Primes and Zeta Functions

PROMYS - Joshua Im

July 3 - August 10, 2023

Primes and Zeta Functions is a course that I took in summer 2023, in the summer program PROMYS by Prof. Li-Mei Lim. Even though the lecture went until August 10th, there are notes only up to August 2nd since I can't find my notes taken. Sections are divided by each week, and subsections are divided by each day of lecture. Problem sets were given every lecture, and listed after the subsections of each day. Problem sets should be ahead of lecture notes. Also, any problem given as a declarative statement should be taken as a PODASIP: Prove Or Disprove And Salvage If Possible. I thank Eamon Zhang and Jack Hsieh for helping me with taking notes.

1 Week 1

1.1 July 3, 2023

Definition 1.1: Squarefree

A natural number is **squarefree** if it has no perfect square factors other than 1.

So 21, 35, and 1 are squarefree, and 12 and 36 are not squarefree.

Question How many squarefree integers are less than 100?

Method We count the multiples of 4, 9, 25, ... Since there are

$$\left\lfloor \frac{99}{4} \right\rfloor \text{ multiples of } 4, \left\lfloor \frac{99}{9} \right\rfloor \text{ multiples of } 9,$$
$$\left\lfloor \frac{99}{25} \right\rfloor \text{ multiples of } 25, \left\lfloor \frac{99}{49} \right\rfloor \text{ multiples of } 49$$

we subtract them.

Remark

Note that we counted multiples of 36 twice: from multiples of 4 and multiples of 9.

Method

$$\text{Approximately } \frac{3}{4} \text{ of the numbers aren't divisible by 4.}$$
$$\text{Approximately } \frac{8}{9} \text{ of the numbers aren't divisible by 9.}$$
$$\text{Approximately } \frac{24}{25} \text{ of the numbers aren't divisible by 25.}$$
$$\dots$$

So approximately $99\left(\frac{3}{4}\right)\left(\frac{8}{9}\right)\left(\frac{24}{25}\right)\left(\frac{48}{49}\right) \approx 62.06$ numbers less than 100 are squarefree.

Problem Set 1

Numericals

Problem 1

Estimate the probability that a natural number less than 1000 is squarefree. What (approximately) is the probability that a natural number less than 2500 is square-free? Less than 5000? Less than 10000?

Problem 2

Consider integer lattice points in the first quadrant (not including lattice points on the x- and y-axes). Among lattice points with no coordinate greater than 100, how many have relatively prime coordinates? What if you allow coordinates up to 1000? Approximate the number of lattice points (a, b) with a, $b \in \mathbb{N}$ and $a \leq 10000$, $b \leq 10000$ such that $\gcd(a, b) = 1$.

Problem 3

Natural questions that arise from P1 and P2 could be: What is the probability that a random natural number is squarefree? What is the probability that a randomly chosen lattice point in the first quadrant (excluding lattice points on the axes) has relatively prime coordinates? Write down infinite sums and infinite products to represent these probabilities, and explain why these are the right expressions. Do you think these expressions have a value, and can you say approximately what they are?

Convergence

Let s_1, s_2, s_3, s_4, ... be a sequence of real numbers.

Definition 1.2: Convergence

A sequence $\{s_n\}$ **converges** to L if for every $\epsilon > 0$ there exists N such that $|s_n - L| < \epsilon$ for all $n > N$.

Problem 4

Let $s_n = r^n$ for some real number r. When does this sequence have a limit, and what is it in those cases?

Problem 5

Let $s_n = n^\alpha$ for some real number α. When does this sequence have a limit, and what is it in those cases?

Problem 6

Write down a definition of what it means for an infinite sum $\sum_{k=0}^{\infty} a_k$ to converge (have a value). Write down a definition of what it means for an infinite product $\prod_{k=0}^{\infty} a_k$ to converge. Give examples of infinite sums and products that *don't* converge.

Problem 7

The partial sum $\sum_{k=0}^{n} ar^k$ is equal to $\frac{a(1-r^{n+1})}{1-r}$, so a geometric series converges if and only if the common ratio r has absolute value less than 1. If the geometric series $\sum_{k=0}^{\infty} ar^k$ converges, it converges to $\frac{a}{1-r}$.

Miscellaneous

Problem 8

Consider the parabola $y = x^2$. Choose two arbitrary points on the parabola, $A = (a, a^2)$ and $B = (b, b^2)$, and let C be the point on the parabola that has x-coordinate halfway between the x-coordinates of A and B (so C has x-coordinate $\frac{a+b}{2}$). If D is the point on the parabola whose x-coordinate is halfway between the x-coordinates of A and C, then show that triangle ABC has 8 times the area of triangle ACD. By continuing this process, show that the area of the region bounded by the line segment AB and the parabola has $\frac{4}{3}$ the area of triangle ABC.

1.2 July 5, 2023

Question How many squarefree integers are less than N?

If we ignore the cross terms (ones that counted multiple times), we get

$$N\left(1-\frac{1}{2^2}-\frac{1}{3^2}-\frac{1}{5^2}-\cdots\right)=N\left(1-\sum_{p\text{ prime}}\frac{1}{p^2}\right)\approx 0.54N.$$

Lemma : Fundamental Theorem of Arithmetic

Every integer greater than 1 has a unique prime factorization.

