PROMYS 2012 - Analytic Class Number Formula

lectures by Jared Weinstein

notes by Zev Chonoles

Lecture 1 July 2, 2012

The motivating example of a class number formula is

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots = \frac{\pi}{4}$$

This is sometimes called the Gregory series.

For $|u| < 1$,

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

Now integrate both sides:

$$\int_0^1 1 - u^2 + u^4 - u^6 + \cdots \; du = \int_0^1 \frac{1}{1+u^2} \; du = \tan^{-1}(u)\Big|_0^1 = \frac{\pi}{4}$$
$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots$$

The alternation of the signs is related to the Legendre symbol.

Let $\chi(n) =$ the nth term in the sequence $1, 0, -1, 0, 1, 0, -1, \ldots$, which is periodic with period 4.

Observations: $\chi(nm) = \chi(n)\chi(m)$. Also, $\chi(p) = (-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right)$ for p an odd prime, where $\left(\frac{-}{p}\right)$ is the Legendre symbol. χ is an example of a Dirichlet character.

Theorem. *There are infinitely many primes.*

Proof (Euler-style). We can see that the harmonic series diverges by

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots \geq 1 + \frac{1}{2} + \underbrace{\frac{1}{4} + \frac{1}{4}}_{\frac{1}{2}} + \underbrace{\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}}_{\frac{1}{2}} + \cdots$$

But notice that the harmonic series is equal to

$$\left(1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots\right)\left(1 + \frac{1}{3} + \frac{1}{9} + \frac{1}{27} + \cdots\right)\left(1 + \frac{1}{5} + \frac{1}{25} + \frac{1}{125} + \cdots\right)\cdots$$

by "FOIL"ing out the product and using unique factorization.

Each of the terms in this product is a geometric series, so the product is equal to

$$\frac{1}{1-\frac{1}{2}} \cdot \frac{1}{1-\frac{1}{3}} \cdot \frac{1}{1-\frac{1}{5}} \cdots$$

The fact that this diverges implies that there exist infinitely many primes (if there were finitely many, we would just have a product of finitely many numbers, which of course exists). □

Trick for avoiding divergent series:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

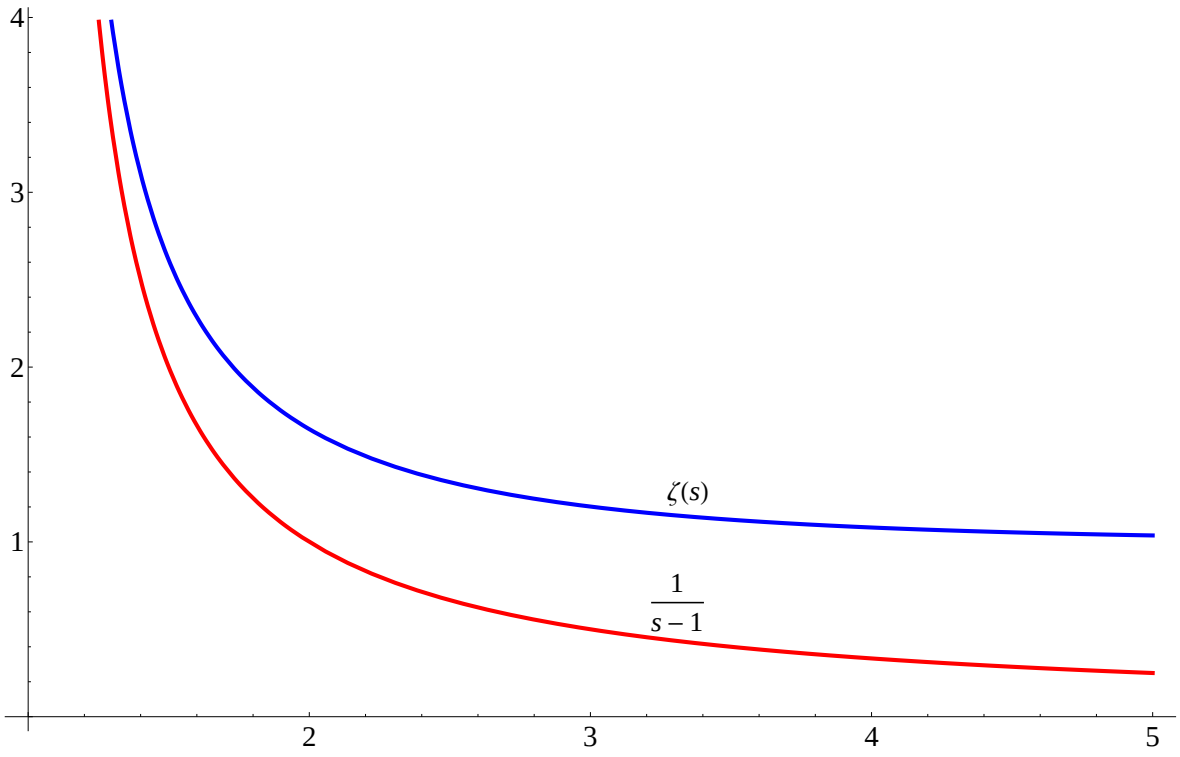
This is the Riemann zeta function. It converges when $s > 1$. Euler's factorization looks like

$$\zeta(s) = \frac{1}{1 - \frac{1}{2^s}} \cdot \frac{1}{1 - \frac{1}{3^s}} \cdot \frac{1}{1 - \frac{1}{5^s}} \cdots = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

Graph:

Theorem. *The limit* $\lim_{s \to 1} \zeta(s) - \frac{1}{s-1}$ *exists.*

This theorem is saying that, even though $\lim_{s \to 1} \zeta(s)$ is infinite (because it becomes the harmonic series), and even though $\lim_{s \to 1} \frac{1}{s-1}$ is infinite, their growth is so matched that the limit of their *difference* exists.



Proof. Using "summation by parts",

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots = \left(1 - \frac{1}{2^s}\right) + 2\left(\frac{1}{2^s} - \frac{1}{3^s}\right) + 3\left(\frac{1}{3^s} - \frac{1}{4^s}\right) + \cdots$$

$$= s\int_1^2 \frac{1}{x^{s+1}}\,dx + s\int_2^3 \frac{2}{x^{s+1}}\,dx + s\int_3^4 \frac{3}{x^{s+1}}\,dx + \cdots = s\int_1^\infty \frac{\lfloor x \rfloor}{x^{s+1}}\,dx$$

where $\lfloor x \rfloor$ is the floor of x. Recall that for any x, we can break it into $x = \lfloor x \rfloor + \langle x \rangle$, where $0 \le \langle x \rangle < 1$. Thus

$$s\int_1^\infty \frac{\lfloor x \rfloor}{x^{s+1}}\,dx = s\int_1^\infty \frac{x}{x^{s+1}}\,dx - s\int_1^\infty \frac{\langle x \rangle}{x^{s+1}}\,dx = \frac{s}{s-1} - sg(s)$$

where $g(s) = \int_1^\infty \frac{\langle x \rangle}{x^{s+1}}\,dx$. Note that

$$\lim_{s \to 1^+} g(s) = \int_1^\infty \frac{\langle x \rangle}{x^2}\,dx < \int_1^\infty \frac{1}{x^2}\,dx = 1$$

Therefore

$$\lim_{s\to 1^+} \zeta(s) - \frac{s}{s-1}$$

exists, and $\frac{s}{s-1} = 1 + \frac{1}{s-1}$. □

Corollary 1. *The series*

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots$$

diverges.

Proof. Fact 1 (easily follows from our theorem):

$$\lim_{s\to 1^+} \zeta(s)(s-1) = 1$$

Fact 2:

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

Taking the $\log$ of both sides of fact 2,

$$\log(\zeta(s)) = \sum_{p \text{ prime}} \log\left(1 - \frac{1}{p^s}\right)^{-1}$$

The Taylor series of $\log(1-x)^{-1}$ is

$$\log(1-x)^{-1} = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots$$

so

$$\log(\zeta(s)) = \sum_{p \text{ prime}} \left[\frac{1}{p^s} + \frac{1}{2p^{2s}} + \frac{1}{3p^{3s}} + \cdots\right] = \sum_{p \text{ prime}} \frac{1}{p^s} + h(s)$$

where $h(s)$ is "the trash". I could prove for you that $\lim_{s\to 1^+} h(s)$ exists, but it's really not that interesting. But taking that as a given,

$$\lim_{s\to 1^+} \log(\zeta(s)) = \sum_{p \text{ prime}} \frac{1}{p} + (\text{limit of } h(s))$$

but $\lim_{s\to 1^+} \log(\zeta(s))$ doesn't exist because $\lim_{s\to 1^+} \zeta(s)$ doesn't exist, so the only possibility is that $\sum_{p \text{ prime}} \frac{1}{p}$ doesn't exist, i.e. the sum diverges.

Fact 1 lets us get something stronger:

$$\lim_{s\to 1^+} \left(\sum_{p \text{ prime}} \frac{1}{p^s} - \log\left(\frac{1}{s-1}\right)\right) \quad \text{exists.}$$

Theorem. *There are infinitely many primes of the form* $4k+1$.

Proof. If $p_1, \ldots, p_n$ are all the primes of the form $4k+1$, let $N = 4(p_1 \cdots p_n)^2 + 1$. If $p \mid N$, then the fact that there exists x such that $x^2 + 1 \equiv 0 \bmod p$ implies that p is of the form $4k+1$, but this can't be one of the p_i, so this is a contradiction. □

A similar proof works to show that there are infinitely many primes of the form $4k+3$.

Let

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

Then we know that $\lim_{s\to 1^+} L(s) = \frac{\pi}{4}$. The function $L(s)$ also has an Euler factorization, because the function χ is multiplicative:

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

Thus, as before,

$$\log(L(s)) = \sum_{p \text{ prime}} \log\left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

and again we can "throw away" all but the linear terms in the Taylor series.

$$\log(L(s)) = \sum_{p \text{ prime}} \frac{\chi(p)}{p^s} + g_1(s)$$

where $\lim_{s\to 1^+} g_1(s)$ exists. Recall that

$$\log(\zeta(s)) = \sum_{p \text{ prime}} \frac{1}{p^s} + g(s)$$

where $\lim_{s\to 1^+} g(s)$ exists. As $s \to 1^+$, $\log(L(s))$ converges, and $\log(\zeta(s))$ diverges. Thus,

$$\text{this diverges } \longrightarrow \frac{1}{2}(\log(\zeta(s)) + \log(L(s))) = \sum_{\substack{p \text{ prime} \\ p \equiv 1 \bmod 4}} \frac{1}{p^s} + (\text{converges})$$

Thus, there are infinitely many primes that are $1 \bmod 4$, and what this tells us is that in fact

$$\sum_{\substack{p \text{ prime} \\ p \equiv 1 \bmod 4}} \frac{1}{p}$$

diverges. Taking $\log(L(s)) - \log(\zeta(s))$ instead of $\log(L(s)) + \log(\zeta(s))$ gives us the same conclusion for primes that are $3 \bmod 4$. □

Last time, we talked about the Riemann zeta function

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

which converges for $s > 1$, and which has a pole at $s = 1$. It has the (very important) Euler factorization

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

which is a consequence of unique factorization in $\mathbb{Z}$. We also know "how fast" the function $\zeta(s)$ blows up:

$$\lim_{s \to 1^+} \left(\zeta(s) - \frac{1}{s-1}\right) \text{ exists.}$$

We saw that this impies that $\sum_{p \text{ prime}} \frac{1}{p}$ diverges.

Now, we'll transport these facts to other number systems. The first number system we see after $\mathbb{Z}$ is the Gaussian integers, $\mathbb{Z}[i]$.

Facts about $\mathbb{Z}[i]$:

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

The inverse of $a + bi \in \mathbb{Q}(i)$ is given by

$$\frac{1}{a+bi} = \frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{a-bi}{a^2+b^2}$$

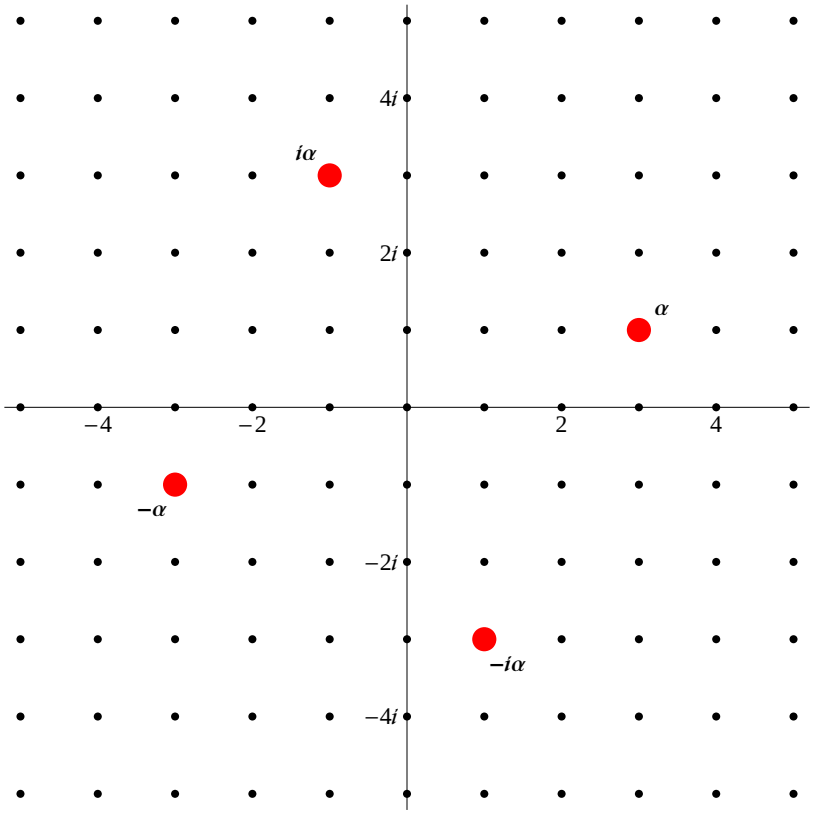
Complex conjugation is defined by $\overline{a+bi} = a - bi$, and it satisfies $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$.

Student(s): Why did you write $\mathbb{Z}[i]$ with square brackets and $\mathbb{Q}(i)$ with parentheses?

$\mathbb{Z}(i)$ not a good notation.

The norm of $\alpha = a + bi$ is defined to be $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$.

The units of $\mathbb{Z}[i]$ are $1, -1, i, -i$. We say that α and β are associates if $\alpha = \beta u$ where u is a unit. Recall that $\alpha \mid \beta$ and $\beta \mid \alpha$ if and only if α and β are associates. Here are the associates of $\alpha = 3 + i$:



What are some of the primes of $\mathbb{Z}[i]$?

Student(s): $1+i$

Right. The prime $1+i$ is weird for a lot of reasons. One is that its conjugate is also an associate: we have

$$\overline{1+i} = 1-i = (-i)(1+i).$$

Another class of primes of $\mathbb{Z}[i]$ are $\pi = a+bi$ where $N(\pi) = a^2+b^2 = p \equiv 1 \bmod 4$. Note that π and $\overline{\pi}$ are not associates; for example, $\pi = 2+3i$ and $\overline{\pi} = 2-3i$.

The final class of primes of $\mathbb{Z}[i]$ are primes p of $\mathbb{Z}$ such that $p \equiv 3 \bmod 4$. Note that $N(p) = p^2$.

