to+\infty$ as $s\to 1^+$.

The crux of the remainder of the proof will be to show that as $s\to 1^+$, $\chi\neq\chi_0$, we want that $L(s,\chi)$ does not tend to 0 or ∞, i.e. that $\log L(s,\chi)$ is bounded as $s\to 1^+$, $\chi\neq\chi_0$.

One part will be easy. To show that $L(s,\chi)$ does not go to infinity, we only need a generalization of the alternating test. To show that this does not go to zero is quite hard, especially for real characters.

14.3. **Generalization of alternating series test.** We generalize the alternating series test to show that $L(s,\chi)$ makes sense for $s>0$.

14.3.1. *Partial summation.* Assume that there is some sequence of complex numbers a_n, and assume that there is "a nice function" $f(n)$. Then we want to consider

$$\sum_{n=A+1}^{B} a_n f(n).$$

Define

$$s_n=\sum_{k=1}^{n} a_k.$$

We can now write

$$\begin{aligned}\sum_{n=A+1}^{B} a_n f(n) &= \sum_{n=A+1}^{B}(s_n-s_{n-1})f(n) = \sum_{n=A+1}^{B} s_n f(n) - \sum_{n=A+1}^{B} s_{n-1}f(n)\\ &= \sum_{n=A+1}^{B} s_n f(n) - \sum_{n=A}^{B-1} s_n f(n+1)\\ &= s_B f(B+1) - s_A f(A+1) - \sum_{n=A+1}^{B} s_n(f(n+1)-f(n))\end{aligned}$$

This is an analog of integration of parts.

14.4. **Alternating series test.** Here, $a_1 = 1$, $a_2 = -1$, $\cdots$, $a_n = \pm 1$, $s_n = 0$ or 1, $f(n)$ is monotone decreasing. Then

$$\left| \sum_{n=A+1}^{B} a_n f(n) \right| \leq f(B+1) + f(A+1) + \sum_{n=A+1}^{B} (f(n) - f(n+1)) = 2f(A+1).$$

This is precisely the alternating series test. Note that all that we needed was that the s_n are bounded.

Proposition 14.4.1. *Given $a_n \in \mathbb{C}$, with $|s_n| \leq S$. Suppose that $f(n)$ is monotone decreasing to zero. Then*

$$\sum a_n f(n)$$

converges (converges).

Proof. We just need to show that the partial sums form a Cauchy sequence, i.e.

$$\left| \sum_{n=A+1}^{B} a_n f(n) \right| < \varepsilon$$

if A is sufficiently big. By partial summation, it is

$$\leq S \left(f(B+1) + f(A+1) + \sum_{n=A+1}^{B} (f(n) - f(n+1)) \right) = 2Sf(A+1).$$

By choosing A sufficiently large, we can make this less than ε. □

We have therefore proved that

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

converges conditionally if $s > 0$. All we have to show is that

$$s_n = \sum_{k=1}^{n} \chi(k)$$

is bounded. But after every q values, the sum is zero, so

$$|s_n| = \left| \sum_{k=1}^{n} \chi(k) \right| \leq \phi(q).$$

15. 11/10

15.1. **Partial summation.** We introduced the idea of partial summation: If there is a nice sequence of complex numbers a_n and some nice function $f(n)$, and if $s_n = \sum_{k \leq n} a_k$, then

$$\sum_{n=A+1}^{B} a_n f(n) = \sum_{n=A+1}^{B} f(n)(s_n - s_{n-1}) = s_B f(B+1) - s_A f(A+1) - \sum_{n=A+1}^{B} s_n (f(n+1) - f(n)).$$

Think of this as integration, i.e.

$$\sum_{n=A+1}^{B} f(n)(s(n)-s(n-1)) = \int_{(A+1)^-}^{B^+} f(t)\,d(s_t) = f(t)s_t|_{(A+1)^-}^{B^+} - \int_{(A+1)^-}^{B^+} f'(t)s_t\,dt$$
$$= s_{B^+}f(B^+) - s_{(A+1)^-}f((A+1)^-) - \int_{(A+1)^-}^{B^+} f'(t)s_t\,dt.$$

The point is that if f is nice and differentiable, we can rewrite our sums as integrals.

Last time, we considered the alternating series test as a nice application of this. Here are more applications:

15.1.1. *Applications.*

Proposition 15.1.1.

$$\sum_{n\le x}\frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right),$$

where $\gamma \approx 0.577\ldots$ is Euler's constant.

Proof. Here,

$$s_t = \sum_{1\le n\le t} 1 = [t].$$

$a_n = 1$ if $n \in \mathbb{N}$, and $f(t) = \frac{1}{t}$. We are interested in

$$\sum_{n\le x}\frac{1}{n} = \int_{1^-}^{x^+}\frac{1}{t}d([t]) = \frac{1}{t}[t]\Big|_{1^-}^{x^+} - \int_{1^-}^{x^+}\frac{1}{t^2}[t]dt = \frac{[x^+]}{x^+} + \int_{1^-}^{x^+}\frac{[t]}{t^2}dt$$
$$= 1 + O\left(\frac{1}{x}\right) + \int_{1^-}^{x^+}\frac{t-\{t\}}{t^2}dt = 1 + O\left(\frac{1}{x}\right) + \log x - \int_{1^-}^{x^+}\frac{\{t\}}{t^2}dt.$$

Here, $[t]$ denotes the integer part of t and $\{x\}$ denotes the fractional part of t, and

$$\int_{1^-}^{x^+}\frac{\{t\}}{t^2}dt = \int_1^\infty \frac{\{t\}}{t^2}dt - \int_x^\infty \frac{\{t\}}{t^2}dt = \text{constant} - O\left(\frac{1}{x}\right).$$

We have therefore proved that

$$\sum_{n\le x}\frac{1}{n} = (\log x) + \left(1 - \int_1^\infty \frac{\{t\}}{t^2}dt\right) + O\left(\frac{1}{x}\right).$$

Let $\gamma = 1 - \int_1^\infty \frac{\{t\}}{t^2}dt$. It is unknown if γ is irrational. □

Remark.

$$\prod_{p\le x}\left(1-\frac{1}{p}\right) \sim \frac{e^{-x}}{\log x}.$$

A similar method can be used to prove other formulas, such as Stirling's formula. Another problem is to show that

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \cdots = \frac{\pi^2}{6}.$$

The point is to compute the sum of the first few terms can lead to a small error because what is left isn't just any random thing. See the homework for details.

15.2. $L(s,\chi)$. Let χ be a character (mod q), $\chi \neq \chi_0$. Then

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad s > 1.$$

We want an expression that makes sense even when $s > 0$. Let

$$S_\chi(x) = \sum_{n \leq x} \chi(n).$$

Then

$$L(s,\chi) = \int_{1^-}^{\infty} \frac{1}{t^s}\, d(S_\chi(t)) = \left.\frac{S_\chi(t)}{t^s}\right|_{1^-}^{\infty} + s\int_{1^-}^{\infty} \frac{S_\chi(t)}{t^{s+1}}\, dt = s\int_1^{\infty} \frac{S_\chi(t)}{t^{s+1}}\, dt.$$

Note that

$$|S_\chi(t)| \leq \phi(q) \quad \text{for all } t \geq 0.$$

Therefore, the preceding integral converges provided that $s \geq 0$. If you thought of this as a complex integral, $s = \sigma + iy$, this converges if $\sigma = \Re s > 0$. Note that we have omitted the case where $\chi = \chi_0$, or the case of the Riemann zeta function. This can also be done for $\zeta(s)$; see the homework. We know that $\zeta(s)$ must blow up at $s = 1$, but we'll get an analog of this feature to get something that makes sense for $s > 0$. This is basically analytic continuation. The point is that if we consider as an example

$$1 + z + z^2 + z^3 + \cdots = \frac{1}{1-z},$$

and the sum makes sense when $|z| \leq 1$, but the right hand side makes sense for $z \neq 1$. They agree when both are well-defined, but one of them is more general. Happily, there is only one way to do this.