Definition 1.3: Möbius Function

The **Möbius function** $\mu(n)$ is defined by

$$\mu(n)=\begin{cases}1 & \text{if } n \text{ is a squarefree positive integer with even prime factors}\\ -1 & \text{if } n \text{ is a squarefree positive integer with odd prime factors}\\ 0 & \text{if } n \text{ is not squarefree.}\end{cases}$$

If we do not ignore the cross terms, we get

$$\begin{aligned}N\Bigg(1&-\frac{1}{2^2}-\frac{1}{3^2}-\frac{1}{5^2}-\cdots\\ &+\frac{1}{2^2\cdot 3^2}+\frac{1}{2^2\cdot 5^2}+\cdots\\ &-\frac{1}{2^2\cdot 3^2\cdot 5^2}-\cdots=\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{5^2}\right)\cdots\end{aligned}$$

because we have unique prime factorization. In this way, we can express an infinite sum as an infinite product.

Remark

The infinite sum can also be expressed as

$$1-\frac{1}{2^2}-\frac{1}{3^2}-\frac{1}{5^2}-\cdots=\sum_{n=0}^{\infty}\frac{\mu(n)}{n^2}.$$

Problem Set 2

Infintie Sums and Products

Problem 1

If $\sum_{k=0}^{\infty} a_k$ is a convergent sum with positive terms, and if $0 < b_k \leq a_k$ for all k, then $\sum_{k=0}^{\infty} b_k$ converges.

Problem 2

If $\sum_{k=0}^{\infty} a_k$ is a divergent sum with positive terms, and if $0 < a_k \leq b_k$ for all k, then $\sum_{k=0}^{\infty} b_k$ diverges.

Problem 3

The series $\sum_{k=0}^{\infty} \frac{1}{k}$ diverges.

Problem 4

The series $\sum_{k=0}^{\infty} \frac{1}{k^s}$ converges if and only if $s > 1$.

Problem 5

The series $\sum_{k=0}^{\infty} \frac{1}{k^s}$ is equal to the infinite product $\prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}$, where the product runs over all positive primes.

Numericals

Problem 6

Using a calculator or computer program, compute $\sum_{k=1}^{n} \frac{1}{k^2}$ for several values of n. Estimate $\sum_{k=1}^{\infty} \frac{1}{k^2}$. Compare your estimate from P5 to your estimates from P3 in Pset 1. Try multiplying them.

Problem 7

Compute some partial products for the infinite product $\prod_{k=1}^{\infty} \frac{2k}{2k-1} \cdot \frac{2k}{2k+1} = \frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \cdots$.

Problem 8

Use a graphing calculator or computational software, compare the graphs of $\sin x$ to the product expression and series expression (using partial products and sums as approximations):

$$\sin x = x \cdot \prod_{k=1}^{\infty} \left(1 - \frac{x^2}{k^2\pi^2}\right)$$

Series Expressions for Functions

Problem 9

If a function $f(x)$ "is" an infinite polynomial $\sum_{k=0}^{\infty} c_k x^k$, then the coefficients c_k satisfy

$$c_k = \frac{f^{(k)}(0)}{k!}.$$

Here, $f^{(k)}(0)$ is the k-th derivative of f evaluated at 0. Note that we say $0! = 1$, following the convention that empty products should be 1.

Problem 10

$\sin x = \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k+1}}{(2k+1)!}$, Compare the graph of $\sin x$ with partial sums of this series.

Problem 11

$\log(1-x) = -\sum_{k=0}^{\infty} \frac{x^k}{k}$. (Note: here log is the natural log, sometimes also written ln.) Compare the graph of $\log(1-x)$ to partial sums of this series.

1.3 July 6, 2023

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p^2}\right)^{-1} = \prod_{p \text{ prime}}$$

$$= \prod_{p \text{ prime}} \left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots\right)$$

$$= \left(1 + \frac{1}{2^2} + \frac{1}{2^4} + \cdots\right)\left(1 + \frac{1}{3^2} + \frac{1}{3^4} + \cdots\right)\left(1 + \frac{1}{5^2} + \frac{1}{5^4} + \cdots\right)\cdots$$

$$= 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^2}.$$

Definition 1.4: Riemann-Zeta Function

The **Riemann-Zeta function** is defined as

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

So $\displaystyle\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)}$.

Theorem 1.1: Basel Problem

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

We first define the power series, which is the fundamental part in the proof.

Definition 1.5: Taylor Series

The **Taylor series** of a function $f(x)$ is

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n = f(0) + f'(0)x + \frac{f''(0)}{2!} x^2 + \cdots.$$

Then this polynomial equals to $f(x)$.

Proof. We compute $\zeta(2)$ by approximating $\sin x$ as polynomials.