(plot of primes in $\mathbb{Z}[i]$)

Let's review the division algorithm in $\mathbb{Z}[i]$. Given $\alpha, \beta \in \mathbb{Z}[i]$, and $\beta \neq 0$, the number $\frac{\alpha}{\beta}$ need not be in $\mathbb{Z}[i]$, but we can always find some $\gamma \in \mathbb{Z}[i]$ such that

$$\sqrt{N\left(\frac{\alpha}{\beta} - \gamma\right)} \leq \frac{\sqrt{2}}{2}$$

$$N\left(\frac{\alpha}{\beta} - \gamma\right) \leq \frac{1}{2}$$

$$N(\underbrace{\alpha - \gamma\beta}_{r}) \leq \frac{1}{2}N(\beta) < N(\beta)$$

so we have $\alpha = \gamma\beta + r$ and $N(r) < N(\beta)$.

Because we have the division algorithm in $\mathbb{Z}[i]$, we also get unique factorization in $\mathbb{Z}[i]$. If $\alpha \in \mathbb{Z}[i]$, $\alpha \neq 0$ or a unit, then $\alpha = \pi_1 \cdots \pi_t$ where the $\pi_i \in \mathbb{Z}[i]$ are primes. This is unique up to reordering and associates.

Now back to the zeta function,

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

We want to define a version for $\mathbb{Q}(i)$. We might try

$$\zeta_{\mathbb{Q}(i)}(s) = \sum_{\alpha \in \mathbb{Z}[i]} \frac{1}{N(\alpha)^s},$$

but we have a few problems. We can't define by 0, and we're also overcounting. The right definition is

$$\zeta_{\mathbb{Q}(i)}(s) = \sum_{\substack{\alpha \in \mathbb{Z}[i] \\ \alpha \neq 0 \\ \text{up to associates}}} \frac{1}{N(\alpha)^s} = \frac{1}{4} \sum_{\alpha \neq 0} \frac{1}{N(\alpha)^s} = \sum_{\substack{(a,b) \\ a>0, b \geq 0}} \frac{1}{(a^2+b^2)^2}$$

Let's calculate the first few terms:

$$\zeta_{\mathbb{Q}(i)}(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{0}{3^s} + \frac{1}{4^s} + \frac{2}{5^s} + \frac{0}{6^s} + \frac{0}{7^s} + \frac{1}{8^s} + \frac{1}{9^s} + \cdots = \sum_{n=1}^{\infty} \frac{r(n)}{n^s}$$

where $r(n) =$ number of ways to write $n = a^2 + b^2$, where $a, b \geq 0$. We have that

$$r(p) = \begin{cases} 1 & \text{if } p = 2, \\ 0 & \text{if } p \equiv 3 \bmod 4, \\ 2 & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

This function $\zeta_{\mathbb{Q}(i)}(s)$ is called the Dedekind zeta function for $\mathbb{Q}(i)$. It also has an Euler factorization, using the same idea as the one for $\zeta(s)$, namely, unique factorization:

$$\zeta_{\mathbb{Q}(i)}(s) = \prod_{\substack{\pi \text{ prime} \\ \text{up to associates}}} \left(1 + \frac{1}{N(\pi)^s} + \frac{1}{N(\pi)^{2s}} + \cdots\right) = \prod_{\substack{\pi \text{ prime} \\ \text{up to associates}}} \left(1 - \frac{1}{N(\pi)^s}\right)^{-1}$$

The primes of $\mathbb{Z}[i]$ were split into three classes, so let's do the same for our Euler factorization:

$$\zeta_{\mathbb{Q}(i)}(s) = \left(1 - \frac{1}{2^s}\right)^{-1} \prod_{\substack{p \text{ prime} \\ p \equiv 1 \bmod 4}} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{\substack{p \text{ prime} \\ p \equiv 3 \bmod 4}} \left(1 - \frac{1}{p^{2s}}\right)^{-1}$$

We can factor the terms in the third part:

$$\zeta_{\mathbb{Q}(i)}(s) = \left(1 - \frac{1}{2^s}\right)^{-1} \prod_{\substack{p \text{ prime} \\ p \equiv 1 \bmod 4}} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{\substack{p \text{ prime} \\ p \equiv 3 \bmod 4}} \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{-1}$$

$$= \zeta(s) \prod_{\substack{p \text{ prime} \\ p \equiv 1 \bmod 4}} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{\substack{p \text{ prime} \\ p \equiv 3 \bmod 4}} \left(1 + \frac{1}{p^s}\right)^{-1}$$

We can write this as

$$\zeta_{\mathbb{Q}(i)}(s) = \zeta(s) \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

where $\chi(n)$ is the nth term in the sequence $0, 1, 0, -1, 0, 1, \ldots$ and specifically $\chi(p) = \left(\frac{-1}{p}\right)$. We define a new function from this,

$$\zeta_{\mathbb{Q}(i)}(s) = \zeta(s)L(s,\chi) = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Note that for two sequences a_n and b_n,

$$\left(\frac{a_1}{1^s} + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \cdots\right)\left(\frac{b_1}{1^s} + \frac{b_2}{2^s} + \frac{b_3}{3^s} + \cdots\right) = \frac{c_1}{1^s} + \frac{c_2}{2^s} + \frac{c_3}{3^s} + \cdots$$

where

$$c_n = \sum_{d|n} a_d b_{n/d}.$$

Thus, we have that $r(n) = \sum_{d|n} \chi(d)$. Let's do some examples:

$$r(17) = \chi(1) + \chi(17) = 1 + 1 = 2$$

$$r(7) = \chi(1) + \chi(7) = 1 - 1 = 0$$

$$r(50) = \chi(1) + \chi(2) + \chi(5) + \chi(10) + \chi(25) + \chi(50) = 1 + 0 + 1 + 0 + 1 + 0 = 3$$

Let's compare

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{vs.} \quad \zeta_{\mathbb{Q}(i)}(s) = \sum_{\substack{\alpha \in \mathbb{Z}[i] \\ \alpha \neq 0 \\ \text{up to units}}} \frac{1}{N(\alpha)^s}.$$

Unique factorization:

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1} \quad \text{vs.} \quad \prod_{\substack{\pi \text{ prime} \\ \text{up to units}}} \left(1 - \frac{1}{N(\pi)^s}\right)^{-1}$$

We have

$$\zeta_{\mathbb{Q}(i)}(s) = \zeta(s) L(\chi, s)$$

where

$$L(\chi, s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \cdots = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

Also,

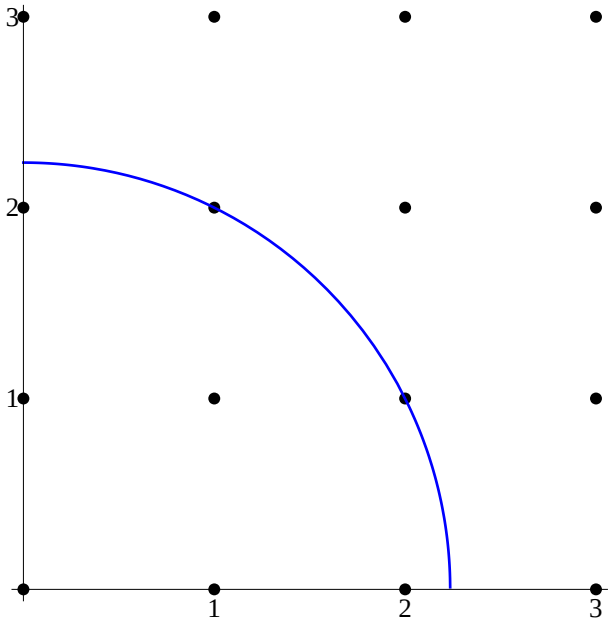
$$\zeta_{\mathbb{Q}(i)}(s) = \sum_{n=1}^{\infty} \frac{r(n)}{n^s}, \quad \text{where } r(n) = \text{the number of ways to write } n = a^2 + b^2 \text{ with } a > 0, b \geq 0.$$

We showed that this implied

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

One can easily see that

$$r(n) = \text{number of lattice points in the first quadrant on the circle of radius } \sqrt{n} \text{ centered at } 0.$$



Just like we had

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = 1\left(1 - \frac{1}{2^s}\right) + 2\left(\frac{1}{2^s} - \frac{1}{3^s}\right) + 3\left(\frac{1}{3^s} - \frac{1}{4^s}\right) + \cdots = s\int_1^\infty \frac{\lfloor x \rfloor}{x^{s+1}}\, dx,$$

we see that

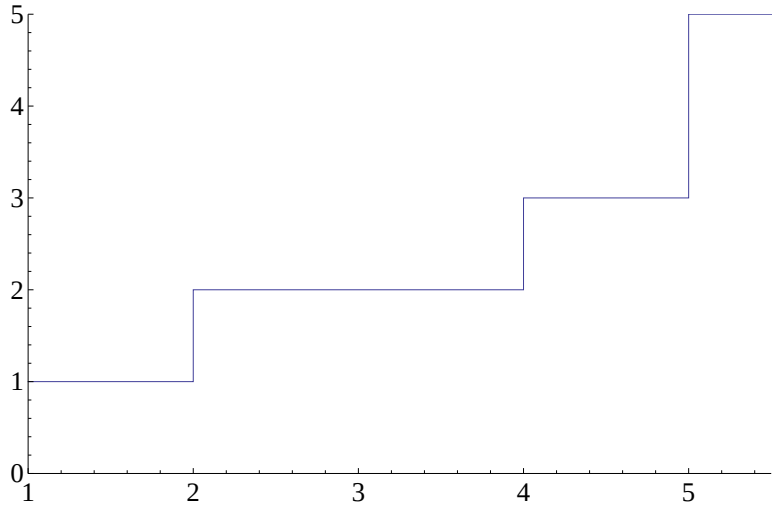
$$\begin{aligned}\zeta_{\mathbb{Q}(i)}(s) &= \frac{r(1)}{1^s} + \frac{r(2)}{2^s} + \frac{r(3)}{3^s} + \cdots \\ &= r(1)\left(\frac{1}{1^s} - \frac{1}{2^s}\right) + (r(1) - r(2))\left(\frac{1}{2^s} - \frac{1}{3^s}\right) + (r(1) + r(2) + r(3))\left(\frac{1}{3^s} - \frac{1}{4^s}\right) + \cdots\end{aligned}$$

Letting $R(x) = r(1) + r(2) + \cdots + r(\lfloor x \rfloor)$,

$$\zeta_{\mathbb{Q}(i)}(s) = R(1)\underbrace{\left(\frac{1}{1^s} - \frac{1}{2^s}\right)}_{s\int_1^2 \frac{1}{x^{s+1}}\, dx} + R(2)\underbrace{\left(\frac{1}{2^s} - \frac{1}{3^s}\right)}_{s\int_2^3 \frac{1}{x^{s+1}}\, dx} + \cdots$$

$$= s\int_1^2 \frac{R(x)}{x^{s+1}}\, dx + s\int_2^3 \frac{R(x)}{x^{s+1}}\, dx + \cdots = s\int_1^\infty \frac{R(x)}{x^{s+1}}\, dx$$

For example, $r(1) = 1, r(2) = 1, r(3) = 0, r(4) = 1, r(5) = 2$. Here is a graph of $R(x)$:



$R(x) = r(1) + r(2) + \cdots + r(\lfloor x \rfloor) = \#$ of lattice points in the first quadrant inside of (and including) the circle of radius $\sqrt{x}$, excluding the origin (since we didn't actually assign a value to $r(0)$).

Clearly, we should have

$$R(x) \approx \text{area of the quarter-circle} = \frac{\pi}{4}x.$$

In the diagram demonstrating $R(5) = 5$, let's put a box to the northwest of each lattice point inside the circle. How much do I have to increase the radius to hit the next points, in the absolute worst-case scenario? $\sqrt{2}$. Similarly, let's underestimate in the worst-case scenario. We get that

$$\text{area of quarter-circle of radius } \sqrt{x} - \sqrt{2} \le R(x) \le \text{area of quarter-circle of radius } \sqrt{x} + \sqrt{2}$$

$$\frac{\pi}{4}(x - 2\sqrt{2x} + 2) \le R(x) \le \frac{\pi}{4}(x + 2\sqrt{2x} + 2)$$

$$\frac{\pi}{4}(-2\sqrt{2x}+2) \leq \underbrace{R(x) - \frac{\pi}{4}x}_{\epsilon(x)} \leq \frac{\pi}{4}(2\sqrt{2x}+2)$$

Because $R(x) = r(1) + \cdots + r(\lfloor x \rfloor)$, we have that

$$\frac{R(x)}{\lfloor x \rfloor} = \frac{r(1)+r(2)+\cdots+r(\lfloor x \rfloor)}{\lfloor x \rfloor} = \text{average number of ways a number} \leq x \text{ can be written as } a^2+b^2$$

We can conclude that

$$\lim_{n\to\infty} \frac{R(n)}{n} = \frac{\pi}{4}$$

Going back to the zeta function,

$$\zeta_{\mathbb{Q}(i)}(s) = s\int_1^\infty \frac{R(x)}{x^{s+1}}\,dx = s\int_1^\infty \frac{\pi/4}{x^s}\,dx + s\int_1^\infty \frac{\epsilon(x)}{x^{s+1}}\,dx$$

We're interested in this as $s \to 1$. This isn't fully rigorous, but we want to say that the integral $s\int_1^\infty \frac{\epsilon(x)}{x^2}\,dx$ converges, and to a continuous fucntion of s, so that at $s=1$ we write

$$\frac{\pi}{4}\int_1^\infty \frac{-2\sqrt{2x}+2}{x^2}\,dx \leq \int_1^\infty \frac{\epsilon(x)}{x^2}\,dx \leq \frac{\pi}{4}\int_1^\infty \frac{2\sqrt{2x}+2}{x^2}\,dx$$

Thus

$$\lim_{s\to 1^+} \zeta_{\mathbb{Q}(i)}(s) - \frac{\pi}{4}\frac{s}{s-1} \text{ converges,}$$

and

$$\lim_{s\to 1^+} \zeta_{\mathbb{Q}(i)}(s)(s-1) = \frac{\pi}{4}$$

$$\frac{\pi}{4} = \lim_{s\to 1^+} L(\chi,s)\zeta(s)(s-1)$$

We proved in the first lecture that $\lim_{s\to 1^+}\zeta(s)(s-1)=1$, so that

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

In the coming classes, we'll do this process for other number systems, like $\mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}[\sqrt{-5}]$, and $\mathbb{Z}_p[x]$.