Claim. If $\chi \neq \chi_0$ and $\sigma > 0$, then $L(\sigma,\chi)$ is infinitely differentiable.

How do you even differentiate this once? Here,

$$\frac{d}{ds}L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)\frac{d}{ds}\left(e^{-s\log n}\right) = \sum_{n=1}^{\infty} \frac{-\log n\chi(n)}{n^s} = \int_{1^-}^{\infty} -\frac{\log n}{t^s} d(S_\chi(t)).$$

This will be absolutely convergent if $s > 1$, but it actually converges for $s > 0$. Part of the point here is that $\chi(n)$ has positive and negative signs.

$$\left(s\int_1^{\infty} \frac{S_\chi(t)}{t^{s+1}}\, dt\right)' = \int_1^{\infty} \frac{S_\chi(t)}{t^{s+1}}\, dt + s\int_1^{\infty} \frac{S_\chi(t)}{t^{s+1}}(-\log t)\, dt.$$

Now, we should be reasonably happy that $L(\sigma,\chi)$ is once differentiable for all $s > 0$. To be completely rigorously, we want to show

$$\left|\frac{L(\sigma+\delta,\chi) - L(\sigma,\chi)}{\delta} - L'(\sigma,\chi)\right| < \varepsilon.$$

So what we're claiming is that $L(\sigma,\chi)$ are very nice functions.

In particular, if σ is very close to one, we can use Taylor's theorem:

$$L(\sigma,\chi) = L(1,\chi) + (\sigma-1)L'(1,\chi) + \frac{(\sigma-1)^2}{2!}L''(1,\chi) + \cdots.$$

We go back to the prove of Dirichlet's theorem. For $\sigma > 1$, we have

$$\sum_{p \equiv a \pmod q} \frac{1}{p^\sigma} = \frac{1}{\phi(q)} \sum_{\chi \pmod q} \overline{\chi(x)} \left(\log L(\sigma, \chi)\right) + O(1).$$

If $\chi = \chi_0$, we know that

$$\log L(\sigma, \chi) = \log \zeta(\sigma) + O(1) = \log \frac{1}{\sigma - 1} + O(1).$$

Therefore,

$$\sum_{p \equiv a \pmod q} \frac{1}{p^\sigma} = \frac{1}{\phi(q)} \log \frac{1}{\sigma - 1} + \frac{1}{\phi(q)} \sum_{\chi \neq \chi_0} \overline{x(a)} \log L(\sigma, \chi) + O(1).$$

Now, as $\sigma \to 1^+$, $L(\sigma, \chi) \to L(1, \chi)$ is finite for $\chi \neq \chi_0$.

We make a key assumption that $L(1, \chi) \neq 0$ for every $\chi \neq \chi_0$. If this is true, we are done with Dirichlet's Theorem.

15.3. $L(1, \chi)$**.** If χ is a complex character ($\chi \neq \overline{\chi}$), then $L(1, \chi) \neq 0$. Moreover, if χ is a real character, then either $L(1, \chi)$ or $L'(1, \chi)$ is not zero. (If there exists a zero at 1, it must be a simple zero.)

Proof. Suppose that χ is complex. Then

$$L(1, \chi) = 0 \Leftrightarrow L(1, \overline{\chi}) = 0$$

because

$$\sum \frac{\chi(n)}{n} = 0 \Leftrightarrow \sum \frac{\overline{\chi}(n)}{n} = \overline{\sum \frac{\chi(n)}{n}}.$$

Take $a = 1$. Then

$$\sum_{p \equiv 1 \bmod q} = \frac{1}{\phi(q)} \sum \log \frac{1}{\sigma - 1} + \frac{1}{\phi(q)} \sum \log L(\sigma, \chi) + O(1).$$

Now, suppose that $L(\sigma, \chi)$ has a zero of order m_χ at $\sigma = 1$. This means that

$$L(1, \chi) = L'(1, \chi) = \cdots = L^{m_\chi - 1}(1, \chi) = 0.$$

We want to say that $m_\chi = 0$.

We have

$$L(\sigma, \chi) \approx c_\chi (\sigma - 1)^{m_\chi}.$$

Therefore,

$$\begin{aligned} \sum_{p \equiv 1 \bmod q} \frac{1}{p^\sigma} &= \frac{1}{\phi(q)} \left(\log \frac{1}{\sigma - 1} + \sum_{\chi \neq \chi_0} m_\chi \log(\sigma - 1) \right) + O(1) \\ &= \frac{1}{\phi(q)} \left(\log \frac{1}{\sigma - 1} \right) \left(1 - \sum_{\chi \neq \chi_0} m_\chi \right) + O(1). \end{aligned}$$

Since there are a positive number of primes in this residue class, the right hand side needs to be positive, so

$$\sum_{\chi \neq \chi_0} m_\chi \leq 1.$$

□

16. 11/15

Today we should finish the proof of Dirichlet's Theorem.

Here's a quick survey of what we've done so far.

16.1. **Review.** We've found Dirichlet characters $\chi \pmod q$ to isolate the arithemtic progressions. We've also defined absolutely convergent functions

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

When $x \neq \chi_0$, we can extend this to something that makes sense for $s > 0$. We did this last time by writing

$$L(s,\chi) = \int_1^\infty \frac{1}{y^s}\, d(s_\chi(y)) = s\int_1^\infty \frac{s_\chi(y)}{y^{s+1}}\, dy.$$

This is infinitely differentiable. Also, as $s \to 1$, we have that $L(s,\chi) \not\to \infty$. We just need to show that it is nonzero.

Why do we want to do this?

$$\begin{aligned}\sum_{x \pmod q} \overline{\chi(a)} \log L(s,\chi) &= \sum_{\chi \pmod q} \overline{\chi}(a) \sum_{k,p} \frac{\chi(p^k)}{kp^{ks}} \\ &= \phi(q) \sum_{\substack{k,p \\ p^k \equiv a \pmod q}} \frac{1}{kp^{ks}} = \phi(q) \sum_{p \equiv a \pmod q} \frac{1}{p^s} + O(1).\end{aligned}$$

We already know what happens for complex-valued characters. Let's recap that. If s is a real number σ, then all of the terms on the right hand side are positive. Take $a = 1$. Then

$$\sum_{x \pmod q} \log L(s,\chi) = \sum_{\substack{p,k \\ p^k \equiv 1 \pmod q}} \frac{1}{kp^{ks}} \geq 0 \quad \text{if } s > 1.$$

Then

$$\prod_p L(s,\chi) \geq 1.$$

Let $s \to 1^+$. This product contain one term that goes to infinity. This means that there can only be at most one term that goes to zero. First, the product is real because they come in conjugate pairs.

If $L(1,\chi) \to 0$, then by Taylor,

$$|L(s,\chi)| \leq C(s-1) \quad \text{for } s \text{ close to } 1.$$

Now, if χ is a complex character, with $L(1,\chi) = 0$, then $L(1,\overline{\chi}) = 0$ also, and

$$\prod_{\chi \bmod q} L(s,\chi) \leq \frac{C}{s-1} C(s-1)C(s-1)C \leq s-1,$$

where the right hand terms represent χ_0, χ, $\overline{\chi}$, and all other characters. This contradicts that the product is at least 1.

If χ is a real characters, then in the same way (Taylor approximation), Twe see that $L(1,\chi)$ and $L'(1,\chi)$ can't both be zero.