Then, the Taylor series of $\sin x$ is

$$\sin x = \sum_{n=0}^{\infty} \frac{(-1)^k}{(2k+1)!} x^{2k+1} = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots.$$

We have another way to find a polynomial expression of $\sin x$. Since the roots of $\sin x$ are $\cdots$, -2π, $-\pi$, 0, π, 2π, $\cdots$, we can express $\sin x$ as

$$\sin x = ax(x-\pi)(x+\pi)(x-2\pi)(x+2\pi)\cdots.$$

From the identity $\lim_{x\to\infty} \frac{\sin x}{x} = 1$, we can find a, and

$$\begin{aligned}\sin x &= x\left(1+\frac{x}{\pi}\right)\left(1-\frac{x}{\pi}\right)\left(1+\frac{x}{2\pi}\right)\left(1-\frac{x}{2\pi}\right)\cdots \\ &= x\left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{4\pi^2}\right)\left(1-\frac{x^2}{9\pi^2}\right)\cdots.\end{aligned}$$

Therefore, we get

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots = x\left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{4\pi^2}\right)\left(1-\frac{x^2}{9\pi^2}\right)\cdots.$$

If we compare the coefficients of x^3, we get

$$-\frac{1}{3!} = -\frac{1}{\pi^2} - \frac{1}{4\pi^2} - \frac{1}{9\pi^2} = -\frac{1}{\pi^2}\left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots\right)$$

So

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}.$$

■

Problem Set 3

Numericals

Problem 1

Make two lists of primes: the primes that are 1 mod 4 and the primes that are 3 mod 4 (up to 50, 100, 150, higher?). Prove that there are infinitely many primes that are 1 mod 4, and that there are infinitely many primes that are 3 mod 4.

Problem 2

Repeat P1, but with 1 mod 3 and 2 mod 3. Any conjectures?

Special Values

Problem 3

Evaluate $\sum_{n=0}^{\infty} \frac{1}{(2n+1)^2} = 1 + \frac{1}{9} + \frac{1}{25} + \frac{1}{49} + \frac{1}{81} + \cdots$.

Problem 4

Evaluate $\zeta(4) = \sum_{n=1}^{\infty} \frac{1}{n^4}$.

Problem 5

Evaluate $\zeta(6) = \sum_{n=1}^{\infty} \frac{1}{n^6}$.

Miscellaneous

Problem 6

Prove that $\frac{\pi}{2} = \prod_{k=1}^{\infty} \frac{2k}{2k-1} \cdot \frac{2k}{2k+1} = \frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdots\cdots$. (Note: If you want to avoid Euler's product formula for sine, use integration by parts to evaluate $\int_0^{\pi/2} \sin^n x \, dx$. You may find that n even and n odd should be treated separately.)

Problem 7

Prove that $\zeta(2) = \frac{\pi^2}{6}$ in another way. One suggestion: First, find an expression for $\arcsin x$ as an infinite (polynomial) series $\arcsin x = \sum_{k=0}^{\infty} c_k x^k$. Setting $x = \sin t$, get a series for t in terms of powers of $\sin t$. Integrate from 0 to $\pi/2$.

2 Week 2

2.1 July 10, 2023

Let $\{a_n\}$ be a sequence. We define a new sequence $\{S_n\}$ by the partial sums, so $S_n = \sum_{i=1}^{n} a_i$. Then, the infinite series $\sum_{i=1}^{\infty}$ converges if the sequence $\{S_n\}$ converges.

Example 1

Consider the geometric series $a_i = 1/2^{i-1}$. Let S_n be the partial sum, so

$$S_n = 1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^{n-1}} = 2 - \frac{1}{2^{n-1}}.$$

We claim the series converges to 2.

Proof. For any $\epsilon > 0$, we claim that there exists N such that $\frac{1}{2^{n-1}} < \epsilon$ if $n > N$. Then, we need $2^{n-1} > \frac{1}{\epsilon}$. This implies $n > \log_2\left(\frac{1}{\epsilon}\right) + 1$, so set $N = \left\lceil \log_2\left(\frac{1}{\epsilon}\right)\right\rceil$. ■

Theorem 2.1: Convergence of the Geometric Series

The geometric series

$$a + ar + ar^2 + \cdots = \sum_{n=0}^{\infty} ar^n$$

converges to $\frac{a}{1-r}$ if and only if $|r| < 1$.

We now move on: when does $\zeta(s)$ converges? For instance,

$$\zeta(0) = \frac{1}{1^0} + \frac{1}{2^0} + \frac{1}{3^0} + \cdots = 1 + 1 + 1 + \cdots$$

diverges, and

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

also diverges.

We first prove that the harmonic series diverges.

Lemma : Divergence of the Harmonic Series

The harmonic series

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots$$

diverges.

Proof. We see that

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{1}{n} &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots \\
&= 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots \\
&\geq 1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \cdots \\
&= 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots .
\end{aligned}$$

So for any M, eventually all partial sums will exceed M, therefore the series diverges. ∎

Theorem 2.2: Convergence of the Riemann-Zeta Function

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

converges for $s > 1$.