Last time, we proved (in an incredibly roundabout way) that

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \frac{\pi}{4}$$

using the arithmetic of $\mathbb{Z}[i]$. There were two phases: there was an algebraic phase, where we defined the zeta function

$$\zeta_{\mathbb{Q}(i)}(s) = \sum_{\substack{\alpha \in \mathbb{Z}[i] \\ \alpha \neq 0 \\ \text{up to units}}} \frac{1}{N(\alpha)^s}$$

Because of unique prime factorization, there was an Euler product

$$\zeta_{\mathbb{Q}(i)}(s) = \prod_{\substack{\pi \text{ prime} \\ \text{up to units}}} \left(1 - \frac{1}{N(\pi)^s}\right)^{-1} = \zeta(s)L(\chi, s)$$

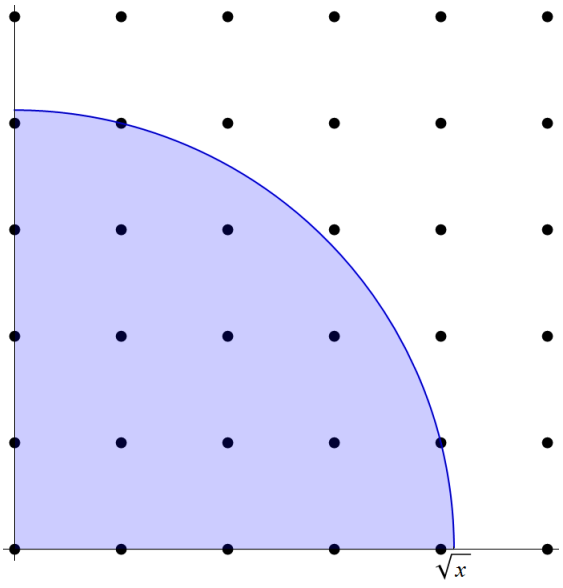
where

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

The analytic phase was computing that

$$\lim_{s \to 1^+} \zeta_{\mathbb{Q}(i)}(s)(s-1) = \frac{\pi}{4}$$

Here, $\frac{\pi}{4}$ arose as the average number of ways a natural number n can be written as $n = a^2 + b^2$ where $a > 0$, $b \geq 0$. We found that by showing the number of lattice points in



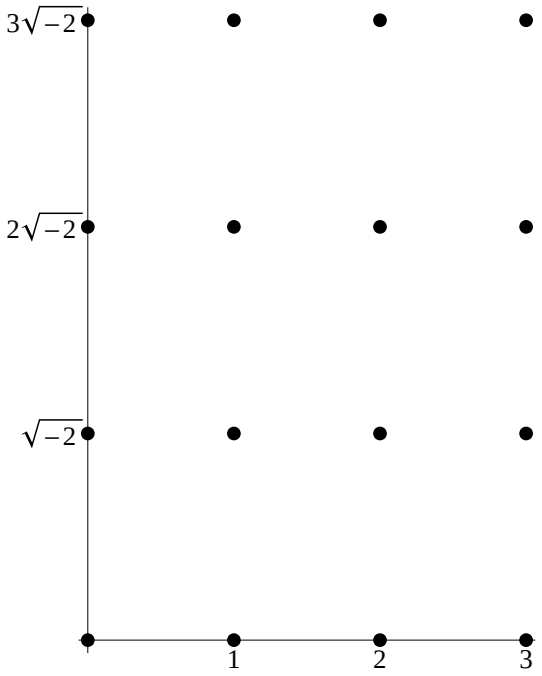
is approximately $\frac{\pi}{4}x$.

Now, we want to forge ahead and repeat this process for other number systems. You've previously studied

$$\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$$

The norm of $a + b\sqrt{-2}$ is defined to be $N(a + b\sqrt{-2}) = a^2 + 2b^2$. The norm is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$. Using that fact, it is easy to show that the units of $\mathbb{Z}[\sqrt{-2}]$ are just 1 and -1.

Does $\mathbb{Z}[\sqrt{-2}]$ have a division algorithm? Yes, because a point in the plane can only get $\frac{\sqrt{3}}{2} < 1$ away from an element of $\mathbb{Z}[\sqrt{-2}]$:



What are the primes of $\mathbb{Z}[\sqrt{-2}]$? Just like for $\mathbb{Z}[i]$, there's one weird one, and two infinite classes.

- Weird prime: $\sqrt{-2}$
- $\pi = a + b\sqrt{-2}$ where $N(\pi) = a^2 + 2b^2 = p$ is a rational prime, $p \equiv 1, 3 \bmod 8$.
- Rational primes p for which $p \equiv 5, 7 \bmod 8$.

If $p = a^2 + 2b^2$ for p a prime, then

$$a^2 + 2b^2 \equiv 0 \bmod p$$
$$(ab^{-1})^2 \equiv -2 \bmod p$$

and thus

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$$

By quadratic reciprocity, this is the case if and only if $p \equiv 1, 3 \bmod 8$. Conversely, if $p \equiv 1, 3 \bmod 8$, then $\left(\frac{-2}{p}\right) = 1$, so that we can solve $x^2 \equiv -2 \bmod p$, so that $p \mid (x+\sqrt{-2})(x-\sqrt{2})$. But p doesn't divide either factor, so p must not be prime in $\mathbb{Z}[\sqrt{-2}]$. Say a non-trivial factorization of p is $p = \alpha\beta$; then $N(p) = p^2 = N(\alpha)N(\beta)$, so we must be able to solve $p = a^2 + 2b^2$.

By unique prime factorization in $\mathbb{Z}[\sqrt{-2}]$, we therefore have that

$$\zeta_{\mathbb{Q}(\sqrt{-2})}(s) = \sum_{\substack{\alpha \in \mathbb{Z}[\sqrt{-2}] \\ \alpha \neq 0 \\ \text{up to } \pm 1}} \frac{1}{N(\alpha)^s}$$

$$= \prod_{\substack{\pi \text{ prime} \\ \text{up to } \pm 1}} \left(1 - \frac{1}{N(\pi)^s}\right)^{-1} = \left(1 - \frac{1}{2^s}\right)^{-1} \prod_{p \equiv 1,3 \bmod 8} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p \equiv 5,7 \bmod 8} \left(1 - \frac{1}{p^{2s}}\right)^{-1}$$

$$= \zeta(s) \prod_{p \equiv 1,3 \bmod 8} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p \equiv 5,7 \bmod 8} \left(1 + \frac{1}{p^s}\right)^{-1}$$

$$= \zeta(s) \left(1 + \frac{1}{3^s} + \frac{1}{9^s} + \cdots\right) \left(1 - \frac{1}{5^s} + \frac{1}{25^s} - \cdots\right) \left(1 - \frac{1}{7^s} + \frac{1}{49^s} - \cdots\right)$$

$$= \zeta(s) \underbrace{\left(1 + \frac{1}{3^s} - \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} - \frac{1}{13^s} - \frac{1}{15^s} + \frac{1}{17^s} + \cdots\right)}_{L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}}$$

where $\chi(n)$ is the nth term in the sequence $1, 0, 1, 0, -1, 0, -1, 0, 1, 0, 1, 0, 1, \ldots$, which has period 8.

The function χ is an example of what is known as a Dirichlet character. In this case, it is a function $\chi : \mathbb{Z}_8 \to \{0, 1, -1\}$ such that

$$\chi(n) = \begin{cases} 0 & \text{if } n \text{ is even,} \\ 1 & \text{if } n \equiv 1, 3 \bmod 8, \\ -1 & \text{if } n \equiv 5, 7 \bmod 8. \end{cases}$$

Note that χ is multiplicative, i.e. $\chi(mn) = \chi(m)\chi(n)$, and that for an odd prime p, $\chi(p) = \left(\frac{-2}{p}\right)$.

Now for the analytic phase. We note that

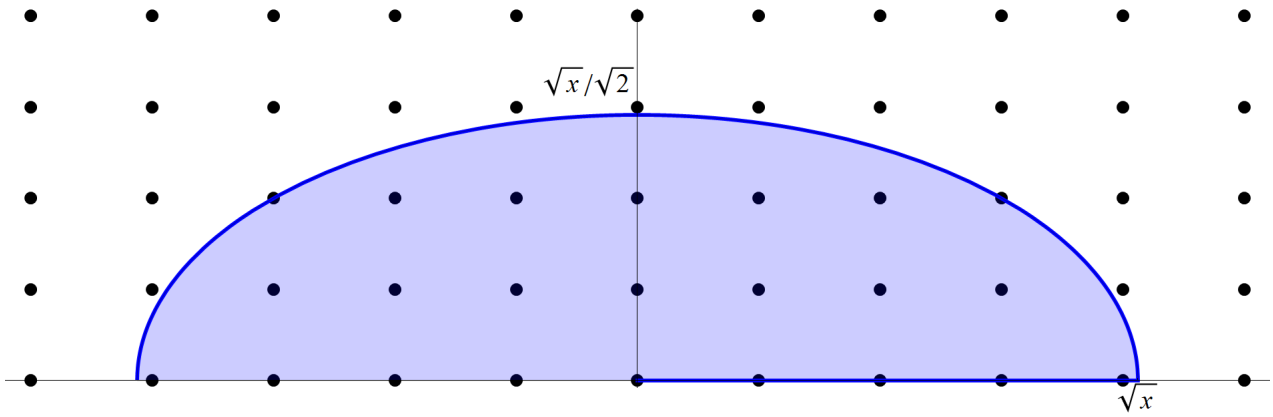
$$\zeta_{\mathbb{Q}(\sqrt{-2})}(s) = \sum_{\substack{\alpha \in \mathbb{Z}[\sqrt{-2}] \\ \alpha \neq 0 \\ \text{up to } \pm 1}} \frac{1}{N(\alpha)^s} = \sum_{n=1}^{\infty} \frac{r(n)}{n^s}$$

where $r(n)$ = the number of ways of writing $n = a^2 + 2b^2$, where (a, b) and $(-a, -b)$ count as the same solution. This is equal to

$$s \int_1^{\infty} \frac{R(x)}{x^{s+1}}\, dx$$

where $R(x) = r(1) + \cdots + r(\lfloor x \rfloor)$ is the number of pairs (a, b) (up to sign) where $(a, b) \neq (0, 0)$ and $a^2 + 2b^2 \leq x$.

Geometrically, it's the number of unit lattice points within (and including) the ellipse with horizontal semimajor axis $\sqrt{x}$ and vertical semiminor axis $\sqrt{x}/\sqrt{2}$, together with the points on the positive x-axis.

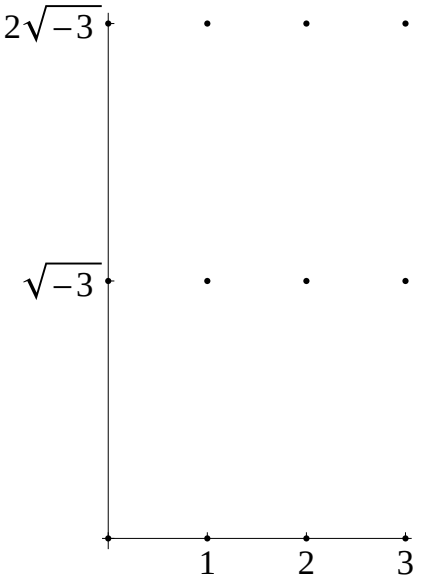


$R(x) =$ number of lattice points in the ellipse that lie in quadrant I or II $\approx \frac{1}{2} \cdot \pi \cdot \sqrt{x} \cdot \frac{\sqrt{x}}{\sqrt{2}}$

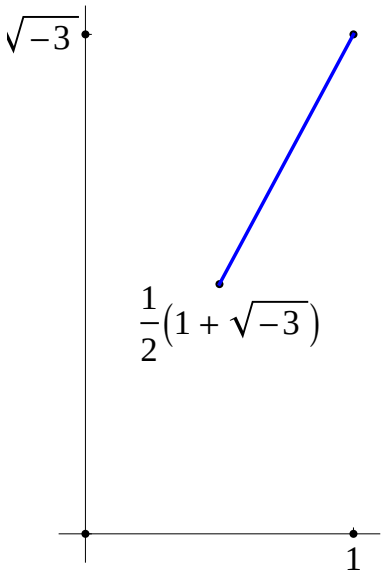
Taking limits,

$$1 + \frac{1}{3} - \frac{1}{5} - \frac{1}{7} + \cdots = L(\chi, 1) = \lim_{s \to 1^+} \zeta_{\mathbb{Q}(\sqrt{-2})}(s)(s-1) = \frac{\pi}{2\sqrt{2}}$$

We seen interesting examples of infinite series dealing with the number systems $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$. Let's consider $\mathbb{Z}[\sqrt{-3}]$:



Nnote that in one of these boxes, the distance from the center to a corner is exactly 1:

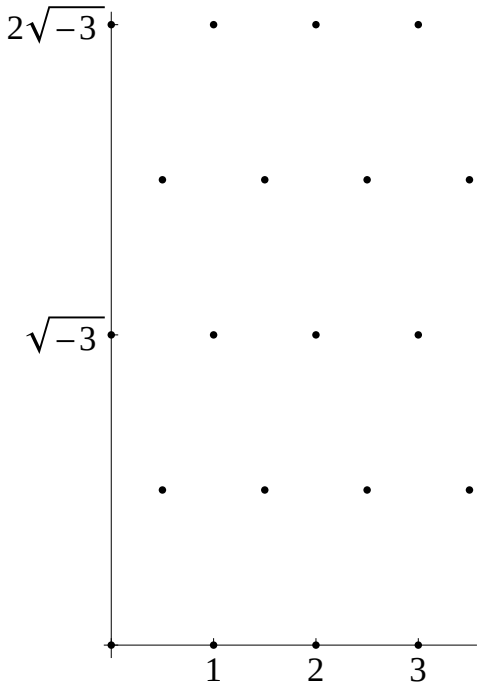


Thus, the division algorithn doesn't hold in $\mathbb{Z}[\sqrt{-3}]$. Now, it doesn't *necessarily* follow that unique factorization will also fail, but in this case, it does fail. Here's an example:

$$4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$$

This isn't just a case of associates looking different, because the only units in $\mathbb{Z}[\sqrt{-3}]$ are 1 and -1.

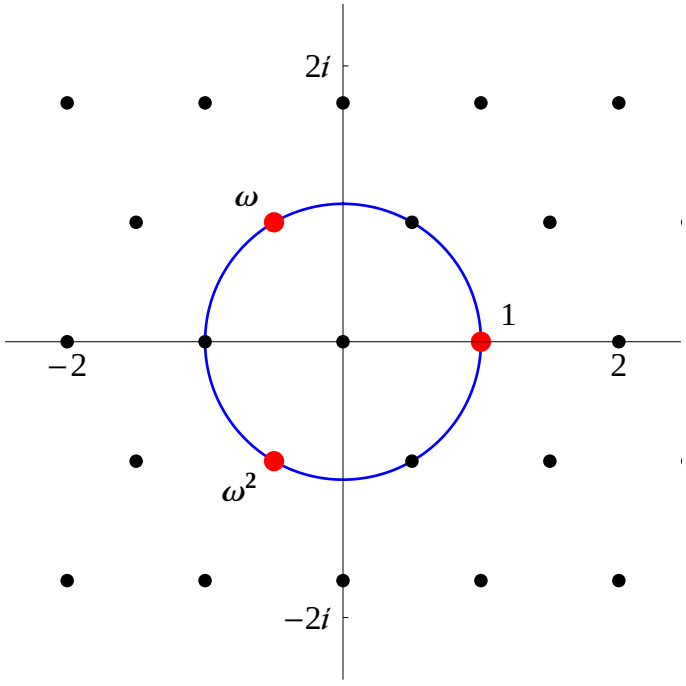
Since the centers of the rectangles seem to be causing this problem, why don't we just add them in?