16.2. $L(1,\chi) \neq 0$ **for real characters** χ**.** Now, we just need to show that if χ is a real character (mod q), $L(1,\chi) \neq 0$. We did several examples in the homework. This is the hardest part of the proof. Dirichlet gave a beautiful proof of this: In half of cases, you get something in terms of π, and in other cases, you get things like the golden ratio. We'll discuss that in the next several lectures. Here, we'll give a slick proof that is harder to understand but can be done more quickly.

Define

$$r_\chi(n) = \sum_{d|n} \chi(d) = \sum_{n=ab} \chi(a).$$

This function $r_\chi(a)$ is multiplicative. If $(m,n) = 1$, then

$$r_\chi(m) r_\chi(n) = \sum_{d_1|m} \chi(d_1) \sum_{d_2|n} \chi(d_2) = \sum_{d|mn} \chi(d) = r_\chi(mn).$$

Since this function is multiplicative, we only need to figure out what this does on prime powers. So

$$r_\chi(p^k) = 1 + \chi(p) + \chi(p^2) + \cdots + \chi(p^k) = \begin{cases} k+1 & \chi(p) = 1 \\ 1 & \chi(p) = 0 \\ 0 & \chi(p) = -1, k \text{ odd} \\ 1 & \chi(p) = -1, k \text{ even.} \end{cases}$$

This in particular means that $r_\chi(n) \geq 0$. In addition, $r_\chi(n) \geq 1$ if $n = m^2$ is a perfect square.

Why do we care about this function? This is a nice function to look at.

Example 16.2.1. If χ is a character (mod 1), so that $\chi(n) = 1$ for all n. Then $r_\chi(n) = d(n)$. We proved in the homework that $d(n)$ is bounded by n^ε, and

$$\sum \frac{d(n)}{n^s} = \zeta(s)^2.$$

Example 16.2.2.

$$\sum \frac{r_\chi(n)}{n^s} = \sum_n \sum_{n=ab} \frac{\chi(a)}{a^s} \frac{1}{b^s} = \sum_{a=1}^\infty \frac{\chi(a)}{a^s} \sum_{b=1}^\infty \frac{1}{b^s} = L(s,\chi)\zeta(s).$$

From this perspective, $r_\chi(s)$ seems like a reasonable thing to consider.

Example 16.2.3. Consider $\chi = \chi_{-4}$. In this case,

$$r_\chi(p^k) = \begin{cases} k+1 & p \equiv 1 \pmod 4 \\ 1 & p \equiv 2 \pmod 4 \\ 0 & p \equiv 3 \pmod 4, p \text{ odd} \\ 1 & p \equiv 3 \pmod 4, p \text{ even} \end{cases}$$

This looks like writing numbers as the sum of two squares. Here,

$$r_\chi(p) = \begin{cases} 2 & p \equiv 1 \pmod 4 \\ 0 & p \equiv 3 \pmod 4 \\ 1 & p = 2 \end{cases}$$

So we can interpret $4r_\chi(n)$ as the number of ways of writing $n = x^2 + y^2$. Another way to think about this is prime factorization in the Gaussian integers. There are only eight ways of writing $p = \pi\overline{\pi}$. The point is that $r_\chi(n)$ is something that we should care about.

The idea of the proof is that x is something large. Consider

$$\sum_{n\le x} \frac{r_\chi(n)}{\sqrt{n}}.$$

- Get a lower bound for this, $\ge \frac{1}{2}\log n + O(1)$.
- If $L(1,\chi) = 0$, it is $O(1)$, which is a contradiction, so $L(1,\chi) \neq 0$.

For the first part, we have

$$\sum_{n\le x} \frac{r_\chi(n)}{\sqrt{n}} \ge \sum_{n=m^2\le x} \frac{1}{m} = \sum_{m\le\sqrt{x}} \frac{1}{m} = \log\sqrt{x} + \gamma + O(1) = \frac{1}{2}\log x + O(1).$$

because $r_\chi(n) = 0$ and $r_\chi(m^2) \ge 1$.

16.2.1. *Interlude on the divisor problem.* We want to consider

$$\sum_{n\le x} d(n).$$

This is

$$\begin{aligned}\sum_{n\le x} d(n) &= \sum_{n\le x}\sum_{d|n} 1 = \sum_{d\le x}\sum_{\substack{n\le x\\ d|n}} 1 = \sum_{d\le x} \left\lfloor \frac{x}{d} \right\rfloor = \sum_{d\le x} \left(\frac{x}{d} + O(1)\right)\\ &= x\left(\log x + \gamma + O\left(\frac{1}{x}\right)\right) + O(x) = x\log x + O(x).\end{aligned}$$

This procedure is very wasteful, since the error we get is not so good. Why is the error term not so good? Approximation of the floor is not so good. This is bad when we know more about the floor.

Dirichlet (in a different context) proved an asymptotic formula with error $O(\sqrt{x})$. This is done using the *hyperbola method*. An example of a hyperbola is $ab = x$, we are interested in counting lattice points lying below the hyperbola $ab = x$. Dirichlet's idea is to pick a point (A, B) on the hyperbola. We can count the points inside the hyperbola with $a \le A$, and we have to add back the terms where $A < a$ and $b \le B$. This gives us two cases.

Case 1:

$$\begin{aligned}\sum_{\substack{a,b\\ ab\le x\\ a\le A}} 1 &= \sum_{a\le A}\sum_{b\le x/a} 1 = \sum_{a\le A}\left(\frac{x}{a} + O(1)\right) = x\left(\log A + \gamma + O\left(\frac{1}{A}\right)\right) + O(A)\\ &= x\log A + \gamma x + O(B) + O(A),\end{aligned}$$

and $AB = x$, so choosing $A, B \approx \sqrt{x}$ gives us a nice error.

Case 2:

$$\sum_{\substack{a,b\\ A<a\\ b\le B\\ ab\le x}} 1 = \sum_{b\le B} \sum_{A\le a\le x/b} 1 = \sum_{b\le B} \left(\frac{x}{b} - A + O(1)\right)$$

$$= x\left(\log B + \gamma + O\left(\frac{1}{B}\right)\right) - A(B + O(1)) + O(B)$$
$$= x\log B + \gamma x - x + O(A) + O(B).$$

Putting the two cases together, we see that

$$\sum_{n\le x} d(n) = \sum_{\substack{a,b\\ ab\le x}} 1 = \text{case 1} + \text{case 2}$$
$$= x\log x + (2\gamma - 1)x + O(A + B) = x\log x + (2\gamma - 1)x + O(\sqrt{x}).$$

by choosing $A = B = \sqrt{x}$. Dirichlet conjectured that the error should be $O(x^{\frac{1}{4}+\varepsilon})$. One way is to replace a hyperbola with a circle. The bound of $O(\sqrt{x})$ has been improved to $O(x^{1/3})$, but Dirichlet's conjecture is still unknown.