Proof.

$$\begin{aligned}
\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s} &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots \\
&= 1 + \left(\frac{1}{2^s} + \frac{1}{3^s}\right) + \left(\frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s}\right) + \cdots \\
&\leq 1 + \left(\frac{1}{2^s} + \frac{1}{2^s}\right) + \left(\frac{1}{4^s} + \frac{1}{4^s} + \frac{1}{4^s} + \frac{1}{4^s}\right) + \cdots \\
&= 1 + 2 \cdot \frac{1}{2^s} + 4 \cdot \frac{1}{4^s} + \cdots \\
&= 1 + 2^{1-s} + 4^{1-s} + \cdots ,
\end{aligned}$$

so $\zeta(s)$ is bounded above by is a geometric series. Since the geometric series converges for $2^{1-s} < 1$, we get that

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

converges for $s > 1$. ■

Problem Set 4

Some Special Functions

Problem 1

Characterize all primes that are $a \bmod m$, where $\gcd(a, m) > 1$.

Problem 2

Consider a function $f : \mathbb{Z}_4 \to \mathbb{C}$. If f satisfies $f(ab) = f(a)f(b)$, then what could f possibly be? What if we add the condition that $f(a) = 0$ if a is not a unit in $\mathbb{Z}_4$?

Problem 3

How would P1 change if $\mathbb{Z}_4$ were replaced with $\mathbb{Z}_p$? $\mathbb{Z}_m$?

Problem 4

How many functions $f : \mathbb{Z}_m \to \mathbb{C}$ are there that satisfy $f(ab) = f(a)f(b)$ and $f(a) = 0$ is $a \notin U_m$?

Bounds for $\zeta(s)$

Problem 5

By inducting on N, show that, for $s > 1$,

$$\frac{1}{s-1} - \frac{1}{(s-1)(N+1)^{s-1}} \leq \sum_{n=1}^{N} \frac{1}{n^s} \leq 1 + \frac{1}{s-1} - \frac{1}{(s-1)N^{s-1}}.$$

You may find the following inequality useful:

$$(1+x)^{\alpha} \geq 1 + \frac{\alpha x}{1+x} \text{ if } x > -1 \text{ and } \alpha > 0.$$

Problem 6

Prove the inequality given above. (It may be easier to prove that $(1+x)^{\alpha} \geq 1 + \alpha x$ for $\alpha > 1$ and $x > -1$ first.)

Problem 7

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

Miscellaneous

Problem 8

For any $N \in \mathbb{N}$, there exist consecutive primes p and q that are at least N apart. (That is, there are at least N composite natural numbers in a row.)

2.2 July 12, 2023

The fact that $\sum_{n=1}^{\infty}\frac{1}{n}$ diverges could be interpreted as

"There are a lot of natural numbers."

We now look for subsets S of $\mathbb{N}$ and $\sum_{n\in S}\frac{1}{n}$, so we can decide how 'big' S is.

Example 2

If $S = \{n^2 \,|\, n \in \mathbb{N}\}$, then

$$\sum_{n\in S}\frac{1}{n} = \sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$$

converges.

Example 3

If $S = \{2^n \,|\, n \in \mathbb{N}\}$, then

$$\sum_{n\in S}\frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{4} + \cdots = 2$$

converges.

Example 4

If $S = \{2n \,|\, n \in \mathbb{N}\}$, then

$$\sum_{n\in S}\frac{1}{n} = \frac{1}{2}\sum_{n=1}^{\infty}\frac{1}{n}$$

diverges.

Example 5

If $S = \{\text{Squarefree numbers}\}$, does $\sum_{n \in S} \frac{1}{n}$ converges or diverges?

Solution Notice that

$$\sum_{n \in S} \frac{1}{n} = \prod_{p \text{ prime}} \left(1 + \frac{1}{p}\right) = \left(1 + \frac{1}{2}\right)\left(1 + \frac{1}{3}\right)\left(1 + \frac{1}{5}\right) \cdots$$

Then,

$$\begin{aligned}
\zeta(2) \sum_{n \in S} \frac{1}{n} &= \prod_{p \text{ prime}} \left(1 - \frac{1}{p^2}\right)^{-1} \left(1 + \frac{1}{p}\right) \\
&= \frac{1}{1 - \frac{1}{p}} \\
&= \sum_{n=1}^{\infty} = \zeta(1).
\end{aligned}$$

So

$$\sum_{n \in S} \frac{1}{n} = \frac{\zeta(1}{\zeta(2)} = \frac{6}{\pi^2} \zeta(1),$$

diverges.

Problem Set 5

Convergence of Infinite Sums and Products

Problem 1

If $\sum a_n$ and $\sum b_n$ are series with positive terms such that

$$\lim_{n \to \infty} \frac{a_n}{b_n} = c$$

where $0 < c < \infty$, then either both series converge of both series diverge. Explain this intuitively before getting ϵ involved.

Problem 2

Let $\sum a_n$ be a series with positive terms. Then $\sum a_n$ converges if and only if $\prod (1 + a_n)$ converges.

Problem 3

If $c_n \geq 0$ and $c_n \neq 1$ for all n, and if $\sum c_n$ converges, then $\prod \frac{1}{1-c_n}$ converges, and the product can be expanded and rearranged in the "natural way" where each factor in the product is written as a geometric series.