So, let's consider

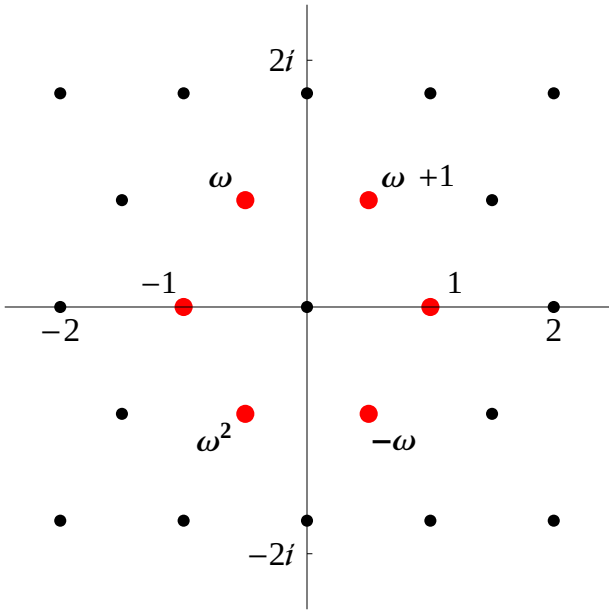
$$\mathbb{Z}[\omega] = \mathbb{Z}[\tfrac{-1+\sqrt{-3}}{2}] = \{\tfrac{a+b\sqrt{-3}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \bmod 2\}$$

where $\omega = \frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity.



Noet that $\omega^2 = -\omega - 1$. Because we can express ω^2 in terms of 1 and ω, any polynomial expression in ω with integer coefficients can be rewritten in the form $a + b\omega$, where $a, b \in \mathbb{Z}$. Thus

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}.$$



(rhobmus, center of one triangle, max distance is $\frac{1}{\sqrt{3}} < 1$)

Thus, $\mathbb{Z}[\omega]$ has division algorithm, and thus unique factorization. Our example is no longer a failure of unique factorization, because

$$1 = \left(\frac{1+\sqrt{-3}}{2}\right)\left(\frac{1-\sqrt{-3}}{2}\right)$$

so that 2, $1+\sqrt{-3}$, and $1-\sqrt{-3}$ are associates.

What are the units of $\mathbb{Z}[\omega]$? Recall that $N(a+b\sqrt{-3}) = a^2+3b^2$. In $\mathbb{Z}[\omega]$, we have that $N(a+b\omega) = (a+b\omega)(a+b\overline{\omega}) = a^2-ab+b^2$. Thus, the only units are $\pm 1, \pm\omega, \pm\omega^2$.

Algebraic Phase: key fact is that $\left(\frac{-3}{p}\right) = 1$ only when

$$\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right) = 1$$

which is the case if and only if $p \equiv 1 \bmod 3$.

What are the primes in $\mathbb{Z}[\omega]$?

- $\sqrt{-3}$
- π such that $N(\pi) = p \equiv 1 \bmod 3$
- $p \equiv 2 \bmod 3$

Let $\chi(n) = n$th term of $1, -1, 0, 1, -1, 0, \ldots$, so that

$$\chi(p) = \begin{cases} 1 & \text{if } p = \pi\overline{\pi} \text{(split)}, \\ -1 & \text{if } p \text{ stays prime (inert)}, \\ 0 & \text{if } 3 = \pi^2 \cdot \text{unit}. \end{cases}$$

Now onto the analytic phase.

$$\zeta_{\mathbb{Q}(\sqrt{-3})}(s) = \sum_{\substack{\alpha \in \mathbb{Z}[\omega] \\ \alpha \neq 0 \\ \text{up to units}}} \frac{1}{N(\alpha)^s} = \zeta(s)L(\chi, s)$$

Letting $R(x) = \#\{\alpha \in \mathbb{Z}[\omega] \mid \alpha \neq 0, N(\alpha) \leq x \text{ up to units}\}$

Dirichlet character χ	relevant system of numbers	$L(\chi, 1)$
$\chi \bmod 3\ (1, -1, 0, \ldots)$	$\mathbb{Z}[\omega]$	$\frac{\pi}{3\sqrt{3}} = \frac{1}{\boxed{6}}\frac{2\pi}{\sqrt{3}}$
$\chi \bmod 4\ (1, 0, -1, 0, \ldots)$	$\mathbb{Z}[i]$	$\frac{\pi}{4} = \frac{1}{\boxed{4}}\frac{2\pi}{\sqrt{4}}$
$\chi \bmod 8\ (1, 0, 1, 0, -1, 0, -1, 0, \ldots)$	$\mathbb{Z}[\sqrt{-2}]$	$\frac{\pi}{2\sqrt{2}} = \frac{1}{\boxed{2}}\frac{2\pi}{\sqrt{8}}$

Note that the boxed number is the number of units in the relevant number system.

However, in $\mathbb{Z}[\sqrt{-5}]$, we don't have unique factorization, because (for example)

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

We don't want to try to add in $\frac{1+\sqrt{-5}}{2}$, because it has a non-integer norm. The only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1.

What is the relevant Dirichlet character for $\mathbb{Z}[\sqrt{-5}]$? First, let's figure out $\left(\frac{-5}{p}\right)$, because we've seen that that is useful information. For $p \neq 2, 5$,

$$\left(\frac{-5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right)$$

$$= \begin{cases} 1 & \text{if } p \equiv 1, 3, 7, 9 \bmod 20, \\ -1 & \text{if } p \equiv 11, 13, 17, 19 \bmod 20. \end{cases}$$

The function $\chi : U_{20} \to \{\pm 1\}$ is multiplicative, $\chi(mn) = \chi(m)\chi(n)$. Then we extend the function to $\mathbb{Z}$ by setting $\chi(n)$ equal to 0 when $\gcd(n, 20) \neq 1$.

What would we predict $L(\chi, 1)$ is? We'd guess $\frac{1}{2} \cdot \frac{2\pi}{\sqrt{20}} = \frac{\pi}{2\sqrt{5}}$.

Computing directly,

$$L(\chi, 1) = \int_0^1 \frac{x + x^3 + x^7 + x^9 - x^{11} - x^{13} - x^{17} - x^{19}}{x(1 - x^{20})}\, dx$$

$$= \int_0^1 1 + x^2 + x^6 + x^8 - x^{10} - x^{12} - x^{16} - x^{18} + x^{20} + x^{22} + \cdots\, dx$$

$$= 1 + \frac{1}{3} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} - \cdots = \frac{\pi}{5}$$

So our guess was off by a factor of 2.

We all know the result in $\mathbb{Z}[i]$ that

$$p \equiv 1 \bmod \iff p = a^2 + b^2 \iff \left(\frac{-1}{p}\right) = 1 \iff p = N(\alpha) = \alpha\overline{\alpha}$$

But in $\mathbb{Z}[\sqrt{-5}]$ similar statements are completely false.

$$\left(\frac{-5}{3}\right) = 1, \text{ but } 3 \neq a^2 + 5b^2$$

$$\left(\frac{-5}{7}\right) = 1, \text{ but } 7 \neq a^2 + 5b^2$$

$$-5 \equiv \square \bmod 2, \text{ but } 2 \neq a^2 + 5b^2$$

Finally works for

$$\left(\frac{-5}{29}\right) = 1, \text{ and } 29 = 3^2 + 5 \cdot 2^2$$

Also note that

$$3 \cdot 3 = 2^2 + 5 \cdot 1^2$$

$$7 \cdot 7 = 2^2 + 5 \cdot 3^2$$

$$3 \cdot 7 = 1^2 + 5 \cdot 2^2$$

$$2 \cdot 3 = 1^2 + 5 \cdot 1^2$$

$$2 \cdot 7 = 3^3 + 5 \cdot 1^2$$

$$2 \cdot 3 \cdot 7 \neq a^2 + 5b^2$$

$$2 \cdot 29 \neq a^2 + 5b^2$$

$$3 \cdot 29 \neq a^2 + 5b^2$$

$$2 \cdot 3 \cdot 29 = 174 = 7^2 + 5 \cdot 5^2 = 13^2 + 5 \cdot 1^2$$

Let

$$S = \left\{\left(\tfrac{-5}{p}\right) = 1, p = x^2 + 5y^2\right\} \quad \text{and} \quad T = \left\{\left(\tfrac{-5}{p}\right) = 1, p \neq x^2 + 5y^2\right\}.$$

If $s_1, \ldots, s_m \in S$, and $t_1, \ldots, t_n \in T$, then

$$s_1 \cdots s_m t_1 \cdots t_n = x^2 + 5y^2 \iff n \text{ is even}$$

Lecture 6 July 12, 2012

Today we'll talk about ideals of rings.

Given $m, n \in \mathbb{Z}$, consider the set $I = \{am + bn \mid a, b \in \mathbb{Z}\}$. We write this set as $m\mathbb{Z} + n\mathbb{Z}$, or as (m, n). There's some amibguity as to whether (m, n) refers to $\gcd(m, n)$ or this set, but it's not so bad; in fact $I = (m, n)\mathbb{Z}$.

Note that I is closed under multiplication, and that $\mathbb{Z}I = I$, i.e. for any $a \in I$ and $n \in \mathbb{Z}$, $an \in I$. A subset of $\mathbb{Z}$ with these two properties is called an ideal. For example, $I = \{0\}$ is an ideal, $\mathbb{Z}$ is an ideal of itself, and $n\mathbb{Z}$ is an ideal for any n. In fact, every ideal of $\mathbb{Z}$ is of that form:

Proposition 1. *Given an ideal $I \subseteq \mathbb{Z}$, there is some $n \in \mathbb{Z}$ such that $I = n\mathbb{Z}$.*

Proof. Assume $I \neq \{0\}$. So I contains some least positive integer n. We claim that $I = n\mathbb{Z}$. We clearly have that $I \supseteq n\mathbb{Z}$, but we need to show the other inclusion. For any $x \in I$, we know there exist $q, r \in \mathbb{Z}$ such that $x = nq + r$ and $0 \leq r < n$. But because I is closed under addition and multiplication, we have that $x - nq = r \in I$, so we must have $r = 0$ (otherwise n wouldn't be the smallest positive integer in I). □

We say that an ideal of the form $n\mathbb{Z}$ are "principal", and we just showed that every ideal of $\mathbb{Z}$ is prinipcal. In modern terms, what this shows is that $\mathbb{Z}$ is a principal ideal domain.

$\mathbb{Z}[i]$ is also a PID.

Proposition 2. *If $p \equiv 1 \bmod 4$, then $p = a^2 + b^2$. Proof: there exists an x such that $x^2 \equiv -1 \bmod p$.*

Proof. Let $I = \{a + bi \mid a, b \in \mathbb{Z}, a \equiv xb \bmod p\}$. It's clearly closed under addition. It is closed under multiplication 1, and also by i, because if $a + bi \in I$ then $-b \equiv x(xb) \equiv xa \bmod p$. Therefore by the distributive law it is closed under multiplication by $\mathbb{Z}[i]$. Thus I is an ideal.

We claim that $I = p\mathbb{Z} + (x + i)\mathbb{Z}$. Because $p \in I$ and $(x + i) \in I$, we must have that $I \supseteq p\mathbb{Z} + (x + i)\mathbb{Z}$. Conversely, if $a + bi \in I$, then $a + bi = (xb + pn) + bi = pn + (x + i)b$, so $I \subseteq p\mathbb{Z} + (x + i)\mathbb{Z}$.

We can talk about

$$\mathbb{Z}[i]_I = \{\text{equivalence classes of } \mathbb{Z}[i] \text{ under the relation } \alpha \sim \beta \text{ when } \alpha \in \beta \in I\}.$$

Because $\mathbb{Z}[i]$ is a PID, $I = (\alpha) = \alpha\mathbb{Z}[i]$, we have that

$$N(I) := \#\mathbb{Z}[i]_I = \#\mathbb{Z}[i]_\alpha = N(\alpha) = a^2 + b^2 = p.$$

□

A principal ideal in a ring R is just an ideal of the form $\alpha R = \{\alpha x \mid x \in R\}$. This is also written (α).

Back to $\mathbb{Z}[\sqrt{-5}]$. Even if $-5 \equiv x^2 \bmod p$, it isn't necessarily true that $p = a^2 + 5b^2$; for example, $p = 2, 3, 7$. On the other hand, $29 = 3^2 + 5 \cdot 2^2$. We noticed last time that $2 \cdot 3, 2 \cdot 7, 3 \cdot 7$ *were* expressible as $a^2 + 5b^2$.

Some ideals in $\mathbb{Z}[\sqrt{-5}]$ are not principal: if $x^2 \equiv -5 \bmod p$, let $I = \{a + b\sqrt{-5} \mid a \equiv x \bmod p\} = p\mathbb{Z} + (x + \sqrt{-5})\mathbb{Z}$. For example, we can take $p = 2$, and $x = 1$. Is $I = (\alpha)$ for some $\alpha \in \mathbb{Z}[\sqrt{-5}]$? If so, then $\alpha \mid 2$. The only $\alpha \in \mathbb{Z}[\sqrt{-5}]$ such that $\alpha \mid 2$ are $\alpha = \pm 1, \pm 2$. But ± 2 doesn't divide $1 + \sqrt{-5}$, so we'd have to have $\alpha = \pm 1$, and thus $I = \mathbb{Z}[\sqrt{-5}]$. However, $1 \notin \mathbb{Z}[\sqrt{-5}]$:

(diagram)

area $= 2\sqrt{5}$, $N(I) = 2$.

In general, the fundamental parallelogram of $p\mathbb{Z} + (x + \sqrt{-5})\mathbb{Z}$ looks like this:

(diagram)

Recall

Theorem (Minkowski's Theorem). *If $S \subset \mathbb{R}^2$ is a symmetric convex body of area $> 4 \cdot$ area$(\diamond) = 4p\sqrt{5}$, then S contains a non-zero lattice point.*

Let S be a closed disk with radius$^2 > \frac{4p\sqrt{5}}{\pi}$, say radius$^2 = \frac{4p\sqrt{5}}{\pi} + \epsilon$. Then there is a non-zero $\alpha \in I$ such that

$$N(\alpha) \leq \frac{4p\sqrt{5}}{\pi} + \epsilon$$

Because $\lfloor \frac{4\sqrt{5}}{\pi} \rfloor = 2$, we can choose ϵ so that $N(\alpha) < 3p$. Because $\alpha \neq 0$, $N(\alpha) > 0$.

If $\alpha \in I = p\mathbb{Z} + (x + \sqrt{-5})\mathbb{Z}$, then $N(\alpha)$ is divisible by $N(I) = p$. Thus we must have $N(\alpha) = p$ or $N(\alpha) = 2p$, so that either $p = x^2 + 5y^2$ (good), e.g. 29, or $2p = x^2 + 5y^2$ (bad), e.g. $2, 3, 7, 23$.

Euler conjectured, but Gauss proved, that if $p \equiv 1, 3, 5, 7 \bmod 20$, i.e. $\left(\frac{-5}{p}\right) = 1$, then either $p = x^2 = 5y^2$ or $2p = x^2 + 5y^2$.

Fermat-type theorems via geometry of numbers

Let p be a prime.