16.2.2. *Back to* $r_\chi(n)$. We use the hyperbola method to bound

$$\sum_{n\le x} \frac{r_\chi(n)}{\sqrt{n}} = \sum_{n\le x}\sum_{n=ab} \frac{\chi(a)}{\sqrt{a}}\frac{1}{\sqrt{b}} = \sum_{\substack{a,b\\ ab\le x}} \frac{\chi(a)}{\sqrt{a}}\frac{1}{\sqrt{b}}.$$

We again split up into two cases $a \le A$ and $a > A$, $b \le B$.
Case 1:

$$\sum_{a\le A} \frac{\chi(a)}{\sqrt{a}} \sum_{b\le \frac{x}{a}} \frac{1}{\sqrt{b}}$$

For now, let's assume

$$\sum_{n\le t} \frac{1}{\sqrt{n}} = 2\sqrt{t} + C + O\left(\frac{1}{\sqrt{t}}\right);$$

the proof will come soon via partial summation. Then the above sums are

$$= \sum_{n\le A} \frac{\chi(a)}{\sqrt{a}}\left(2\sqrt{\frac{x}{a}} + C + O\left(\sqrt{\frac{a}{x}}\right)\right) = 2\sqrt{x}\sum_{a\le A}\frac{\chi(a)}{a} + C\sum_{a\le A}\frac{\chi(a)}{\sqrt{a}} + O\left(\frac{A}{\sqrt{x}}\right)$$

Case 2:

$$\sum_{b\le B}\frac{1}{\sqrt{b}}\sum_{A<a<x/b}\frac{\chi(a)}{\sqrt{a}}.$$

We don't know much here.

Recall

$$\begin{aligned} L(s,\chi) &= s\int_1^\infty \frac{s_\chi(y)}{y^{s+1}}\,dy = \sum_{n\le z}\frac{\chi(n)}{n^s} + \int_z^\infty \frac{1}{y^s} d(s_\chi(y)) \\ &= \sum_{n\le z}\frac{\chi(n)}{n^s} + \left[\frac{s_\chi(y)}{y^s}\right]_z^\infty + s\int_z^\infty \frac{s_\chi(y)}{y^{s+1}}\,dy \\ &= \sum_{n\le z}\frac{\chi(n)}{n^s} + O\left(\frac{|s_\chi(z)|}{z^s}\right) + O\left(s\int_z^\infty \frac{\phi(q)}{y^{s+1}}\,dy\right), \end{aligned}$$

so

$$L(1,\chi) = \sum_{n\le z}\frac{\chi(n)}{n} + O\left(\frac{\phi(q)}{z}\right)$$

and

$$L(1/2,\chi) = \sum_{n\le z}\frac{\chi(n)}{\sqrt{n}} + O\left(\frac{\phi(q)}{\sqrt{z}}\right).$$

In case 1, we then have that

$$\begin{aligned} &2\sqrt{x}\sum_{a\le A}\frac{\chi(a)}{a} + C\sum_{a\le A}\frac{\chi(a)}{\sqrt{a}} + O\left(\frac{A}{\sqrt{x}}\right) \\ &= 2\sqrt{x}\left(L(1,\chi) + O\left(\frac{\phi(q)}{A}\right)\right) + L(1/2,\chi) + O(\frac{1}{\sqrt{A}}) + O(A/\sqrt{x}). \end{aligned}$$

When $A = B = \sqrt{x}$ and we assume $L(1,\chi) = 0$, this is $O(1)$.

17. 11/17

Today we are actually going to finish the proof of Dirichlet's Theorem.

17.1. **Finishing the proof.** Let's recall where we're at. We want to show that $L(1,\chi) \neq 0$ for real characters χ. This is quite hard.

We were looking at

$$r_\chi(n) = \sum_{d|n}\chi(d) = \sum_{ab=n}\chi(a).$$

Note that $r_\chi(n) \ge 0$, $r_\chi(n) \ge 1$ if $n = m^2$, and

$$\sum_{n\le x}\frac{r_\chi(n)}{\sqrt{n}} \ge \sum_{n\le\sqrt{x}}\frac{1}{m} = \frac{1}{2}\log x + O(1).$$

We will use this fact that we still need to prove later:

$$\sum_{n\le t}\frac{1}{\sqrt{n}} = 2\sqrt{t} + C + O\left(\frac{1}{\sqrt{t}}\right).$$

We want an upper bound, and we used the hyperbola method. The point is to count all points under a hyperbola containing the point $AB = x$, which requires splitting into two regions $a \le A$ and $a > A$, $b \le B$. We will end up choosing $A = B = \sqrt{x}$.

In the first case,

$$\sum_{a\le A}\frac{\chi(a)}{\sqrt{a}}\sum_{b\le x/a}\frac{1}{\sqrt{b}}=2\sqrt{x}\sum_{a\le A}\frac{\chi(a)}{a}+C\sum_{a\le A}\frac{\chi(a)}{\sqrt{a}}+O\left(\frac{A}{\sqrt{x}}\right).$$

In the second case, we will consider

$$\sum_{b\le B}\frac{1}{\sqrt{b}}\sum_{A<a\le x/b}\frac{\chi(a)}{\sqrt{b}}$$

We will keep a q a fixed constant and let $x\to\infty$. We could write

$$L(s,\chi)=\int_1^\infty s\frac{s_\chi(y)}{y^{s+1}}\,dy,$$

where

$$s_\chi(y)=\sum_{a\le y}\chi(a).$$

If you write

$$L(s,\chi)=\sum_{n\le z}\frac{\chi(n)}{n^s}+\int_{z^+}^\infty\frac{d(s_\chi(y))}{y^s},$$

we want to show that the tail is small. Here, $s>0$. To do this, integrate by parts:

$$\int_{z^+}^\infty\frac{d(s_\chi(y))}{y^s}=\frac{s_\chi(y)}{y^s}\bigg|_{z^+}^\infty+s\int_{z^+}^\infty\frac{s_\chi(y)}{y^{s+1}}\,dy=-\frac{s_\chi(z^+)}{z^s}+s\int_{z^+}^\infty\frac{s_\chi(y)}{y^{s+1}}\,dy.$$

Since $|s_\chi(y)|\le\phi(q)=O(1)$, so this integral

$$\left|\int_{z^+}^\infty\frac{s_\chi(y)}{y^{s+1}}\,dy\right|\le\frac{\phi(q)}{z^s}+\phi(q)\int_z^\infty\frac{s}{y^{s+1}}\,dy=2\frac{\phi(q)}{z^s}.$$

Therefore,

$$L(s,\chi)=\sum_{n\le z}\frac{\chi(n)}{n^s}+\int_{z^+}^\infty\frac{d(s_\chi(y))}{y^s}=\sum_{n\le z}\frac{\chi(n)}{n^s}+O\left(\frac{1}{z^s}\right).$$

We can hence genuinely approximate this by taking the first few terms of the series. We can now have bounds for each of the two cases.

In the first case, we now have

$$\begin{aligned}&2\sqrt{x}\left(L(1,\chi)+O\left(\frac{1}{A}\right)\right)+C\left(L(\frac{1}{2},\chi)+O\left(\frac{1}{\sqrt{A}}\right)\right)+O\left(\frac{A}{\sqrt{x}}\right)\\=&2\sqrt{x}L(1,\chi)+CL(\frac{1}{2},\chi)+O\left(\frac{A}{\sqrt{x}}+\frac{\sqrt{x}}{A}+\frac{1}{\sqrt{A}}\right)=O(1),\end{aligned}$$

Plugging in $A=\sqrt{x}$, and assuming to the contrary that $L(1,\chi)=0$, we get a net bounded contribution from case 1.

Now, let's look at case 2. We want to bound

$$\sum_{b\le B}\frac{1}{\sqrt{b}}\sum_{A<a\le x/b}\frac{\chi(a)}{\sqrt{b}}.$$

Here,

$$L(\frac{1}{2},\chi) = \sum_{n\le x/b} \frac{\chi(n)}{\sqrt{n}} + O\left(\sqrt{\frac{b}{x}}\right),$$

and

$$L(\frac{1}{2},\chi) = \sum_{n\le A} \frac{\chi(n)}{\sqrt{n}} + O\left(\sqrt{\frac{1}{A}}\right),$$

so that subtracting gives

$$\sum_{A<A\le x/b} \frac{\chi(a)}{\sqrt{a}} = O\left(\sqrt{\frac{b}{x}} + \frac{1}{\sqrt{A}}\right).$$

Therefore, case 2 gives a contribution of

$$\sum_{b\le B} \frac{1}{\sqrt{b}} O\left(\sqrt{\frac{b}{x}} + \frac{1}{\sqrt{A}}\right) = O\left(\frac{B}{\sqrt{x}}\right) + O\left(\frac{\sqrt{B}}{\sqrt{A}}\right) = O(1)$$

when we set $A = B = \sqrt{x}$.