Dirichlet Density

Definition 2.1: Dirichlet Density

We define the **Dirichlet density** of a set of primes P to be

$$d(P) = \lim_{s \to 1^+} \frac{\sum_{p \in P} p^{-s}}{\log(s-1)^{-1}}.$$

Problem 4

The set of all primes has Dirichlet density 1.

Problem 5

If P is a set that contains all but finitely many primes, then $d(P) = 1$.

Problem 6

A finite set of primes has Dirichlet density 0.

Problem 7

If P_1 and P_2 are two disjoint sets of primes,then $d(P_1 \cup P_2) = d(P_1) + d(P_2)$.

Miscellaneous

Problem 8

Another natural way to define the density of a set of primes P could be:

$$D(P) = \lim_{X \to \infty} \frac{\#\{p \in P \,|\, p < X\}}{\pi(X)},$$

where $\pi(X)$ is the number of primes less than X. The set of primes with first (decimal) digit 1 does not have a density in this sense, but does have a Dirichlet density.

2.3 July 13, 2023

Problem Set 6

Dirichlet Characters and L-functions

Definition 2.2: Dirichlet Character

A **DIrichlet chatacter mod m** is a function $\chi : U_m \to \mathbb{C}$ that satisfies $\chi(ab) = \chi(a)\chi(b)$.

We extend χ to all of $\mathbb{Z}$ using periodicity (i.e. $\chi(a+m) = \chi(a)$) and by defining $\chi(a) = 0$ is $\gcd(a, m) \neq 1$.

Problem 1

Dirichlet characters are totally multiplicative. That is, $\chi(ab) = \chi(a)\chi(b)$ for all a, $b \in \mathbb{Z}$.

Problem 2

For each Dirichlet character χ mod 4, compute

$$\sum_{a=0}^{3} \chi(a).$$

Problem 3

In general, what is the sum

$$\sum_{a=0}^{m-1} \chi(a)$$

where χ is a Dirichlet character mod m?

Problem 4

If you fix an integer and vary the characters instead, what happens to the sum? That is, if you let S be the set of Dirichlet characters mod 4 (for example), compute

$$\sum_{\chi \in S} \chi(a).$$

Problem 5

If $a_1, a_2, a_3, \ldots,$ is a totally multiplicative sequence (that is, $a_{mn} = a_m a_n$ for all m and n in $\mathbb{N}$), and if $|a_n| \leq 1$ for all n, then

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s}}$$

for $s > 1$, and both the sum and product can be rearranged.

Problem 6

If χ is the Dirichlet character mod 4 with $\chi(3) = -1$, we define

$$L(s, \chi) = \sum_{n=0}^{\infty} \frac{\chi(n)}{n^s}.$$

This converges for $s > 1$ and has an Euler product.

Problem 7

Using $\zeta(s)$, $L(s, \chi)$,and logarithms of these functions, find an expression that is approximately

$$\sum_{p \equiv 1 \mod 4} \frac{1}{p^s}.$$

What is the error between your expression and this sum? What about the sum over primes that are 3 mod 4 instead of 1 mod 4?

3 Week 3

3.1 July 17, 2023

Example 6

If $S = \{\text{Prime numbers}\}$, does $\sum_{n \in S} \frac{1}{n}$ converges or diverges?

Solution We saw that

$$\zeta(s) = \sum_{n \in \mathbb{N}} \frac{1}{n^s} = \prod_{p \,\text{prime}} \left(1 - \frac{1}{p^s}\right)^{-1},$$

and

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

if $|x| < 1$. Then,

$$\begin{aligned}
\log \zeta(s) &= \log \sum_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1} \\
&= -\log \sum_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right) \\
&= \sum_{p \text{ prime}} \left(\frac{1}{p^s} + \frac{1}{2p^{2s}} + \frac{1}{3p^{3s}} + \cdots\right) \\
&= \sum_{p \text{ prime}} \frac{1}{p^s} + \sum_{p \text{ prime}} \sum_{n \geq 2} \frac{1}{np^{ns}}
\end{aligned}$$

We claim that $\displaystyle\sum_{p \text{ prime}} \sum_{n \geq 2} \frac{1}{np^n}$ is bounded above by $\dfrac{\pi^2}{6}$. Since

$$\begin{aligned}
\sum_{p \text{ prime}} \sum_{n \geq 2} \frac{1}{np^n} &= \sum_{p \text{ prime}} \frac{1}{2p^2} + \frac{1}{3p^3} + \frac{1}{4p^4} + \cdots \\
&\leq \sum_{p \text{ prime}} \frac{1}{p^2} + \frac{1}{p^3} + \frac{1}{p^4} + \cdots \\
&= \sum_{p \text{ prime}} \frac{1}{p^2}\left(\frac{1}{1 - \frac{1}{p}}\right) \\
&\leq \sum_{p \text{ prime}} \frac{1}{(p-1)^2} < \sum_{n \in \mathbb{N}} \frac{1}{n^2},
\end{aligned}$$

$\displaystyle\sum_{p \text{ prime}} \sum_{n \geq 2} \frac{1}{np^n}$ is bounded above by $\dfrac{\pi^2}{6}$. We also see that this is bounded below by 0. Therefore,

$$\begin{aligned}
\sum_{p \text{ prime}} \frac{1}{p} &= \lim_{s \to 1^+} \sum_{p \text{ prime}} \frac{1}{p^s} \\
&= \lim_{s \to 1^+} \log \zeta(s) - \sum_{p \text{ prime}} \sum_{n \geq 2} \frac{1}{np^n} \\
&> \lim_{s \to 1^+} \log \zeta(s) - \frac{\pi^2}{6}
\end{aligned}$$

diverges because $\log \zeta(1)$ diverges.