$x^2 \equiv -1 \bmod p$	$x^2 \equiv -5 \bmod p$
$R = \mathbb{Z}[i]$	$R = \mathbb{Z}[\sqrt{-5}]$
$I = \{a + bi \in R \mid a \equiv xb \bmod p\}$ is an ideal	$I = \{a + b\sqrt{-5} \in R \mid a \equiv xb \bmod p\}$ is an ideal

We define the norm of an ideal $I \subseteq R$ to be $N(I) = |R/I| = p$. For $\alpha \in I$, we have that $N(\alpha) \equiv 0 \bmod p$. For example, if $\alpha = a + b\sqrt{-5} \in I$, then

$$N(\alpha) = a^2 + 5b^2 \equiv (xb)^2 + 5b^2 \equiv (x^2 + 5)b^2 \equiv 0 \bmod p$$

The ideal I always looks like a lattice in our examples. The volume of a fundamental parallelogram for these lattices was

$$\mathrm{vol}(\diamond) = \begin{cases} p & \text{if } R = \mathbb{Z}[i] \\ p\sqrt{5} & \text{if } R = \mathbb{Z}[\sqrt{-5}] \end{cases}$$

Minkowski's theorem tells us that there exists a non-zero $\alpha \in I$ such that

$$N(\alpha) < \begin{cases} \frac{4p}{\pi} < 2p & \text{if } R = \mathbb{Z}[i] \\ \frac{4p\sqrt{5}}{\pi} < 3p & \text{if } R = \mathbb{Z}[\sqrt{-5}] \end{cases}$$

Therefore in $\mathbb{Z}[i]$, we have $p = N(\alpha) = x^2 + y^2$, while in $\mathbb{Z}[\sqrt{-5}]$, all we can conclude is that either $p = N(\alpha) = x^2 + 5y^2$, or $2p = N(\alpha) = x^2 + 5y^2$.

Let's review ideals in $\mathbb{Z}$. We proved that any ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, for some $n \in \mathbb{Z}$.

Note that $n \mid m$ if and only if $n\mathbb{Z} \supseteq m\mathbb{Z}$.

The ideals $2\mathbb{Z}$, $3\mathbb{Z}$, $5\mathbb{Z}$, ... are prime; a prime ideal (for our purposes) is an ideal $P \neq QR$ for any ideals Q, R neither of which is $\mathbb{Z}$ itself. Note that $\mathbb{Z} = 1\mathbb{Z}$ and $(\mathbb{Z})(n\mathbb{Z}) = n\mathbb{Z}$.

Prime ideals in $\mathbb{Z}$ factor uniquely into prime ideals: for any non-zero ideal $I \subseteq \mathbb{Z}$,

$$I = P_1^{e_1} \cdots P_n^{e_n}$$

One of the advantages of ideals is that we don't have to worry about units anymore. When stating unique factorization for elements of $\mathbb{Z}$, we have

$$6 = 2 \cdot 3 = (-2) \cdot (-3)$$

but for ideals, $6\mathbb{Z} = (2\mathbb{Z})(3\mathbb{Z})$.

The ideal generated by a subset $S \subset R$ is defined to be

$$\{\text{sums of the form } \sum_{i=1}^{n} x_i a_i \mid a_i \in S, x_i \in R\}$$

It is easy to check this is closed under addition, and closed under multiplication by elements of R.

For integers, this notation agrees with the notation for gcd, namely

$$\text{as elements } (n_1, \ldots, n_k) = \gcd(n_1, \ldots, n_k), \qquad \text{as ideals } (n_1, \ldots, n_k) = (\gcd(n_1, \ldots, n_k)).$$

Now, we can define the product of two ideals I and J of a ring R as being the ideal

$$IJ = \text{ideal generated by } \{\alpha\beta \mid \alpha \in I, \beta \in J\}.$$

Here's the example we're interested in. Let $R = \mathbb{Z}[\sqrt{-5}]$, and let $I = (2, 1 + \sqrt{-5})$, $J = (3, 1 + \sqrt{-5})$. Then

$$IJ = (6, 2(1 + \sqrt{-5}), 3(1 + \sqrt{-5}), -4 + 2\sqrt{5})$$

Because $2(1 + \sqrt{-5})$ and $3(1 + \sqrt{-5})$ are in IJ, so is their difference $1 + \sqrt{-5}$, and it generates anything $2(1 + \sqrt{-5})$ and $3(1 + \sqrt{-5})$ can, so

$$IJ = (6, 1 + \sqrt{-5}, -4 + 2\sqrt{-5}) = ((1 + \sqrt{-5})(1 - \sqrt{-5}), 1 + \sqrt{-5}, (1 + \sqrt{-5})^2) = (1 + \sqrt{-5})$$

As an example, if p is prime, and $x^2 \equiv -5 \bmod p$, then $I = (p, x + \sqrt{-5})$, and $N(I) = p$. Minkowski gives two possibilities

- there is a non-zero $\alpha \in I$ such that $N(\alpha) = p$, so that $I = (\alpha)$ is principal! (We knew $I \supseteq (\alpha)$, but their norms are equal, so we must have $I = (\alpha)$)
- there is a non-zero $\alpha \in I$ such that $N(\alpha) = 2p$, $I \supsetneq (\alpha)$, and there is some ideal J such that $2p = N(IJ) = N(I)N(J)$. We can see that $J = (2, 1 + \sqrt{-5})$.

In $\mathbb{Z}[\sqrt{-5}]$, if I is a non-zero ideal, then either I is principal, or IP is principal where $P = (2, 1 + \sqrt{-5})$.

Consequence: if I, J are non-principal, then we claim that IJ is principal.

Let's talk more about $\mathbb{Z}[\sqrt{-5}]$. Once we understand this case, we'll be all set to understand the general case.

Recall that

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

is a failure of unique factorization in $\mathbb{Z}[\sqrt{-5}]$, because all four of these elements are irreducible, i.e. they cannot be written as a product of two other elements, both not units. As ideals,

$$(2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) = (4, 2(1 + \sqrt{-5}), 2(1 - \sqrt{-5}), 6) = (2)$$

and similarly

$$(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = (3)$$

Thus, looking at ideals,

$$(6) = (2) \cdot (3) = (1 + \sqrt{-5})(1 - \sqrt{-5}) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$$

This might cause you to think that we can fix unique factorization by looking at ideals, and you'd be right.

Generalities on ideals

The unit ideal of a ring R is just R itself. Note that $(1) = R$, and that $RI = I$. A proper ideal is an ideal $\neq (1)$. A prime ideal P is a proper ideal with the property $ab \in P \implies a \in P$ or $b \in P$. This should remind you of $p \mid ab \implies p \mid a$ or $p \mid b$, viewed under the slogan "to contain is to divide".

If P is a prime ideal and $P \supseteq I_1 \cdots I_n$ for ideals $I_1, \ldots, I_n$, then $P \supseteq I_i$ for some i. Here's the proof: if not, then there exists $a_i \in I_i \setminus P$ for all i, and then $a_1 \cdots a_n \in I_1 \cdots I_n \subseteq P$, but the fact that P is a prime ideal would then imply that one of the $a_i \in P$, which is a contradiction.

Lastly, a maximal ideal is a proper ideal not contained in any other proper ideal. To compare, note that in $\mathbb{Z}$, the zero ideal (0) is prime, because $ab \in (0)$ implies $ab = 0$ which implies $a = 0$ or $b = 0$, hence $a \in (0)$ or $b \in (0)$, but the zero ideal is not maximal, because any proper ideal e.g. (17) will contain it.

So, in $\mathbb{Z}$, we have

Ideals:	(0),	(1),	(2),	(3),	(4),	$\ldots$
Prime ideals:	(0),	(2),	(3),	(5),	(7),	$\ldots$
Maximal ideals:	(2),	(3),	(5),	(7),	$\ldots$	

A Dedekind domain R is a domain in which

- All non-zero prime ideals are maximal.
- Every proper ideal is the product of prime ideals.

It turns out these properties already imply a kind of unique factorization. In a Dedekind domain, let $I \neq (0)$ be a proper ideal. Then $I = P_1 \cdots P_n$, where each $P_i \neq (0)$ is a prime ideals. Suppose we had a different factorization $I = Q_1 \cdots Q_n$. Then because

$$P_1 \supseteq I = Q_1 \cdots Q_m$$

we have that $P_1 \supseteq Q_i$ for some i. Thus $P_1 = Q_i$. Continuing, we can conclude that $\{P_1, \ldots, P_n\} = \{Q_1, \ldots, Q_m\}$.

Factorization of ideals in $\mathbb{Z}[\sqrt{-5}]$

Recall that $(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})$, even though the element 2 is irreducible.

We claim that if p is a prime in $\mathbb{Z}$, and $x^2 \equiv -5 \bmod p$ has a solution, then $(p) = (p, x+\sqrt{-5})(p, x-\sqrt{-5})$. Suppose for the moment that $p \neq 2, 5$. Note that

$$\begin{aligned}(p, x+\sqrt{-5})(p, x-\sqrt{-5}) &= (p^2, p(x+\sqrt{-5}), p(x-\sqrt{-5}), x^2+5) \\ &= (p)(p, x+\sqrt{-5}, x-\sqrt{-5}, \tfrac{x^2+5}{p})\end{aligned}$$

Because ideals are closed under addition, $2x$ and $2\sqrt{-5}$ are also in the ideal on the right. Because $p \neq 2$, we have $\gcd(2x, p) = \gcd(x, p)$. If $\gcd(x, p) = p$, then the congruence $x^2 \equiv -5 \bmod p$ tells us that $p = 5$, which we also assumed was not the case. Thus $\gcd(x, p) = 1$, so that the ideal on the right is (1), proving our claim.

If $I \subseteq R$ is an ideal, we can talk about

$$R_I = \{\text{equivalence classes under } a \sim b \iff a - b \in I\}$$

Note that in the real world, people write this as R/I, but we'll use this notation by analogy with the PROMYS notation $\mathbb{Z}_5$.

Note that R_I is a ring under the obvious operations on equivalence classes.

The function

$$\mathbb{Z}[\sqrt{-5}]/(p, x+\sqrt{-5}) \longrightarrow \mathbb{Z}_p$$

defined by $\overline{a+b\sqrt{-5}} \longmapsto \overline{a-bx}$ is an isomorphism.

It's easy to show that if $I \subset R$ is an ideal, then

$$R_I \text{ is a field} \iff I \text{ is a maximal ideal.}$$

Let's go back and look at the ideals (2) and (5).

$$(2) = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5}) = (2, 1+\sqrt{-5})^2$$

$$(5) = (\sqrt{-5})^2$$

If there is no solution to $x^2 \equiv -5 \bmod p$, then (p) is a maximal ideal.

$$\mathbb{Z}[\sqrt{-5}]/(p) = (\mathbb{Z}[x]/(x^2+5))/(p) = \mathbb{Z}_p[x]/(x^2+5)$$

is a field with p^2 elements (don't confuse the indeterminate x with the integer x from before!)

Thus, we've completely determined the prime ideals of $\mathbb{Z}[\sqrt{-5}]$.

- (0)
- "ramified": the "edge cases" $(\sqrt{-5})$ and $(2, 1+\sqrt{-5})$
- "split": $(p, x+\sqrt{-5})$ when $\left(\frac{-5}{p}\right) = 1$ and $x^2 \equiv -5 \bmod p$
- "inert": (p) when $\left(\frac{-5}{p}\right) = -1$.

Student(s): What about $(p, x-\sqrt{-5})$ for the split case?

Good question - that corresponds to just taking the other solution to $x^2 \equiv -5 \bmod p$. In other words,

$$(p, x+\sqrt{-5}) = (p, (-x)-\sqrt{-5})$$

Let's return to our work from before. For the algebraic phase,

$$\zeta_{\mathbb{Q}(\sqrt{-5})}(s) = \sum_{\substack{\text{ideals} \\ I \subseteq \mathbb{Z}[\sqrt{-5}] \\ I \neq (0)}} \frac{1}{N(I)^s}$$

which equals

$$\prod_{\text{maximal } P} \left(1 - \frac{1}{N(P)^s}\right)^{-1} = \zeta(s)L(\chi, s)$$

due to unique factorization of ideals. The χ is a Dirichlet character modulo 20, namely $\chi(p) = \left(\frac{-5}{p}\right)$.

In the ring $\mathbb{Z}[\sqrt{-5}]$, we saw that non-zero ideals are principal, or not principal. Using Minkowski's theorem, if $I \neq (0)$ is a non-principal ideal, then IP is principal where $P = (2, 1 + \sqrt{-5})$. In general, if p denotes principal and n denotes non-principal, then

$\times$	p	n
p	p	n
n	n	p

The proof was just that if both I and J are non-principal, then $IJPP = (IP)(JP)$ is principal $\times$ principal = principal.

From yesterday, recall that

- P is a prime ideal when $P \neq (1)$ and $ab \in P \implies a \in P$ or $b \in P$
- M is a maximal ideal when $M \neq (1)$ and $M \not\subset M'$ for any proper ideal M'
- maximal $\implies$ prime
- A Dedekind domain is a domain where
  - every non-zero prime ideal is maximal
  - every ideal can be factored into prime ideals
  - every $\neq 0$ ideal admits a unique factorization into primes

We haven't actually shown that $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain yet. In fact, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\omega]$ where $\omega = \frac{-1+\sqrt{-3}}{2}$, $\mathbb{Z}[\sqrt{-5}]$, and $\mathbb{Z}[\frac{-1+\sqrt{-23}}{2}]$ are all Dedekind domains.

However, $\mathbb{Z}[\sqrt{-3}]$ is not. If $I = (2, 1 + \sqrt{-3})$, then I is prime, but

$$I^2 = (4, 2(1 + \sqrt{-3}), (1 + \sqrt{-3})^2) = (4, 2(1 + \sqrt{-3}), -2 + 2\sqrt{-3}) = (2)(2, 1 + \sqrt{-3})$$

so that $I^2 = (2)I$. Also, the ideal (2) doesn't even factor into primes. In a Dedekind domain, we can cancel ideals from both sides of an equation.

To prove that every prime ideal is maximal in these rings isn't too ring.

For the other condition, it's enough to show that if A and B are ideals of R with $A \subseteq B$, then there exists an ideal C such that $A = BC$ (to contain is to divide).

Assuming this is true, let's show that every non-zero proper ideal I factors into primes. We can use the same kind of well-ordering principle argument we do for the integers, together with the concept of the norm of an ideal, $N(I) = \# R/I$.

Let $S = \{I \neq (0), (1) \mid I \neq$ a product of prime ideals $P_1 \cdots P_n\}$. If S is non-empty, we can choose an ideal in S of least nrom. Then certainly I is not maximal, so $I \subsetneq J$ for some other $J \neq (0)$. By our assumption, there is some proper ideal K such that $I = JK$, but $N(J), N(K) < N(I)$ so that $J, K \notin S$, hence

$$I = JK = P_1 \cdots P_n Q_1 \cdots Q_m.$$

Now, we claim that we can further reduce checking that our rings are Dedekind domains to checking that if I an ideal in R, then there exists a non-zero J such that $IJ = (\alpha)$ for some principal ideal (α).

To see that that condition implies that "to contain is to divide", suppose that $A \subseteq B$. Apply our condition to B, so that there is some non-zero B' such that $BB' = (\beta)$. Intuitively, we want to say something like

$$\frac{A}{B} = \frac{BB'}{(\beta)}$$

but that doesn't really make sense. Let $C = \beta^{-1}AB'$; this is clearly closed under multiplication by the ring and under addition, and it is actually an ideal (i.e. all of its elements are in the ring R) because

$$A \subseteq B \implies AB' \subseteq BB' = (\beta) \implies \beta^{-1}AB' \subseteq R$$

Thus

$$BC = B(\beta^{-1}AB') = \beta^{-1}ABB' = \beta\beta^{-1}A = A.$$

So, for any of the fields

$$K = \mathbb{Q}(i),\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-163}),\ \ldots$$

there is a corresponding Dedekind domain inside it

$$R = \mathbb{Z}[i],\ \mathbb{Z}[\sqrt{2}],\ \mathbb{Z}[\tfrac{-1+\sqrt{-3}}{2}],\ \mathbb{Z}[\tfrac{-1+\sqrt{-163}}{2}],\ \ldots$$

We can now define the Dedekind zeta function of K,

$$\zeta_K(s) = \sum_{\substack{\text{ideals} \\ I \neq (0)}} \frac{1}{N(I)^s} = \prod_{\substack{\text{prime ideals} \\ P \neq (p)}} \left(1 - \frac{1}{N(P)^s}\right)^{-1}$$

Question: What is $\lim_{s \to 1^+} \zeta_K(s)(s-1)$?