We can now put the cases together. We have therefore proved that if $L(1,\chi) = 0$,

$$\sum_{n\le x} \frac{r_\chi(n)}{\sqrt{n}} = O(1),$$

which is a contradiction! □

Why doesn't this work for complex characters? The lower bound needed $r_\chi(n)$, which we explicithly computed to be real and taking nice values. You can probably make it work with complex numbers, but it would take a bit of work.

There's one thing that we forgot to check:

$$\sum_{n\le t} \frac{1}{\sqrt{n}} = \int_{1^-}^{t} \frac{d(\sum_{n\le y} 1)}{\sqrt{y}} = \frac{[y]}{\sqrt{y}}\Big|_{1^-}^{x} + \frac{1}{2}\int_1^x \frac{[y]}{y^{3/2}}\,dy.$$

17.2. **Why is $L(1,\chi_{-4}) = \frac{\pi}{4}$?** We saw that

$$r_{\chi_{-4}}(p) = \begin{cases} 2 & p \equiv 1 \pmod 4 \\ 1 & p = 2 \\ 0 & p \equiv 3 \pmod 4. \end{cases}$$

17.2.1. *Counting ways to write as sum of two squares.* This is (almost) counting the number of ways of writing $p = x^2 + y^2$. If $p \equiv 3 \pmod 4$, we proved that this is not possible. If $p = 2$, there are four ways to do this: $(\pm 1)^2 + (\pm 1)^2$. Note that $4 = r_{\chi_{-4}}(2)$. We claim that when $p \equiv 1 \pmod 4$, there are 8 ways.

Write

$$p = x^2 + y^2 = (x+iy)(x-iy) = \pi_1\overline{\pi}_1$$

where $x+iy$ and $x-iy$ are primes in $\mathbb{Z}[i]$. We have unique factorization, so this factorization is unique up to units.

If π is a prime in $\mathbb{Z}[i]$ with norm $N(\pi) = p$, then $p = x^2 + y^2 = (x+iy)(x-iy)$, then either $x + iy = (\pm 1 \text{ or } \pm i)\pi$ or $x - iy = (\pm 1 \text{ or } \pm i)\pi$. This gives our desired 8 solutions.

Therefore, $4r_{\chi_{-4}}(p)$ gives the number of ways of writing p as a sum of two squares. This also works more generally.

If $p \equiv 3 \pmod 4$, there are 4 ways to write p^2 as a sum of two squares: $(\pm p)^2 + 0^2$ and $0^2 + (\pm p)^2$, and indeed, $r_{\chi_{-4}}(p^2) = 1$.

If $p \equiv 1 \pmod 4$, then

$$r^2\pi^2 = p^2 = x^2 + y^2 = (x + iy)(x - iy).$$

Either $r^2 \mid (x + iy)$ or $\pi^2 \mid (x - iy)$ or $x + iy = \text{unit} \cdot p$ and $x - iy = \text{unit} \cdot p$, which gives us a total of 12 solutions.

If $n = pq$, $p, q \equiv 1 \pmod 4$, we have $p = p'\overline{p}'$, $q = q'\overline{q}'$. If $pq = (x + iy)(x - iy)$, then $p'q' \mid (x + iy)$ or $p'\overline{q}' \mid (x + iy)$ or $\overline{p}'q' \mid (x + iy)$ or $\overline{p}'\overline{q}' \mid (x + iy)$.

Now, by examining the prime factorization, we can see that the number of ways of writing $n = x^2 + y^2$ is $4r_{\chi_{-4}}(n)$.

Now, consider

$$\sum_{n \le x} 4r_{\chi_{-4}}(n).$$

We will use the hyperbola method to connect this to $L(1, \chi_{-4})$. We can also write this as

$$\sum_{n \le x} 4r_{\chi_{-4}}(n) = \sum_{n \le x} \{(a, b) : a^2 + b^2 = n\} = \sum_{\substack{(a,b) \\ a^2+b^2 \le x}} 1,$$

which is the number of lattice points inside of a circle of radius $\sqrt{x}$. How many integer points should lie in a circle? This should roughly be

$$= \text{area} + O(\text{circumference}) = \pi x + O(\sqrt{x}).$$

Here, it seems that the error should actually be better: there's a significant amount of cancellation. Things should work out nicely, and it seems like the error should only be $O(x^{1/4+\varepsilon})$. This is a conjecture called Gauss's Circle Problem, and it is closely related to Dirichlet's Divisor Problem. We already know that $O(x^{1/3})$.

17.2.2. *Hyperbola method again.* Consider any character $\chi \neq \chi_0 \pmod q$. Then

$$\sum_{ab \le x} \chi(a) = \sum_{n \le x} r_\chi(n) = \sum_{a \le A} \chi(a) \sum_{b \le x/a} 1 + \sum_{b \le B} \sum_{A < a \le x/b} \chi(a).$$

In case 1,

$$\sum_{a \le A} \chi(a) \left(\frac{x}{a} + O(1) \right) = x(L(1, \chi) + O(\frac{1}{A})) + O(A) = xL(1, \chi) + O(A + \frac{x}{A}),$$

and we again choose $A = \sqrt{x}$.

For case 2,

$$\sum_{b \le B} \sum_{A < a \le x/b} \chi(a) = O\left(\sum_{b \le B} \phi(q) \right) = O(B),$$

so therefore,

$$\sum_{n \le x} r_\chi(n) = xL(1, \chi) + O(\sqrt{x}),$$

choosing $A = B = \sqrt{x}$. Then when $\chi = \chi_{-4}$, we have

$$4\sum_{n\le x} r_{\chi_{-4}}(n) = 4xL(1,\chi) + O(\sqrt{x}) = \pi x + O(\sqrt{x}).$$

Therefore, $L(1,\chi_{-4}) = \frac{\pi}{4}$. Dirichlet found this proof, and he found how this generalizes.

17.2.3. *Binary quadratic forms.* This is something of the form

$$f(x,y) = ax^2 + bxy + cy^2,$$

$a, b, c \in \mathbb{Z}$, $a > 0$. For example, $x^2 + y^2$. We say that such a form is primitive if $(a,b,c) = 1$. The discriminant is $b^2 - 4ac$, which is what we get when we try to complete the square. Here,

$$4af(x,y) = 4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 - dy^2.$$

If $d < 0$, then the binary quadratic form is positive definite. If $d > 0$, then the form is indefinite, taking positive and negative values. In the case $d = m^2$, we get a degenerate situation $(2ax + by + my)(2ax + by - my)$. We only care about the case $d < 0$. For example, in the case $x^2 + y^2$, we have $d = -4$.

In $\mathbb{Q}(\sqrt{5})$, we have

$$\left(\frac{1+\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{2}\right) = -1,$$

so the golden ratio is invertible here. The structure is more complicated for $d > 0$ than for $d < 0$.

The plan is to understand all quadratic forms of a given discriminant. There should be lots of such quadratic forms. There is are three variables $d = b^2 - 4ac$ and one equation, so there should be lots of solutions. Just like $x^5 + y^5 = z^5$.

As an example, $x^2 + y^2 = (x+y)^2 + y^2 = x^2 + 2xy + y^2$. Of course, these are "the same" because there is a nice change of variables. It will turn out that there is only one of discriminant -4, and the number of quadratic forms is called the *class number*.