Lemma : Fermat

If $p \mid x^2 + 1$ and p is prime, then p is either 2 or 1 mod 4.

Theorem 3.1: Infinite Primes of 1 mod 4

There are infinitely many primes that are 1 mod 4.

Proof. Suppose there are finitely many primes of the form 1 mod 4, $p_1, p_2, \ldots, p_k$. Let $p = p_1 p_2 \cdots p_k$. Then we can generate a new prime by $4p^2 + 1$.

Consider a prime p_i such that $p_i \mid 4p^2 + 1$. Since $4p^2 + 1$ is odd, p_i cannot be even, hence p_i is 1 mod 4. Then, $p_i \mid p$ because p is the product of all 1 mod 4 primes. Then, $p_i \mid 4p^2 + 1 - 4p^2 = 1$, which is a contradiction. Therefore, there are infinitely many 1 mod 4 primes. ■

Problem Set 7

Dirichlet Characters and L-functions

Problem 1

Let $\chi(n)$ be the Dirichlet character mod 3 with

$$\chi(n) = \begin{cases} 1 & \text{if } n \equiv 1 \mod 3 \\ -1 & \text{if } n \equiv 2 \mod 3 \\ 0 & \text{if } 3 \mid n \end{cases}$$

Then $L(s, \chi) = \displaystyle\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges for $s > 0$ and is equal to $\displaystyle\prod_p \frac{1}{1 - \chi(p)p^{-s}}$ when $s > 1$.

Problem 2

With $L(s, \chi)$ as in P1, $L(1, \chi)$ converges. Do some numericals to see if you can guess what the sum is.

Problem 3

With $L(s, \chi)$ as in P1, what is $L(2, \chi)$?

Problem 4

Using $L(s, \chi)$, show that there are infinitely many primes that are 1 mod 3, and infinitely many primes that are 2 mod 3.

Other Primes and Zeta Functions

For a Gaussian integer $\alpha = a + bi$, we defined the norm to be $N\alpha = a^2 + b^2$.

Problem 5

If $\alpha \neq 0$, $N\alpha = \#\mathbb{Z}[i]_\alpha$. (Notice the analogy with $|n| = \#\mathbb{Z}_n$ for integers n.)

Problem 6

Let $K = \mathbb{Z}[i]$, and define the zeta function

$$\zeta_K(s) = \prod_{(\pi)} \frac{1}{1 - N\pi^{-s}}$$

where the product is taken over nonassociative irreducible elements of $\mathbb{Z}[i]$. For example, only one of $1 + 2i$, $-2 + i$, $-1 - 2i$, and $2 - i$ contribute to the product. Then $\zeta_K(s)$ converges for $s > 1$ and

$$\zeta_K(s) = \sum_{(\alpha)} \frac{1}{N\alpha^s}$$

where the summation is over nonassociative elements of $\mathbb{Z}[i]$.

Problem 7

If $L(s, \chi) = \displaystyle\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ where χ is the Dirichlet character mod 4 with

$$\chi(n) = \begin{cases} 1 & n \equiv 1 \mod 4 \\ -1 & n \equiv 3 \mod 4 \\ 0 & \text{otherwise} \end{cases}$$

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

Problem 8

Use $\zeta_K(s)$ to show that $\mathbb{Z}[i]$ has infinitely many irreducible elements.

3.2 July 19, 2023

Definition 3.1: Dirichlet Character mod 4

The **Dirichlet Character mod 4** $\chi(n)$ is defined as

$$\chi(n) = \begin{cases} 1 & n \equiv 1 \mod 4 \\ -1 & n \equiv 3 \mod 4 \\ 0 & \text{otherwise.} \end{cases}$$

The Dirichlet character satisfies $\chi(mn) = \chi(m)\chi(n)$.

Definition 3.2: Dirichlet L-function

We define **Dirichlet L-function** as

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

Example 7

Does the alternating series $L(s, \chi) = \frac{1}{1^s} - \frac{1}{3^s} + \frac{1}{5^s} - \cdots$ converges or diverges?

Solution Use the alternating series test. Since the sequence $1/1^s$, $1/3^s$, $1/5^s$, $\cdots$ is decreasing if $s > 0$, and $\lim_{n\to\infty} \frac{1}{n^s} = 0$, the alternating series converges.

Example 8

Let $\chi_0(n) = \begin{cases} 1 & 2 \nmid n \\ 0 & 2 \mid n. \end{cases}$ Does $L(s, \chi_0) = \frac{1}{1^s} + \frac{1}{3^s} + \frac{1}{5^s} + \cdots$ converges or diverges?