Question: How do primes in $\mathbb{Z}$ factor into primes in R?

	$\mathbb{Z}[i]$	$\mathbb{Z}[\omega]$	$\mathbb{Z}[\sqrt{-2}]$	$\mathbb{Z}[\sqrt{-5}]$
ramified $(p) = P^2$	2	3	2	2,5
split $(p) = PQ$ for $P \neq Q$	$p \equiv 1 \bmod 4$	$p \equiv 1 \bmod 3$	$p \equiv 1, 3 \bmod 8$	$p \equiv 1, 3, 7, 9 \bmod 20$
inert (p) is prime	$p \equiv 3 \bmod 4$	$p \equiv 2 \bmod 3$	$p \equiv 5, 7 \bmod 8$	$p \equiv 11, 13, 17, 19 \bmod 20$
modulus	4	3	8	20

Let $K = \mathbb{Q}(\sqrt{d})$ where d is a squarefree integer, $d \neq 1$. We call K a "quadratic field". It consists of all the numbers of the form

$$\alpha = a + b\sqrt{d}, \quad a, b \in \mathbb{Q}.$$

We defined the trace and the norm of α, respectively, to be

$$T(\alpha) = \alpha + \overline{\alpha} = 2a \qquad N(\alpha) = \alpha\overline{\alpha} = a^2 - db^2.$$

For any $\alpha \in K$, we have $T(\alpha), N(\alpha) \in \mathbb{Q}$. We've been considering the set R defined by

$$R = \{\alpha \in K \mid N(\alpha), T(\alpha) \in \mathbb{Z}\}.$$

On the homework, you should have found that

$$R = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Letting

$$\eta = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \bmod 4, \\ \frac{-1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

we have that

$$T(\eta) = \begin{cases} 0 & \text{if } d \equiv 2, 3 \bmod 4, \\ -1 & \text{if } d \equiv 1 \bmod 4, \end{cases} \qquad N(\eta) = \begin{cases} d & \text{if } d \equiv 2, 3 \bmod 4, \\ \frac{1-d}{4} & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

and that η is a root of the polynomial $f \in \mathbb{Z}[x]$ defined by

$$f(x) = \begin{cases} x^2 - d & \text{if } d \equiv 2, 3 \bmod 4, \\ x^2 + x + \frac{1-d}{4} & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Theorem. *The ring R is a Dedekind domain. That is, every non-zero prime ideal is maximal, every ideal factors into primes, and every non-zero proper ideal factors into primes uniquely.*

Let's first show that every non-zero prime ideal is maximal.

Proposition 3. *Let I be an ideal. Then we know that I is maximal $\iff$ R/I is a field.*

Proof. Let $\overline{x} \in R/I$, and suppose $\overline{x} \neq \overline{0}$, i.e. $x \notin I$. The ideal $I + (x)$ is an ideal of R containing I. □

Example. Let $R = \mathbb{Z}[i] = \mathbb{Z}[x]/(x^2 + 1)$, and let $I = (p)$ where p is a rational prime. Then

$$R/I = \mathbb{Z}[i]/(p) = (\mathbb{Z}[x]/(x^2 + 1))/(p) = \mathbb{Z}_p[x]/(x^2 + 1).$$

This is a field if and only if $x^2 + 1$ is irreducible in $\mathbb{Z}_p[x]$.

If $P \subset R$ is a maximal ideal, then R/P is a field with finitely many elements. You might know from your first year that we can only have $\#R/P = p^n$ for some prime number p and some n. Since we're in a finite field, if you add $\overline{1}$ to itself over and over, you have to start getting the same values; in fact, $\overline{p} = \overline{0}$. Thus, $p \in P$, so that $(p) \subset P$, and thus $p = PQ$ for some other ideal Q (because to divide is to contain).

Thus, our strategy for classifying the prime ideals of R will be to factor each of the ideals (p) in R into prime ideals of R.

Let's consider the case that: $R = \mathbb{Z}[\sqrt{d}]$, so that $d \equiv 2, 3 \bmod 4$.

If $p \mid d$, then

$$(p, \sqrt{d})^2 = (p^2, p\sqrt{d}, d) = (p)(p, \sqrt{d}, \tfrac{d}{p}) = (p)$$

where the last equality follows from the fact that d is squarefree, so that p cannot divide $\frac{d}{p}$, hence $(p, \sqrt{d}, \frac{d}{p}) = (1)$.

If $p = 2$ and $d = 2, 3 \bmod 4$, then

$$(2) = (2, 1 + \sqrt{d})^2 = (4, 2(1 + \sqrt{d}), 1 + d + 2\sqrt{d}) = (2)(2, 1 + \sqrt{d},)$$

Thus, if $p \mid 2d$, we have that $(p) = P^2$ for some prime ideal P of R with $N(P) = p$.

Now suppose $p \nmid 2d$. We have that

$$R/(p) = (\mathbb{Z}[x]/(x^2 - d))/(p) = \mathbb{Z}_p[x]/(x^2 - d)$$

and that (p) is maximal $\iff$ $x^2 - d$ is irreducible modulo p.

The polynomial $x^2 - d$ factors modulo p $\iff$ $d \equiv \square \bmod p$ $\iff$ $\left(\frac{d}{p}\right) = 1$.

If $p \equiv 3 \bmod 4$, we have

$$\left(\frac{d}{p}\right) = \underbrace{(-1)^{\frac{p-1}{2}}}_{\substack{\text{depends on} \\ p \bmod 4}} \underbrace{\left(\frac{p}{d}\right)}_{\substack{\text{depends on} \\ p \bmod d}}$$

so that the entire expression depends on $p \bmod 4d$. Thus, in the $d \equiv 3 \bmod 4$ case,

ramified	$(p) = P^2$	$p \mid 2d$
split	$(p) = P\overline{P}$	$(-1)^{\frac{p-1}{2}} \left(\frac{p}{d}\right)_{\text{Jac}} = 1$
inert	(p) is prime	the above is $\neq 1$

If $d \equiv 2 \bmod 4$, then $d = 2e$ for some odd e.

$$\left(\frac{d}{p}\right) = \left(\frac{2e}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{e}{p}\right) = \underbrace{(-1)^{\frac{p^2-1}{8}}}_{\substack{\text{depends on} \\ p \bmod 8}} \underbrace{(-1)^{\frac{p-1}{2}\frac{e-1}{p}}}_{\substack{\text{depends on} \\ p \bmod 4}} \underbrace{\left(\frac{p}{e}\right)_{\text{Jac}}}_{\substack{\text{depends on} \\ p \bmod e}}$$

so the entire expression depends on $p \bmod 8e$ (note that $8e = 4d$).

Define a Dirichlet character χ modulo $4d$ as follows: when $d \equiv 3 \bmod 4$,

$$\chi(n) = \begin{cases} 0 & \text{if } \gcd(n, 4d) > 1, \\ (-1)^{\frac{n-1}{2}} \left(\frac{n}{d}\right)_{\text{Jac}} & \text{if } \gcd(n, 4d) = 1. \end{cases}$$

In the $d \equiv 2 \bmod 4$ case, with $d = 2e$,

$$\chi(n) = \begin{cases} 0 & \text{if } \gcd(n, 4d) > 1, \\ (-1)^{\frac{n^2-1}{8}}(-1)^{\frac{n-1}{2}\frac{e-1}{2}} \left(\frac{n}{e}\right) & \text{if } \gcd(n, 4d) = 1. \end{cases}$$

We have to check that $\chi(mn) = \chi(m)\chi(n)$. This follows from

$$\left(\frac{mn}{d}\right)_{\text{Jac}} = \left(\frac{m}{d}\right)_{\text{Jac}} \left(\frac{n}{d}\right)_{\text{Jac}}$$

Thus, at least in the $d \equiv 2, 3 \bmod 4$ cases, there's a Dirichlet character χ mod $4d$ such that

$$\chi(p) = \begin{cases} 0 & \text{if } (p) = P^2, \\ 1 & \text{if } (p) = P\overline{P}, \\ -1 & \text{if } (p) \text{ prime.} \end{cases}$$

Let p be a prime. We're interested in how the polynomial x^2-d can factor modulo p. There are three possibilities:

$$x^2 - d \equiv \begin{cases} (x-a)^2 \\ (x-a)(x-b) \text{ for some } a \not\equiv b \\ \text{irreducible} \end{cases}$$

Note that if $x^2 - d \equiv (x-a)^2 = x^2 - 2ax + a^2$, we must have that $2a \equiv 0 \bmod p$ and that $a^2 \equiv -d \bmod p$, so that either $p = 2$, or $p \mid a$ and hence $p \mid d$. In fact, $x^2 - d \equiv (x-a)^2 \bmod p$ if and only if $p \mid 2d$. If $p \nmid 2d$, then we can use the Legendre symbol to distinguish the cases. In general, we can say that

$$x^2 - d \equiv \begin{cases} (x-a)^2 & \text{if } \left(\frac{d}{p}\right) = 0 \text{ (assuming } p \text{ is odd)} \\ (x-a)(x-b) \text{ for some } a \not\equiv b, & \text{if } \left(\frac{d}{p}\right) = 1 \\ \text{irreducible} & \text{if } \left(\frac{d}{p}\right) = -1 \end{cases}$$

Last time, we said that if $d \equiv 3 \bmod 4$, then $\left(\frac{d}{p}\right)$ depends only on the value of $p \bmod 4d$. If $p \nmid 2p$, then

$$\left(\frac{d}{p}\right) = \left(\frac{p}{d}\right)_{\text{Jac}} (-1)^{\frac{p-1}{2}\frac{d-1}{2}} = \left(\frac{p}{d}\right)_{\text{Jac}} (-1)^{\frac{p-1}{2}}$$

but this is actually an error; we only know how to make sense of the Jacobi symbol when $d > 0$. But it's okay; if $d < 0$, then

$$\left(\frac{d}{p}\right) = \left(\frac{-|d|}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{|d|}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{|d|}\right)_{\text{Jac}} (-1)^{\frac{p-1}{2}\frac{|d|-1}{2}}$$

and $\frac{|d|-1}{2}$ is even, so that either way, we get

$$\left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{|d|}\right)_{\text{Jac}}$$

Thus, in the case that $d \equiv 3 \bmod 4$, we can define χ by

$$\chi(n) = \begin{cases} 0 & \text{if } \gcd(n, 2d) > 1, \\ (-1)^{\frac{n-1}{2}} \left(\frac{n}{|d|}\right)_{\text{Jac}} & \gcd(n, 2d) = 1. \end{cases}$$

Note that $\chi(n)$ depends only on $n \bmod 4d$, that $\chi(mn) = \chi(m)\chi(n)$, and that for a (positive) prime p,

$$\chi(p) = \begin{cases} 0 & \text{if } x^2 - d \equiv (x-a)^2 \bmod p, \\ 1 & \text{if } x^2 - d \equiv (x-a)(x-b) \bmod p, \\ -1 & \text{if } x^2 - d \text{ is irreducible } \bmod p. \end{cases}$$

Because χ is a periodic function on the positive integers, we can extend χ to negative numbers as well by defining

$$\chi(-1) = (-1)\left(\frac{-1}{|d|}\right) = (-1)(-1)^{\frac{|d|-1}{2}} = \begin{cases} 1 & \text{if } d > 0, \\ -1 & \text{if } d < 0 \end{cases} \text{ (because } d \equiv 3 \bmod 4)$$

If χ is any Dirichlet character, we must either choose $\chi(-1) = \pm 1$ because $\chi(-1)^2 = \chi((-1)^2) = \chi(1) = 1$. Thus, χ is an even function or odd function, depending on whether $\chi(-1) = 1$ or -1, respectively.

When $d \equiv 2 \bmod 4$, we again get a Dirichlet character χ modulo $4d$ that is even or odd depending on whether $d > 0$ or $d < 0$.

Now we consider the case of $d \equiv 1 \bmod 4$. So we need to figure out how the polynomial $x^2 + x - \frac{d-1}{4}$ factors modulo p.

If $p = 2$, then if $d \equiv 1 \bmod 8$, it factors as $x(x+1)$, while if $d \equiv 5 \bmod 8$, it is $x^2 + x + 1$ which is irreducible. Thus, it factors modulo 2 if and only if $\left(\frac{2}{|d|}\right) = 1$.

If $p \neq 2$, then

$$\begin{aligned} x^2 + x + \frac{d-1}{4} &\equiv x^2 + x + \frac{1}{4} - \frac{d}{4} \bmod p \\ &\equiv \left(x + \frac{1}{2}\right)^2 - \frac{d}{4} \bmod p \end{aligned}$$

so that the polynomial factors if and only if $\frac{d}{4} \equiv \square \bmod p$, which is the case if and only if $\left(\frac{d}{p}\right) = 1$.

If $d > 0$, then $\left(\frac{d}{p}\right) = \left(\frac{p}{|d|}\right)_{\text{Jac}}$, and if $d < 0$, then

$$\left(\frac{d}{p}\right) = \left(\frac{-|d|}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{|d|}{p}\right) = \cdots \text{ (same trick) } = \left(\frac{p}{|d|}\right)$$

Thus, if $p \nmid d$ then $x^2 + x + \frac{d-1}{4}$ factors $\iff \left(\frac{p}{|d|}\right)_{\text{Jac}} = 1$, and if $p \mid d$, then

$$x^2 + x + \frac{d-1}{4} \equiv x^2 + x + \frac{1}{4} \equiv \left(x + \frac{1}{2}\right)^2$$

Therefore, in the $d \equiv 1 \bmod 4$ case, we can let

$$\chi(n) = \begin{cases} 0 & \text{if } (n, d) > 1, \\ \left(\frac{n}{|d|}\right)_{\text{Jac}} & \text{if } (n, d) = 1. \end{cases}$$

To summarize, let $d \neq 1$ be squarefree. Let

$$D = \begin{cases} 4d & \text{if } d \equiv 2, 3 \bmod 4, \\ d & \text{if } d \equiv 1 \bmod 4 \end{cases} \qquad \text{and} \qquad f(x) = \begin{cases} x^2 - d & \text{if } d \equiv 2, 3 \bmod 4, \\ x^2 + x - \frac{d-1}{4} & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

Theorem. *There is a Dirichlet character modulo D such that if p is a positive prime, then $f(x)$ modulo p either is square, splits, or is irreducible as $\chi(p)$ is $0, 1, -1$.*

Let's go back to quadratic fields. Let $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{D})$. Then we say that D is the discriminant of K, and

$$R = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod 4, \\ \mathbb{Z}[\frac{-1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

is called the "ring of integers of K". Then if p is a positive prime of $\mathbb{Z}$, then

$$(p) = \begin{cases} P^2 & \text{if } \chi(p) = 0, \\ P\overline{P} & \text{if } \chi(p) = 1, \\ P \text{ prime} & \text{if } \chi(p) = -1. \end{cases}$$

The "algebraic phase":

$$\zeta_K(s) = \sum_{\substack{I \subseteq R \\ \text{non-zero} \\ \text{ideals}}} \frac{1}{N(I)^s} = \prod_{\substack{\text{prime } P \\ P \neq (0)}} \left(1 - \frac{1}{N(P)^s}\right)^{-1}$$

$$= \prod_{\substack{p \in \mathbb{Z} \\ \text{prime}}} \prod_{P|(p)} \left(1 - \frac{1}{N(P)^s}\right)^{-1} = \prod_{\chi(p)=0} \left(1 - \frac{1}{p^s}\right)^{-1} \cdot \prod_{\chi(p)=1} \left(1 - \frac{1}{p^s}\right)^{-2} \cdot \prod_{\chi(p)=-1} \left(1 - \frac{1}{p^{2s}}\right)^{-1}$$

Thus,

$$\zeta_K(s) = \zeta(s) \prod_{\chi(p)=1} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{\chi(p)=-1} \left(1 + \frac{1}{p^s}\right)^{-1} = \zeta(s) \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

Writing the second product as

$$\prod_p \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{p^{2s}} + \cdots\right) = 1 + \frac{\chi(2)}{2^s} + \frac{\chi(3)}{3^s} + \cdots$$

we have that

$$\zeta_K(s) = \zeta(s) L(\chi, s)$$

where χ is a quadratic Dirichlet character modulo D, which takes values $0, 1, -1$.