18. 11/29

The final will be Monday at 8:30am, and it will cover everything through last week.

18.1. **Review of last lecture.** We considered $\chi \pmod 4$. Then

$$4r_\chi(n) = \#\{n = x^2 + y^2\}.$$

Then

$$4\sum_{n\le x} r_\chi(n) = \#\{(x,y) \in \mathbb{Z}^2 : x^2 + y^2 \le x\} = \pi x + O(\sqrt{x}).$$

In addition, we know that

$$r_\chi(a) = \sum_{ab=n} \chi(a).$$

Using the hyperbola method, we proved that

$$\sum_{n\le x} r_\chi(n) = 4xL(1,\chi) + O(\sqrt{x}),$$

and comparing our two formulas gives $L(1,\chi) = \frac{\pi}{4}$.

18.2. **Binary quadratic forms.**

Definition 18.2.1. Binary quadratic forms are expressions of the form $f(x,y) = ax^2+bxy+cy^2$, which has discriminant $D = b^2 - 4ac$.

Completing the square yields

$$4af(x,y) = (2ax+by)^2 - Dy^2.$$

If $a > 0$ and $D < 0$, we see $f(x,y) \geq 0$ is positive definite. If $D > 0$, then $f(x,y)$ is indefinite. If D is a square, then the expression above factors into two linear terms, and we consider this case to be degenerate.

We will mainly focus on the case of $D < 0$. The form is now positive definite. Given a quadratic form, what numbers can be expressed by it?

Question. Describe the numbers represented by a positive definite binary quadratic form $f(x,y)$.

Definition 18.2.2. We say that $f(x,y)$ is *primitive* if $(a,b,c) = 1$.

We will assume throughout that f is primitive.

Definition 18.2.3. n is primitively represented by $f(x,y)$ if $n = f(r,s)$ with $(r,s) = 1$.

We can of course think of a quadratic form in terms of a matrix.

$$f(x,y) = ax^2+bxy+cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

We can make some simplifications on our quadratic form as follows. If we take a form x^2+y^2, we can do a change of variable $x = X+Y$ and $y = Y$, which gives us the new quadratic form $X^2+2XY+Y^2$. Both of these quadratic forms have $D = -4$, and they represent the same numbers – any number that can be represented by one form can also be represented by the other. If x, y are integers, then so are X, Y, and conversely. Understanding one is the same as understanding the other; they are equivalent.

This is really like doing linear algebra. We want to do a change of basis replacing (x,y) by a matrix times (x,y). We need this matrix to be invertible over the integers.

Definition 18.2.4. A quadratic form $f(x,y)$ is equivalent to a form $g(X,Y)$ if there is a matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ with $\alpha,\beta,\gamma,\delta \in \mathbb{Z}$ and the determinant [1] is $\alpha\delta - \beta\gamma = +1$ such that with

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$$

we have $f(x,y) = g(X,Y)$.

We have

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$$

[1] In order for the matrix to be invertible over the integers, we need the determinant to be ± 1. We further restrict it to be $+1$ in this case.

so this is obviously invertible over the integers:

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

We claimed that this is a equivalence relation. Something is equivalent to itself via the identity matrix, and transitivity follows because such matrices form a group via multiplying the two change of basis matrices.

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix},$$

where

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

is the matrix for g. If $g \sim h$ via the matrix $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ then the matrix for h is

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^T \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

Remark. So why do we want to make this definition? What is the point of this? If two quadratic forms are equivalent then their discriminants are the same.

Example 18.2.5. What are the quadratic forms of discriminant -4? There are a lot of these. Starting from $x^2 + y^2$, pick any matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$, which gives a change of variable

$$x = \alpha X + \beta Y$$
$$y = \gamma X + \delta Y$$

and yields a new equivalent quadratic form

$$(\alpha X + \beta Y)^2 + (\gamma X + \delta Y)^2$$

of discriminant -4.

We will reduce all quadratic forms to a finite class of inequivalent quadratic forms.

Theorem 18.2.6. *There are only finitely many inequivalent classes of positive definite binary quadratic forms of a given discriminant.*

18.3. **Proof of the theorem.** We want to give an algorithm to make the coefficients of the quadratic form as small as possible; we like working with quadratic forms like $x^2 + y^2$. This is called induction theory.

18.3.1. *Reduction theory.* Consider

$$ax^2 + bxy + cy^2$$

with the assumption that $a > 0$, $c > 0$, and $D = b^2 - 4ac < 0$. Every such form is equivalent to one with $|b| \leq a \leq c$.

Denote the above quadratic form by $(a, b, c) = ax^2 + bxy + cy^2$. There are two operations that we want to do.

Operation I:

We want to flip x and y to get $x = Y$ and $y = X$. This matrix has determinant -1, so this doesn't quite work. Instead, take $x = -Y$ and $y = X$, yielding matrix $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$. This means that $(a, b, c) \sim (c, -b, a)$.

Operation II:

The other operation is replacing $x = X + nY$ and $y = Y$ for some $n \in \mathbb{Z}$. This corresponds to a matrix $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, which clearly has determinant 1. The inverse is given by $Y = y$ and $X = x - ny$, with matrix $\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$. Under this operation, we have

$$ax^2 + bxy + cy^2 = a(X + nY)^2 + b(X + nY)y + cY^2 = aX^2 + (2an + b)XY + (an^2 + bn + c)Y^2.$$

This yields the equivalence

$$(a, b, c) \sim (a, 2an + b, an^2 + bn + c).$$

Algorithm 18.3.1. Start with (a, b, c).

(1) Choose n so that $|2an + b| \leq a$ and use operation II. We get (a_1, b_1, c_1) with $|b_1| \leq a_1$.
(2) If $c_1 \leq a_1$, use operation I to flip $(c_1, -b_1, a_1)$.
(3) Repeat as needed.

This clearly terminates because one of the variables always decreases. This can also be seen from the following nice geometric process.

18.3.2. *Geometric view.* Let $\mathbb{H}$ be the upper half plane, so that

$$\mathbb{H} = \{x + iy : y > 0\}.$$

Consider any matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$, with $a, b, c, d \in \mathbb{R}$ and $ad - bc = 1$. This matrix can act on the upper half plane via the *Mobius transformation*

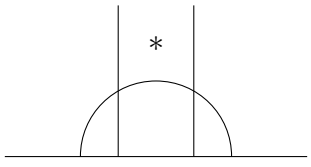
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + d}{cz + d},$$

and

$$\Im \frac{az + d}{cz + d} = \frac{y}{|cz + d|^2}.$$

Every point of $\mathbb{H}$ is equivalent under $SL_2(\mathbb{Z})$ to a point

Draw the lines $x = 1/2$, $x = -1/2$, and the unit circle. Take the region between the two vertical lines and above the circle. This region is called the *fundamental domain*.



Now,

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} z = z + n,$$

so the first step of the algorithm moves z until it lies between the vertical lines $x = 1/2$ and $x = -1/2$. Now,

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} z = -\frac{1}{z}.$$

We flip this point, causing it to lie above the circle (but possibly messing up the real coordinate), and we repeat.

The argument on binary quadratic forms is exact the same as the algorithm to put

$$\frac{-b + \sqrt{D}}{2a}$$

inside this fundamental domain.

Given (a, b, c) and if $|b| = a$ choose $b > 0$, then we have

$$(a, a, c) \sim (a, -a, c) \quad \text{if } a < c$$

and if $a = c$ if

$$(a, b, a) \sim (a, -b, a).$$

Definition 18.3.2. A binary quadratic form is called *reduced* if $|b| \leq a \leq c$ and

(1) if $|b| = a$ then choose $b > 0$
(2) if $a = c$ then choose $b \geq 0$.