Solution We see that

$$\begin{aligned} L(s, \chi_0) &= \frac{1}{1^s} + \frac{1}{3^s} + \frac{1}{5^s} + \cdots \\ \frac{1}{2^s} L(s, \chi_0) &= \frac{1}{2^s} + \frac{1}{6^s} + \frac{1}{10^s} + \cdots \\ \frac{1}{4^s} L(s, \chi_0) &= \frac{1}{4^s} + \frac{1}{12^s} + \frac{1}{20^s} + \cdots. \end{aligned}$$

Therefore,

$$\left(1 + \frac{1}{2^s} + \frac{1}{4^s} + \cdots\right) L(s, \chi_0) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \zeta(s).$$

So since $\left(1-\frac{1}{2^s}\right)^{-1} L(s,\chi_0) = \zeta(s)$, $\lim_{s\to 1^+} L(s,\chi_0)$ diverges.

Remark

Even though the alternating series $L(s,\chi) = 1/1^s - 1/3^s + 1/5^s - \cdots$ converges, $L(s,\chi_0) = 1/1^s + 1/3^s + 1/5^s + \cdots$ diverges. this implies that the convergence of the alternating series doesn't say that the series converges absolutely.

Question Does $\displaystyle\sum_{\substack{p\equiv 1 \mod 4 \\ p \text{ prime}}} \frac{1}{p}$ and $\displaystyle\sum_{\substack{p\equiv 3 \mod 4 \\ p \text{ prime}}} \frac{1}{p}$ converge or diverge?

Theorem 3.2

$\displaystyle\sum_{\substack{p\equiv 1 \mod 4 \\ p \text{ prime}}} \frac{1}{p^s}$ converges if and only if $s > 1$.

It is easy to prove that $\displaystyle\sum_{\substack{p\equiv 1 \mod 4 \\ p \text{ prime}}} \frac{1}{p^s}$ converges when $s > 1$ because it is smaller than $\zeta(s)$. We only prove that $\displaystyle\sum_{\substack{p\equiv 1 \mod 4 \\ p \text{ prime}}} \frac{1}{p}$ diverges.

Proof.

$$\begin{aligned}
\log L(1,\chi) &= \sum_{p \text{ prime}} \log\left(1 - \frac{\chi(p)}{p}\right)^{-1} \\
&= \sum_{p \text{ prime}} \left(\frac{\chi(p)}{p} + \frac{\chi(p^2)}{2p^2} + \frac{\chi(p^3)}{3p^3} + \cdots\right. \\
&= \sum_{p \text{ prime}} \frac{\chi(p)}{p^s} + \sum_{p \text{ prime}} \sum_{n\geq 2} \frac{\chi(p^n)}{np^n}
\end{aligned}$$

We see that

$$-\sum_{p \text{ prime}} \sum_{n\geq 2} \frac{1}{np^n} < \sum_{p \text{ prime}} \sum_{n\geq 2} \frac{\chi(p^n)}{np^n} < \sum_{p \text{ prime}} \sum_{n\geq 2} \frac{1}{np^n},$$

so $\sum_{p \text{ prime}} \sum_{n \geq 2} \frac{\chi(p^n)}{np^n}$ is bounded by $-\frac{\pi^2}{6}$ and $\frac{\pi^2}{6}$. Then

$$\begin{aligned}
\lim_{s \to 1^+} \log \zeta(s) + \log L(1, \chi) &= \sum_{p \text{ prime}} \frac{1}{p} + \left(\text{stuff bounded by } 0 \text{ and } \frac{\pi^2}{6}\right) \\
&\quad + \sum_{p \text{ prime}} \frac{\chi(p)}{p} + \left(\text{stuff bounded by } -\frac{\pi^2}{6} \text{ and } \frac{\pi^2}{6}\right) \\
&= \frac{1}{2} + 2 \sum_{\substack{p \equiv 1 \bmod 4 \\ p \text{ prime}}} \frac{1}{p} + (\text{bounded stuff})
\end{aligned}$$

Since the left-hand side diverges, the right side should also diverge, which implies that $\sum_{\substack{p \equiv 1 \bmod 4 \\ p \text{ prime}}} \frac{1}{p}$ diverges. ■

Similarly, we can find that

$$\log \zeta(s) - \log L(s, \chi) = 2 \sum_{\substack{p \equiv 3 \bmod 4 \\ p \text{ prime}}} \frac{1}{p^s} + (\text{bounded stuff}),$$

so $\sum_{\substack{p \equiv 3 \bmod 4 \\ p \text{ prime}}} \frac{1}{p}$ diverges.

Theorem 3.3

$\sum_{\substack{p \equiv 3 \bmod 4 \\ p \text{ prime}}} \frac{1}{p^s}$ converges if and only if $s > 1$.

Problem Set 8

Dirichlet Characters and L-functions

Problem 1

Let $p = 5$. Write down a table of all the Dirichlet characters mod p with their values on each congruence class mod 5.

Problem 2

How many Dirichlet characters are there mod 5? Can you generalize?

Problem 3

Use your table to compute $\sum_{\chi} \chi(a)\overline{\chi(b)}$ for fixed a and b. Also compute $\sum_{a=0}^{4} \chi_i(a)\overline{\chi_j(a)}$ for a fixed pair of characters χ_i and χ_j. Any conjectures?