We're interested in finding

$$\lim_{s \to 1^+} \zeta_K(s)(s-1) = \lim_{s \to 1^+} \zeta(s)(s-1) L(\chi, s) = \lim_{s \to 1^+} L(\chi, s) = L(\chi, 1)$$

R forms a lattice in $\mathbb{C}$

(diagram)

$$\#\{\text{non-zero ideals } I \text{ such that } N(I) \leq x\} = \frac{1}{w} \cdot \#\{\alpha \in R, \alpha \neq 0 \text{ such that } N(\alpha) = a^2+b^2 \leq x, \text{ where } \alpha = a+bi\}$$

where w is the number of units of R. This is approximately equal to

$$\frac{1}{w} \cdot \frac{\text{vol(circle)}}{\text{vol(parallelogram)}} = \frac{1}{w} \cdot \frac{\pi x}{\sqrt{|D|}/2} + O(\sqrt{x}) = \frac{2\pi x}{w\sqrt{|D|}}$$

Thus $L(1,\chi) = \frac{2\pi}{w\sqrt{|D|}}$. For example, for $\mathbb{Z}[i]$, we have $D = -4$ and $w = 4$, so

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots = \frac{\pi}{4}$$

For $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, we have $D = -3$ and $w = 6$, so we get

$$1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \frac{1}{7} - \frac{1}{8} + \cdots = \frac{\pi}{3\sqrt{3}}$$

However, in $\mathbb{Z}[\sqrt{-5}]$ (which is not a PID), we have $D = -20$ and $w = 2$, but

$$L(1,\chi) = \frac{\pi}{2\sqrt{5}} \neq \frac{2\pi}{2\sqrt{20}}$$

Thus,

$$\{\text{non-zero ideals in } R = \mathbb{Z}[\sqrt{-5}]\} \longleftrightarrow \{\text{non-zero } (\alpha)\} \sqcup \{\text{non-principal ideals}\}$$

Let $P = (2, 1+\sqrt{-5})$. Then we've seen that for I non-principal, $IP = (\alpha)$ for some α. Thus, we have a correspondence

$$\{\text{non-principal ideals}\} \longleftrightarrow \{\alpha \neq 0, \alpha \in P \text{ (up to units)}\}$$

by sending an ideal I to the α that occurs as $IP = (\alpha)$ Let $K = \mathbb{Q}(\sqrt{-5})$. Then

$$\zeta_K(s) = \sum_{I \neq (0)} \frac{1}{N(I)^s} = \sum_{\substack{I \neq (0) \\ \text{principal}}} \frac{1}{N(I)^s} + \sum_{\substack{I \text{ non-} \\ \text{principal}}} \frac{1}{N(I)^s}$$

If $A(x) = \#\{I \neq (0), N(I) \leq x\}$, then

$$A(x) = A_p(x) + A_{np}(x) = \#\{I \text{ principal}, N(I) \leq x\} + \#\{I \text{ non-principal}, N(I) \leq x\}$$

$$= \frac{1}{w}\#\{\alpha \in R, \alpha \neq 0, N(\alpha) \leq x\} + \frac{1}{w}\#\{\alpha \in P, \alpha \neq 0, N(\alpha) \leq 2x\}$$

Note that on the right, $N(I) \leq x$ if and only if $2NI \leq 2x$ if and only if $N(\alpha) \leq 2x$.

$$\approx \frac{1}{w}\frac{2\pi x}{\sqrt{|D|}}\frac{\pi}{2\sqrt{5}} + \frac{1}{2}\frac{2\pi x}{2\sqrt{5}} = \frac{\pi}{\sqrt{5}}x$$

More generally, in $\mathbb{Q}(\sqrt{d})$, let's define I and J, ideals of R, to be equivalent when there are non-zero $\alpha, \beta \in R$ such that $(\alpha)I = (\beta)J$. This defines an equivalence relation $\sim$ on the non-zero ideals of R. Note that if $I \sim (\gamma)$, then $(\alpha)I = (\beta\gamma)$ and hence $I = (\alpha^{-1}\beta\gamma)$, so that I is prinicipal. Thus, the principal ideals form exactly one equivalence class of $\sim$.

Note also that if $I \sim J$ and L is an ideal, then $IL \sim JL$, so that we can make an operation on the equivalence classes of $\sim$. If $[I]$ is the equivalence class of I, then we can define

$$[I] \cdot [J] = [IJ]$$

Multiplication of equivalence classes is commutative and associative, and there is an identiy, namely $[(1)]$. In order to have inverses, we need to know that for any ideal I there is some J such that $IJ = (\alpha)$, so that

$$[I][J] = [IJ] = [(\alpha)] = [(1)]$$

We showed this on the homework. Thus, the set of equivalence classes form a group, called the class group. The number D uniquely specifies $K = \mathbb{Q}(\sqrt{d})$, so we will call the class group H_D.

For example, H_{-4}, H_{-3}, H_8, H_{-8} are all trivial groups.

However, H_{-20} is a group with two elements, because any $[I] \neq [(1)]$ has inverse $[(P)]$, because any non-principal ideal I has the property that IP is principal.

We have that H_D is the trivial group $\iff$ R is a PID $\iff$ R has UPF.

H_D is the "obstruction" to R being a PID.

Theorem. *H_D is a finite group. We call the size of H_D the class number, h_D.*

As usual, $K = \mathbb{Q}(\sqrt{d})$ for some squarefree $d \neq 1$, and R is the ring of integers in K, namely $R = \mathbb{Z}[\sqrt{d}]$ (in which case $D = 4d$) or $R = \mathbb{Z}[\frac{-1+\sqrt{d}}{2}]$ (in which case $D = d$).

We put an equivalence relation on the non-zero ideals of R, defined by $I \sim J$ if $(\alpha)I = (\beta)J$ for some non-zero $\alpha, \beta \in R$. We defined H_D to be the group of equivalence classes of ideals, under multiplication.

If $H_D = \{[(1)]\}$, then every ideal is principal, which by definition is the case iff R is a PID, so R would also have UPF. In fact, the converse holds as well; R has UPF implies that $H_D = \{[(1)]\}$. Intuitively, the group H_D measures how far R is from being a PID. Today, we'll be proving (only for $D < 0$, but it's true in general)

Theorem. *H_D is a finite group.*

Proof. If we plot points of R in $\mathbb{C} \cong \mathbb{R}^2$, then R is a lattice, with $\mathrm{vol}(R) = \frac{\sqrt{|D|}}{2}$. If $I \subset R$ is any non-zero ideal, then I is also a lattice, with

$$\mathrm{vol}(I) = \mathrm{vol}(R) \cdot N(I) = \frac{\sqrt{|D|}}{2} \cdot N(I)$$

(diagram)

Lemma 1. *Let $M = \frac{2}{\pi}\sqrt{|D|}$. Then every non-zero ideal $I \subset R$ contains some $\alpha \neq 0$ with $N(\alpha) < M \cdot N(I)$.*

Proof. If $S =$ the circle of radius x centered at 0, then S contains a non-zero lattice point α as long as $\mathrm{vol}(S) > 4\,\mathrm{vol}(I)$, or equivalently

$$\pi x^2 > 2\sqrt{|D|} \cdot N(I)$$
$$x^2 > M \cdot N(I)$$

Let $x = \sqrt{M \cdot N(I)} + \epsilon$. Then we get an α in I such that $N(\alpha) \leq x^2$, i.e. $N(\alpha) \leq M \cdot N(I)$ (we fiddled with this ϵ a bit, but since $M \cdot N(I)$ is not an integer and $N(\alpha)$ is, we're okay). □

Lemma 2. *Every equivalence class of ideals contains some I such that $N(I) < M$.*

Proof. Say that $[I]$ is an equivalence class of ideals. Choose $J \in [I]^{-1}$, i.e. an ideal J such that $IJ =$ principal. There exists some non-zero $\alpha \in J$ such that $N(\alpha) < M \cdot N(J)$. But then $(\alpha) \subset J$, so that $(\alpha) = JL$ for some ideal L. Thus $N(\alpha) = N(J) \cdot N(L)$, and thus $N(L) < M$. Because $[J][L] = [(1)]$, we have that $[L] = [J]^{-1} = [I]$. □

Lemma 3. *There are only finitely many ideals I of norm n.*

Proof. If $N(I) = n$, then we claim $n \in I$. This is because R/I is an abelian group under addition of size n, hence $\overline{n} = \overline{1} + \cdots + \overline{1} = \overline{0}$.

Thus, if $N(I) = n$, we have that $n \in I$, and hence $(n) \subseteq I$. Thus $I \mid (n) = P_1^{a_1} \cdots P_t^{a_t}$, and because I will also factor into prime ideals, there can only be finitely many divisors of (n), and hence only finitely many ideals of norm n. □

□

Example. $d = D = -23$, so that $R = \mathbb{Z}[\eta]$ where $\eta = \frac{-1+\sqrt{-23}}{2}$ satisfies $\eta^2 + \eta + 6 = 0$.

We have that $M \approx 3.05$, so we want to classify all the ideals of norm ≤ 3.

Given an ideal class $[I]$ of R, we define the partial zeta function

$$\zeta_{[I]}(s) = \sum_{J \in [I]} \frac{1}{N(J)^s}$$

Let I' be an ideal with $II' = (\alpha)$. If $J \sim I$, then $JI' \sim II' \sim (1)$, so that $JI' = (\beta)$ for some $\beta \in I'$. We actually get a correspondence

$$[I] \longleftrightarrow \{\beta \in I', \beta \neq 0 \text{ up to units}\}$$
$$J \longrightarrow JI' = (\beta)$$
$$J \longleftarrow (\beta)(I')^{-1}$$

Thus,

$$\zeta_{[I]}(s) = N(I')^s \sum_{\substack{\beta \in I' \\ \beta \neq 0 \\ \text{up to units}}} \frac{1}{N(\beta)^s}$$

We want to figure out

$$\lim_{s \to 1^+} \left(\sum_{\substack{\beta \in I' \\ \beta \neq 0 \\ \text{up to units}}} \frac{1}{N(\beta)^s} \right) (s-1)$$

(picture) The number of β such that $N(\beta) \leq x$, $\beta \in I'$, $\beta \neq 0$ is approximately

$$\frac{\pi x}{\text{vol}(I')} = \frac{\pi}{\frac{\sqrt{|D|}}{2} \cdot N(I')}$$

To find this up to units, we just divide by $w = \#$ units.

Let $K = \mathbb{Q}(\sqrt{d})$, for $d \neq 1$ squarefree, let D be the discriminant of K, let χ be the Dirichlet character modulo D, and let R be the ring of integers of K.

We've seen that

$$\chi(p) = \begin{cases} 0 & (p) = P^2 \text{ (ramified)} \\ 1 & (p) = PQ \text{ (split)} \\ -1 & (p) = \text{prime (inert)} \end{cases}$$

This let us do the "algebraic phrase",

$$\zeta_K(s) = \zeta(s)L(s,\chi)$$

Last time, we did the analytic phase, though only for $D < 0$: we showed that H_D is finite, and that

$$\lim_{s \to 1^+} \zeta_K(s)(s-1) = \frac{2\pi}{w\sqrt{|D|}}\, h_D$$

where $h_D = \#H_D$ and $w =$ number of units in R. Note that $w = 2$ unless $R = \mathbb{Z}[i]$, in which case $w = 4$, or $R = \mathbb{Z}[\omega]$, in which case $w = 6$.

Combining phases, we get the class number formula for $\mathbb{Q}(\sqrt{D})$ for $D < 0$, when $\chi(-1) = -1$,

$$L(1,\chi) = \frac{2\pi}{w\sqrt{|D|}}\, h_D$$

On the homeworks, you showed that

$$-\frac{\pi}{|D|\sqrt{|D|}} \sum_{a=1}^{D-1} \chi(a)a = \frac{2\pi}{w\sqrt{|D|}}\, h_D$$

and canceling a bit,

$$-\frac{1}{|D|} \sum_{a=1}^{D-1} \chi(a)a = \frac{2}{w}\, h_D$$

which is just a relationship between two rational numbers.

Let's do some examples. For $D = -3$, we have

$$-\frac{1}{|-3|}(1-2) = \frac{2}{6} \cdot 1 \qquad \checkmark$$

For $D = -4$, we have

$$-\frac{1}{|-4|}(1-3) = \frac{2}{4} \cdot 1 \qquad \checkmark$$

The next largest discriminant is $D = -7$, which corresponds to $\mathbb{Z}[\frac{-1+\sqrt{-7}}{2}]$, a ring that we haven't investigated yet.

$$-\frac{1}{|-7|}(1+2-3+4-5-6) = \frac{2}{2} \cdot 1 \implies h_{-7} = 1$$

For $D = -8$, i.e. for $\mathbb{Z}[\sqrt{-2}]$, we have

$$-\frac{1}{|-8|}(1+3-5-7) = \frac{2}{2} \cdot 1 \implies h_{-8} = 1$$

For $D = -20$, i.e. for $\mathbb{Z}[\sqrt{-5}]$, we have

$$-\frac{1}{|-20|}(1+3+7+9-11-13-17-19) = \frac{2}{2}\cdot 2 \implies h_{-20} = 2$$

Now let's consider the case of $D > 0$. We now say that K is a real quadratic field. The main differences with the imaginary quadratic fields is that there are infintiely many units, and that norms of elements can be negative (thus, we have $N((\alpha)) = |N(\alpha)|$).

For example, let's consider $\mathbb{Z}[\sqrt{2}]$. The units are $\pm(1+\sqrt{2})^n$ for $n \in \mathbb{Z}$. For $\alpha = a+b\sqrt{d}$, we define $\alpha' = a-b\sqrt{d}$, and then

$$N(\alpha) = \alpha\alpha' = a^2 - db^2 = \pm 1 \iff \alpha \text{ is a unit.}$$

To see that there are infinitely many units in $\mathbb{Z}[\sqrt{d}]$, note that we know there is a solution to Pell's equation

$$a^2 - db^2 = \pm 1$$

with $a + b\sqrt{d} \neq \pm 1$, and so $|a + b\sqrt{d}| \neq 0, 1$. All powers of this solution will also be solutions.