Every positive definite binary quadratic form is equivalent to a (unique) reduced form.1

Two reduced forms are inequivalent (to be justified later).

We want to compute all reduced forms of a given discriminant. We will give an upper bound for a, giving a finite number of choices for a, b. Then c is fixed by the discriminant $D = b^2 - 4ac$, $D < 0$. For a reduced form (a, b, c), we have $|D| = 4ac - b^2 \geq 4ac - a^2 \geq 4a^2 - a^2 = 3a^2$, so therefore

$$a \leq \sqrt{\frac{|a|}{3}}.$$

There are only finitely many choices for a. For each, there are a finite number of choices for b and hence for c.

The number of real binary quadratic forms of a given discriminant D is called the *class number* $h(D)$. We've shown that this is a finite number.

Example 18.3.3. $D = -4$. We require

$$a \leq \sqrt{\frac{4}{3}} \implies a = 1.$$

This means that $|b| \leq 1$ and $b^2 - 4ac = -4$. Note that b has the same parity as the discriminant, so b is even and hence $b = 0$ and $c = 1$. So there is only one quadratic form of discriminant -4, and this is $x^2 + y^2$. The class number is 1.

Example 18.3.4. $D = -3$. We now want

$$a \leq \sqrt{\frac{3}{3}} \implies a = 1.$$

Then b is odd and $|b| \leq 1 \implies b = \pm 1$. Then $c = 1$. But we said that if $a = |b|$ then we choose $b \geq 0$, so $x^2 + xy + y^2$ is the unique equivalence class of quadratic forms of discriminant -3.

Note that $D = -5$ is impossible; the only allowed discriminants are those equivalent to 0 or 1 (mod 4).

18.4. **Sum of two squares revisited.** We again prove that if $p \equiv 1 \pmod 4$ then $p = x^2 + y^2$.

Proof. We have

$$\left(\frac{-1}{p}\right) = 1$$

and

$$\left(\frac{-4}{p}\right) = 1,$$

so $-4 \equiv n^2 \pmod p$, so then $-4 = n^2 - pc$. So we get a solution to $-4 \equiv n^2 \pmod{4p}$ by the Chinese Remainder Theorem. This gives $-4 = n^2 - 4pc$. Consider the quadratic form $px^2 + nxy + cy^2$ of discriminant -4. □

We will also consider forms of the form $x^2 + 3y^2$.

19. 12/1

19.1. **Reduced binary quadratic forms.** Last time we were looking at binary quadratic forms $ax^2 + bxy + cy^2$ where $(a, b, c) = 1$, $a, c > 0$, and $b^2 - 4ac < 0$. We proved the following:

Theorem 19.1.1 (Reduction Theory)**.** *Each form is equivalent to a form with $|b| \le a \le c$ and $D = b^2 - 4ac$ with the caveat that if $|b| = a$ then choose b positive, and if $a = c$ then choose b positive.*

Keep in mind that b has the same parity as the discriminant D and $D \equiv 0, 1 \pmod 4$.

Last time, we gave an algorithm for producing reduced forms. We didn't prove, however, that two reduced forms are inequivalent, and we sketch the proof here. It's a sketch because it's like a calculus exercise.

Proof. Suppose we have a reduced form $f(x, y) = ax^2 + bxy + cy^2$. We gave the bound last time of

$$a \le \sqrt{\frac{|D|}{3}}.$$

What is the smallest value represented by f? We want to show that this is $a = f(\pm 1, 0)$. Other numbers that are represented are $c = f(0, \pm 1)$ and $a + b + c = f(1, 1)$. Choose ± 1 and ± 1 such that $a - |b| + c = f(\pm 1, \pm 1)$.

The smallest number represented is a and the second smallest number that is properly[2] represented is c, and the third smallest properly represented is $a - |b| + c$. This is left as an exercise to think through. The general idea is that

$$f(x, y) \ge ax^2 - |b|\left(\frac{x^2 + y^2}{2}\right) + cy^2 \ge \left(a - \frac{|b|}{2}\right)x^2 + \left(c - \frac{|b|}{2}\right)y^2 \ge (a - |b| + c)\min(x^2, y^2).$$

Given this fact, two reduced forms must be inequivalent, because the smallest numbers that they represent will give the coefficients a and c and then b. There are a few special cases to think through – what happens for $a = c$? □

[2]Proper means $(x, y) = 1$.

Now we've given a complete theory of producing inequivalent reduced forms. The number of reduced forms is the class number, denoted by $h(D)$.

Example 19.1.2. When $D = -4$, we have $h(-4) = 1$, and the only reduced form is $x^2 + y^2$.

Example 19.1.3. When $D = -3$, we have $h(-3) = 1$, and the only reduced form is $x^2 + xy + y^2$.

Example 19.1.4. When $D = -7$, we want

$$a \leq \sqrt{7/3} \implies a = 1.$$

In addition, $|b| \leq a$ and b is odd so $b = 1$. Then by the discriminant, we get $c = 2$ and the only reduced form is $x^2 + xy + 2y^2$.

Example 19.1.5. For $D = -8$, then as above, $a = 1$, and b must be even so $b = 0$, and the only reduced form is $x^2 + 2y^2$.

Example 19.1.6. $D = -12$. Here, $a \leq 2$. If $a = 1$ then $b = 0$, and we get $x^2 + 3y^2$ as a reduced form. If $a = 2$, then b can be 0 or 2. If $b = 0$, we cannot get a value for c, while if $b = 2$, we get $c = 2$, and so we get $2x^2 + 2xy + 2y^2 = 2(x^2 + xy + y^2)$, which isn't primitive. In this case, we also see that $h(-12) = 1$.

There are only finitely numbers with class number 1, so let's do an example where the class number is more than one.

Example 19.1.7. $D = -20$. Here, $a \leq 2$. In the case $a = 1$, we have $b = 0$, so $c = 5$. This is the form $x^2 + 5y^2$.

In the case $a = 2$, b must be even, so $b = 0$ or $b = 2$. If $b = 0$ then $-20 = -4 \times 2 \times c$ is not possible, and if $b = -2$ then $c = 3$, and we get a second reduced form $2x^2 + 2xy + 3y^2$.

Therefore, $h(-20) = 2$.

We see that as the discriminant gets larger, we have to consider more and more cases, and there's a good chance something works.

Remark. If $D \equiv 0, 1 \pmod 4$ then $h(D) \geq 1$. Why?

If $D \equiv 0 \pmod 4$ then use $x^2 - \frac{D}{4}y^2$, and if $D \equiv 1 \pmod 4$ then use $x^2 + xy + \frac{1-D}{4}y^2$.

Why is the theory of binary quadratic forms very pretty?

Let n be odd, and suppose that $(n, D) = 1$. We want to know: Can $n = f(x, y)$ for some binary quadratic form f of discriminant D and $(x, y) = 1$?

Suppose that p and q are coprime, and $f(p, q) = n$. We go back to the Euclidean Algorithm to claim that we can find r and s such that

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} \in SL_2(\mathbb{Z}).$$

If we make a change of basis

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} p & r \\ q & s \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix},$$

we get a transformation

$$\begin{aligned} f(x, y) &\to g(X, Y) = nx^2 + (B)xy + (C)y^2 \\ f(p, q) &\to g(1, 0). \end{aligned}$$

Since f and g has the same discriminant, we must have $D = B^2 - 4Cn$, which means that D is congruent to a square (mod n).

This is actually an equivalent condition. Conversely, if D is a square (mod n), then n is represented properly by a binary quadratic form of discriminant D. This is because we can write $D = b^2 - (\cdot)n$. We would love to have $(\cdot)$ divisible by 4. How can we rig it so that it is even? We want b to have the same parity of D. We can rewrite the previous expression by $D = (b+n)^2 - (\cdot)n$. Since n is odd, b or $b+n$ has the same parity as D. So we do have a solution to $D = b^2 - 4nc$. Then $nx^2 + bxy + cy^2$ is a form of discriminant D and it represents n. This is actually a beautiful theorem.

This gives us a lot of consequences.

Example 19.1.8. $D = -4$. When is -4 congruent to a square (mod n)? If $n = p$ is prime then $p \equiv 1 \pmod 4$.

Example 19.1.9. $D = -8$, with form $x^2 + 2y^2$. When is $p = x^2 + 2y^2$? We want -8 to be a square (mod p), which requires

$$\left(\frac{-8}{p}\right) = 1 \implies p = \begin{cases} 3 \pmod 8 \\ 1 \pmod 8. \end{cases}$$

Remark. Quadratic reciprocity told us that $\left(\frac{-8}{p}\right)$ depends on $p \pmod 8$.

In general, if p is an odd prime, $(p, D) = 1$, then when is $\left(\frac{D}{p}\right) = 1$? This only depends (by quadratic reciprocity) on $p \pmod{|D|}$.

Example 19.1.10. $D = -12$. There is one reduced form $x^2 + 3y^2$. To be represented by this form $p = x^2 + 3y^2$, we want $\left(\frac{-12}{p}\right) = 1 \Leftrightarrow \left(\frac{-3}{p}\right) = 1$, which means that $p \equiv 1 \pmod 3$ by quadratic reciprocity. For example, if $p = 1 \pmod 4$, we see that $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1$.

Example 19.1.11. $D = -20$. We have two reduced forms $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$. If we choose a prime $p \neq 2, 5$, we want to ask if p can be properly represented by a form of discriminant -20, which requires $\left(\frac{-20}{p}\right) = 1$.

Suppose that $p \equiv 1 \pmod 4$. Then we want

$$\left(\frac{5}{p}\right) = 1 = \left(\frac{p}{5}\right) \implies p \equiv 1, 4 \pmod 5$$

In the case that $p \equiv 3 \pmod 4$, so we want

$$\left(\frac{-20}{p}\right) = 1 \implies \left(\frac{5}{p}\right) = -1 = \left(\frac{p}{5}\right) \implies p \equiv 2, 3 \pmod 5.$$

Combining these conditions, we see that the primes that work are $p \equiv 1, 3, 7, 9 \pmod{20}$. For these p, either $p = x^2 + 5y^2$ or $p = 2x^2 + 2xy + 3y^2$.

Eventually, this kind of statement is all you can say. But here we have an extra piece of luck: $p = x^2 + 5y^2$ requires $p \equiv 1, 4 \pmod 5$, while $p = 2x^2 + 2xy + 3y^2 = (2x + y)^2 + 5y^2$ requires $p \equiv 2, 3 \pmod 5$.

Now, if $p \equiv 1, 9 \pmod{20}$ then $p = x^2 + 5y^2$, and if $p \equiv 3, 7 \pmod{20}$ then $p = 2x^2 + 2xy + 3y^2$. Euler wrote down these types of results and Gauss did the general theory, which he called *genus theory*.

We want to connect this back to L-functions. This related to why we get nice values like $\frac{\pi}{4}$.

19.2. **Relation to L-functions.** If n is odd and $(n, D) = 1$, what does it mean to say that D is a square (mod n).

Suppose that $n = p_1 \dots p_k$ (square-free). Then $\left(\frac{D}{p_i}\right) = 1$ for each p_i, $i = 1, 2, \dots, k$.

Notice that

$$\prod_{i=1}^{k} \left(1 + \left(\frac{D}{p_i}\right)\right) = 0$$

unless D is a square (mod $p_1 \dots p_k$). Multiplying this product, there are 2^n terms, sort of like the divisor function.

Extend the Legendre symbol to all numbers via

$$\left(\frac{D}{n}\right) = \prod_{p^\alpha || n} \left(\frac{D}{p}\right)^\alpha.$$

Note that this is completely multiplicative and periodic, so it is a character (mod $|D|$). There are a few things to be checked here. Applying this,

$$\prod_{i=1}^{k} \left(1 + \left(\frac{D}{p_i}\right)\right) = \sum_{n=ab} \left(\frac{D}{b}\right)$$

Assume that $D < 0$, and D is called a fundamental discriminant, which means that $D \neq a^2 b$ with b is a discriminant and $a > 1$. For example, $-12 = -3 \cdot 4$ is not a fundamental discriminant, but -20 is a fundamental discriminant even though $-20 = -5 \cdot 4$ because -5 is not a discriminant.

Then we have $\chi(n) = \left(\frac{D}{n}\right)$ is a real character (mod $|D|$). Then

$$r_\chi(n) = \sum_{ab=n} \chi(b),$$

and

$$2r_\chi(n) = \#\{n = f(x, y) : f \text{ over } \textit{all} \text{ reduced forms of discriminant 1, and } (x, y) \in \mathbb{Z}^2\}.$$

(We have two special cases. If $D = -3$, use $6r_\chi(n)$, and if $D = -4$, use $4r_\chi(n)$.)

Now, like we did with characters (mod 4), we use the hyperbola method to get that

$$\sum_{n \leq x} 2r_\chi(n) \sim 2L(1, \chi)x.$$

This is also equal to

$$\sum_{\substack{f=\text{red. bin. quad. forms} \\ ax^2+bxy+cy^2}} \sum_{\substack{(x,y) \\ f(x,y) \leq X}} 1.$$

This is an ellipse $ax^2 + bxy + cy^2 \leq X$. How many lattice points are inside the ellipse? The answer is roughly the area of the ellipse, and we can work this out. We get

$$\sum_{\substack{f=\text{red. bin. quad. forms} \\ ax^2+bxy+cy^2}} \sum_{\substack{(x,y) \\ f(x,y) \leq X}} 1 \sim \frac{2\pi X}{\sqrt{|D|}}.$$

It's the same answer for every reduced binary quadratic form, so we end up getting

$$\sum_{n \le x} 2r_\chi(n) \sim 2L(1,\chi)x \sim \frac{2\pi X}{\sqrt{|D|}} h(D),$$

so for $D < -4$, we get

$$L(1,\chi) = \frac{\pi h(D)}{\sqrt{|D|}},$$

which is an amazing theorem of Dirichlet. This tells us why the some of the L-functions are nonzero. In the other case, we count lattice points inside a hyperbola and do the same thing.

19.3. **Why is $n^2 + n + 41$ a prime?** We can show that the class number of $D = -163$ is -1. This is rather surprising. We want

$$a \le \sqrt{\frac{163}{3}} \implies a \le 7.$$

So we have to check that $a = 2, 3, 4, 5, 6, 7$, and b is odd. It's not too bad, we just have to check. We get that the only reduced quadratic form $x^2 + xy + 41y^2$.

So then $n^2 + n + 41 = f(n, 1)$. If $n \le 39$, then we can check that $f(n, 1) = 41$. Suppose that $f(n, 1)$ is composite. This means that there exists a prime $p < 41$ with $p \mid f(n, 1)$, which means that -163 is a square (mod n), which means that -163 is a square (mod p), which means that p is represented by some form of discriminant -163. But this form cannot represent numbers between 1 and 41, so we're done.

This actually generalizes. If $h(1 - 4A) = 1$, then $n^2 + n + A$ is prime for $n \le A - 1$. Sadly, the largest value for which this works is -163. This is Gauss's class number problem, and it was solved in the 1950s.

E-mail address: moorxu@stanford.edu