For a ring $\mathbb{Z}[\eta]$ with $\eta = \frac{-1+\sqrt{d}}{2}$, to show there are infinitely many units, we instead want to solve

$$N(a+b\eta) = (a+b\eta)(a+b\eta') = a^2 - ab + \left(\frac{-1+d}{4}\right)b^2 = \pm 1$$

We can do this with the magic box, for example for $D = 5$, in which case $R = \mathbb{Z}[\frac{-1+\sqrt{5}}{2}]$, we have that $\frac{-1+\sqrt{5}}{2} = [0; \overline{1}]$, so that

		0	1	1	1	1	1
0	1	0	1	1	2	3	5
1	0	1	1	2	3	5	8

Thus, R always has a unit $\neq \pm 1$.

We plot R inside $\mathbb{R}^2$ somewhat differently. We previously plotted $a + bi$ as (a, b), for example. Now, we'll plot $a + b\sqrt{d}$ as $(a + b\sqrt{d}, a - b\sqrt{d})$.

(diagram)

We can see from this picture that the volume of the fundamental parallelogram of $\mathbb{Z}[\sqrt{2}]$ is $\sqrt{8}$. In fact, in general $\text{vol}(R) = \sqrt{|D|}$, regardless of whether we are looking at real or imaginary quadratic fields.

Let ϵ be the smallest unit such that $\epsilon > 1$. We can talk about this because the units must be on the hyperbola $xy = 1$ or $xy = -1$, and lattice points can't get arbitrarily close to each other.

We claim that any unit in R is $\pm\epsilon^n$ for some $n \in \mathbb{Z}$. For any unit $\mu > 0$ (we can just take $-\mu$ for a negative unit), we must have that $\epsilon^n \leq \mu < \epsilon^{n+1}$ for some n, because the powers of ϵ are discrete and

Let K be a quadratic field. What we figured out last class was that

$$\lim_{s\to 1^+} \zeta_K(s)(s-1) = \begin{cases} \dfrac{2h\log(\epsilon)}{\sqrt{|D|}} & \text{if } K \text{ is a real field,} \\ \dfrac{2\pi h}{w\sqrt{|D|}} & \text{if } K \text{ is an imaginary field} \end{cases}$$

where $D =$ discriminant, $h =$ class number, $w =$ roots of unity, and $\epsilon =$ fundamental unit.

Areas under hyperbolas $\longrightarrow$ logarithms

Areas under circles, ellipses $\longrightarrow \pi$

Now let's talk about more general fields, not necessarily quadratic anymore. If $K = \mathbb{Q}(\sqrt[3]{2})$, then

$$R = \mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}.$$

This R is a Dedekind domain. The fundamental unit is

$$(\underbrace{1 + \sqrt[3]{2} + \sqrt[3]{4}}_{\epsilon})(-1 + \sqrt[3]{2}) = 1.$$

Then

$$\lim_{s\to 1^+} \zeta_K(s)(s-1) = \frac{\pi}{3\sqrt{3}}\log(\epsilon)$$

(for this R, we have $h = 1$).

A number $\alpha \in \mathbb{C}$ is algebraic if $f(\alpha) = 0$ for some $f(x) = a_0 + a_1x + \cdots + a_nx^n$ for some $a_i \in \mathbb{Q}$, $a_n \neq 0$.

A number field is a field of the form $\mathbb{Q}(\alpha)$ for some algebraic α, e.g. $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\theta)$ where $\theta^3 + \theta + 1 = 0$.

There is an analog of the class number formula for any number field K.

Now, onto something seemingly unrelated. You probably know the formulas

$$1 + 2 + \cdots + (n-1) = \frac{n(n-1)}{2} = \frac{n^2}{2} - \frac{n}{2}$$

$$1^2 + \cdots + (n-1)^2 = \frac{n^3}{3} - \frac{n^2}{2} + \frac{n}{6}$$

We might predict that

$$1^m + \cdots + (n-1)^m = S_m(n) = \text{polynomial in } n \text{ of degree } m+1.$$

We declare $S_0(n) = n$.

Consider the exponential generating function

$$S_0(n) + S_1(n)\frac{x}{1!} + S_2(n)\frac{x^2}{2!} + S_3(n)\frac{x^3}{3!} + \cdots$$

$$= \sum_{m=0}^{\infty} S_m(n)\frac{x^m}{m!} = \sum_{m=0}^{\infty}\sum_{k=0}^{n-1}\frac{k^m x^m}{m!} = \sum_{k=0}^{n-1} e^{kx} = \frac{e^{nx}-1}{e^x-1}$$

and note that Taylor's theorem implies that

$$S_m(n) = \frac{d^m}{dx^m}\left(\frac{e^{nx}-1}{e^x-1}\right)\Big|_{x=0}.$$

Now, $\frac{1}{e^x-1}$ would have a discontinuity at $x=0$, but expanding the numerator $e^{nx}-1$ as a Taylor series, we see that it has no constant term, and it turns out (via L'Hopital's rule) that $\frac{x}{e^x-1}$ is perfectly well-behaved.

$$B_m = \frac{d^{(m)}}{dx^{(m)}}\left(\frac{x}{e^x-1}\right)\Big|_{x=0}$$

so

$$\frac{x}{e^x-1} = B_0 + B_1 x + B_2\frac{x^2}{2!} + B_3\frac{x^3}{3!} + \cdots$$

m	B_m
0	1
1	$-\frac{1}{2}$
2	$\frac{1}{6}$
3	0
4	$-\frac{1}{30}$
5	0
6	$\frac{1}{42}$
7	0
8	$-\frac{1}{30}$
9	0
10	$\frac{5}{66}$
11	0
12	$-\frac{691}{2730}$

$$\frac{e^{nx}-1}{e^x-1} = \sum_{m=0}^{\infty}\frac{S_m(n)x^m}{m!}$$

$$= \frac{e^{nx}-1}{x}\frac{x}{e^x-1} = \frac{1}{x}\left(nx + \frac{n^2x^2}{2!} + \frac{n^3x^3}{3!} + \cdots\right)$$

$$= \frac{1}{x}\left(B_0 + B_1x + B_2\frac{x^2}{2!} + \frac{B_3}{x^3}3! + \cdots\right)$$

Thus,

$$S_0(n) = nB_0$$

$$S_1(n) = \frac{n^2}{2!}B_0 + \frac{nB_1}{1!}$$

$$S_2(n) = 2!\left(\frac{n^3}{3!}B_0 + \frac{n^2}{2!}\frac{B_1}{1!} + \frac{n}{1!}\frac{B_2}{2!}\right)$$

The pattern seems to be

$$S_m(n) = \frac{1}{m+1}\left(n^{m+1}B_0 + \binom{m+1}{1}B_1 + \binom{m+1}{2}n^{m-1}B_2 + \cdots + \binom{m+1}{m}nB_m\right)$$

This looks somewhat similar to a binomial expansion; in fact if we expand

$$\text{“}\frac{1}{m+1}\left[(n+B)^{m+1} - B^{m+1}\right]''$$

and replace B^k with B_k, we get the correct answer. Thus, for example,

$$S_3(n) = \frac{1}{4}\left((n+B)^4 - B^4\right) = \frac{1}{4}\left(n^4 + 4n^3B_1 + 6n^2B_2 + 4nB_3\right)$$

Euler proved that for any even $m \geq 2$,

$$\zeta(m) = \frac{|B_m|(2\pi)^m}{2(m!)}$$

and that

$$\sum_{m=0}^{\infty} \frac{B_m x^m}{m!} = \frac{x}{e^x - 1} = -\frac{x}{1 - e^x} = -x\sum_{n=0}^{\infty} e^{nx}$$

so that

$$\sum_{m=0}^{\infty} \frac{B_m x^{m-1}}{m(m-1)!} = -\sum_{n=0}^{\infty} e^{nx}$$

$$\zeta(1-m) = -\frac{B_m}{m}$$

Roots of Unity

$$\zeta_1 = 1 \qquad X - 1$$

$$\zeta_2 = -1 \qquad X + 1 = \frac{X^2 - 1}{X - 1}$$

$$\zeta_3 = -\frac{1}{2} + \frac{\sqrt{-3}}{2} \qquad X^2 + X + 1 = \frac{X^3 - 1}{X - 1}$$

$$\zeta_4 = i \qquad X^2 + 1 = \frac{X^4 - 1}{(X - 1)(X + 1)}$$

$$\zeta_5 \qquad X^4 + X^3 + X^2 + X + 1 = \frac{X^5 - 1}{X - 1}$$

$$\zeta_6 = -\frac{1}{2} - \frac{\sqrt{-3}}{2} \qquad X^2 - X + 1 = \frac{X^6 - 1}{(X - 1)(X + 1)(X^2 - X - 1)}$$

In general, the polynomial for ζ_p where p is a prime is $X^{p-1} + X^{p-2} + \cdots + X + 1$.

The nth cyclotimic field is

$$\mathbb{Q}(\zeta_n) = \{a_0 + a_1\zeta_n + \cdots + a_{\phi(n)-1}\zeta_n^{\phi(n)-1} \mid a_i \in \mathbb{Q}\}.$$

This is a field of degree $\phi(n)$.

We only really talked about quadratic fields, e.g. $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(\sqrt{-11})$. The only cylcotomic fields that are quadratic are $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$. Note that we aren't missing $\mathbb{Q}(\zeta_6)$ because $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3)$.

The ring $\mathbb{Z}[\zeta_n]$ is a Dedekind ring, so it has unique factorization of ideals. We're interested in knowing how big its class group is.

Let's review our work for these quadratic cyclotomic fields.

$$\zeta_{\mathbb{Q}(\zeta_3)}(s) = \zeta(s)L(s, \chi_{-3}) \qquad \text{where} \quad \begin{array}{c|ccccc} n & 1 & 2 & 3 & 4 & 5 \\ \chi_{-3}(n) & 1 & -1 & 0 & 1 & -1 \end{array} \qquad = x^2 + x + 1 \bmod p$$

$$\zeta_{\mathbb{Q}(\zeta_4)}(s) = \zeta(s)L(s, \chi_{-4}) \qquad \text{where} \quad \begin{array}{c|ccccc} n & 1 & 2 & 3 & 4 & 5 \\ \chi_{-4}(n) & 1 & 0 & -1 & 0 & 1 \end{array} \qquad = x^2 + 1 \bmod p$$

On the homework, you looked at how $x^4 + x^3 + x^2 + x + 1$ factors modulo p.

When $p = 5$, we get $\Phi \equiv (x - 1)^4 = x4 - 4x^3 + 6x^2 - 4x + 1 \bmod 5$.

When $p \equiv 1 \bmod 5$, U_p has $p - 1$ elements, and U_p has a generator g, and if we let $h = g^{\frac{p-1}{5}}$, then $h^5 = 1$, and $h \neq 1$, so that $\Phi \equiv (x - h)(x - h^2)(x - h^3)(x - h^4) \bmod p$.

If $p \not\equiv 1 \bmod 5$, then there are no roots of Φ in $\mathbb{Z}_p$, because if $\Phi(h) = 0$ then $h^5 - 1 = \Phi(h)(h - 1) = 0$, so that h is an element of order 5 in U_p, hence $5 \mid p - 1$. Thus, if $p \not\equiv 1 \bmod 5$, either Φ is irreducible or it factors into two quadratics.

Let's suppose it factors into two irreducible quadratics, $f(x)$ and $g(x)$. Then $\mathbb{Z}_p[x]/(f(x))$ is a field of p^2 elements. It has a root of f, let's call it h.

$$\Phi(x) \equiv \begin{cases} (x-1)^4 & p = 5 \\ (x-a)(x-b)(x-c)(x-b) & p \equiv 1 \bmod 5 \\ \text{irreducible} & p \equiv 2, 3 \bmod 5 \\ P(x)Q(x), \text{ each irreducible} & p \equiv 4 \bmod 5 \end{cases}$$

$$(p) \equiv \begin{cases} P^4 & p = 5 \quad \text{totally ramified} \quad N(P) = p \\ P_1P_2P_3P_4 & p \equiv 1 \bmod 5 \quad \text{totally split} \quad N(P_i) = p \\ P & p \equiv 2, 3 \bmod 5 \quad \text{inert} \quad N(P) = p^4 \\ P_1P_2 & p \equiv 4 \bmod 5 \quad \text{split into two factors} \quad N(P_i) = p^2 \end{cases}$$

$$\zeta_{\mathbb{Q}(\zeta_5)}(s) = \prod_P \left(1 - \frac{1}{N(P)^s}\right)^{-1}$$

$$= \left(1 - \frac{1}{5^s}\right)^{-1} \prod_{p \equiv 1 \bmod 5} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p \equiv 2,3 \bmod 5} \left(1 - \frac{1}{p^{4s}}\right)^{-1} \prod_{p \equiv 4 \bmod 5} \left(1 - \frac{1}{p^{2s}}\right)^{-2}$$

Dirichlet characters modulo 5:

	1	2	3	4
$\mathbf{1}$	1	1	1	1
χ	1	i	$-i$	-1
χ^2	1	-1	-1	1
χ^3	1	$-i$	i	-1

Claim:

$$\zeta_{\mathbb{Q}(\zeta_5)}(s) = \zeta(s)L(\chi, s)L(\chi^2, s)L(\chi^3, s)$$

The Euler factor at p for $p \neq 5$ is

$$\left(1 - \frac{1}{p^s}\right)\left(1 - \frac{\chi(p)}{p^s}\right)\left(1 - \frac{\chi^2(p)}{p^s}\right)\left(1 - \frac{\chi^3(p)}{p^s}\right)$$

If $p \equiv 1 \bmod 5$, this becomes

$$\left(1 - \frac{1}{p^s}\right)^4$$

If $p \equiv 2, 3 \bmod 5$, this becomes

$$\left(1 - \frac{1}{p^s}\right)\left(1 - \frac{i}{p^s}\right)\left(1 + \frac{i}{p^s}\right)\left(1 + \frac{1}{p^s}\right) = \left(1 - \frac{1}{p^{4s}}\right)$$

If $p \equiv 4 \bmod 5$, this becomes

$$\left(1 - \frac{1}{p^s}\right)\left(1 + \frac{1}{p^s}\right)\left(1 + \frac{1}{p^s}\right)\left(1 - \frac{1}{p^s}\right) = \left(1 - \frac{1}{p^{2s}}\right)^2$$

Analytic Phase:

$$\lim_{s \to 1^+} \zeta_{\mathbb{Q}(\zeta_5)}(s)(s-1) = \frac{2\pi^2}{5^2\sqrt{5}\log\left(\frac{1+\sqrt{5}}{2}\right)}h = L(\chi, 1)L(\chi^2, 1)L(\chi^3, 1)$$

In theory, you know how to break this up from the homework:

$$L(\chi, 1) = \frac{\pi}{5\sqrt{5}}(1 + 2i - 3i - 4) = \frac{\pi}{5\sqrt{5}}(-3 - i)$$

$$L(\chi^2, 1) = \frac{1}{\sqrt{5}} \log\left(\frac{1+\sqrt{5}}{2}\right)$$

(χ^2 is different because χ^2 is even (since $\chi^2(-1) = 1$), so we get a $\log$ instead of a π)

$$L(\chi^3, 1) = \frac{\pi}{5\sqrt{5}}(-3 + i)$$

Multiplying these all together, we can deduce that $h = 1$, so that $\mathbb{Z}[\zeta_5]$ has UPF.