Problem 4

Using Dirichlet characters, zeta functions, and logarithms thereof, can you find an expression that is close to $\sum_{p \equiv 1 \bmod 5} \frac{1}{p^s}$? What is the error between your expression and this sum?

Other Primes and Zeta Functions

Let $\zeta_K(s)$ be the zeta function for $\mathbb{Z}[i]$ defined in Pset 7:

$$\zeta_K(s) = \prod_{(\pi)} \frac{1}{1 - N\pi^{-s}}$$

where the product is taken over nonassociative irreducible elements of $\mathbb{Z}[i]$. Recall that

$$\zeta_K(s) = \sum_{(\alpha)} \frac{1}{N\alpha^s}$$

where the summation is over nonassociative elements of $\mathbb{Z}[i]$. (This converges for $s > 1$.)

Problem 5

What proportion of elements of $\mathbb{Z}[i]$ are squarefree?

Problem 6

What is the probability that two randomly chosen Gaussian integers are relatively prime?

3.3 July 20, 2023

Example 9

Find the value of $\sum_{n=0}^{\infty}(-1)^n \frac{1}{2n+1} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots$.

Solution Let $f(x) = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \cdots$. Then $f(1) = L(1, \chi)$. If we take the derivative of $f(x)$,

$$\begin{aligned} f'(x) &= 1 - x^2 + x^4 - x^6 + \cdots \\ &= \frac{1}{1+x^2} \end{aligned}$$

Since $f'(x) = 1/(1+x^2)$, $f(x) = \arctan x + C$ for some constant C. To find C, substitute $x = 0$, and you get $\arctan 0 + C = C = 0$, so $C = 0$, and $f(x) = \arctan x$. Therefore,

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = f(1) = \arctan 1 = \frac{\pi}{4}.$$

Problem Set 9

Primes in Congruence Classes

Recall from Pset 5 that the Dirichlet density of a set of primes P is defined to be:

$$d(P) = \lim_{s \to 1^+} \frac{\sum_{p \in P} p^{-s}}{\log(s-1)^{-1}}.$$

Problem 1

The Dirichlet density of primes that are 1 mod 4 is 1/2. The Dirichlet density of primes that are 3 mod 4 is also 1/2.

Problem 2

The Dirichlet density of primes that are 1 mod 3 is 1/2. The Dirichlet density of primes that are 2 mod 3 is also 1/2.

Problem 3

There are infinitely many primes that are a mod m, and the Dirichlet density of such primes is $1/\varphi(m)$.

Dirichlet L-functions at $s = 1$

Problem 4

Consider

$$F(s) = \prod_{\chi \bmod 5} L(s, \chi)$$

where the product is taken over Dirichlet characters mod 5. Then $F(s) \geq 1$ for $s > 1$.

Problem 5

If χ is a Dirichlet character mod 5 that takes complex values, then $L(1, \chi) \neq 0$.

4 Week 4

4.1 July 24, 2023

Problem Set 10

Beyond $s > 1$

Problem 1

Define

$$\zeta_2(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}.$$

Then $\zeta_2(s)$ converges for $s > 0$ and when $s > 1$, $\zeta_2(s) = (1 - 2^{1-s})\zeta(s)$. Thus, using $\zeta_2(s)$, we have a way to extend the definition of $\zeta(s)$ to $s > 0$.

Problem 2

For any natural number $m \geq 2$, define

$$\zeta_m(s) = 1 + \frac{1}{2^s} + \cdots + \frac{1}{(m-1)^s} - \frac{m-1}{m^s} + \cdots = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where $a_n = 1$ for $n \not\equiv 0 \bmod m$ and $a_n = -(m-1)$ for $n \equiv 0 \bmod m$. Then $\zeta_m(s) = (1 - m^{1-s})\zeta(s)$ when $s > 1$, and we can extend the definition of $\zeta(s)$ to $s > 0$ using the formula

$$\zeta(s) = \frac{\zeta_m(s)}{(1 - m^{1-s})}.$$

This ration does not depend on the choice of m, so using different values of m will not change the extended definition of $\zeta(s)$.

Problem 3

$\zeta(s) < 0$ for $0 < s < 1$.

Dirichlet L-functions at $s = 1$

Definition 4.1: Gauss Sum

Define the **Gauss sum** mod a prime p to be:

$$g_p = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \omega^a$$

where $(\frac{a}{p})$ is the usual Legendre symbol and $\omega = e^{2\pi i/p}$ is a p-th root of unity.

Problem 4

Evaluate g_p for various primes p.

Problem 5

If $L(s, \chi)$ is the Dirichlet L-function with Dirichlet character equal to the Legendre symbol, and g_p and ω are defined as above, then

$$\frac{\prod_r (1 - \omega^r)}{\prod_n (1 - \omega^n)} = e^{g_p L(1,\chi)},$$

where the product over r is the product over all quadratic residues mod p and the product over n is the product over all quadratic nonresidues mod p.

Problem 6

Use the previous problem to compute $L(1, \chi)$ for $p = 5$ and χ the Dirichlet character that is equal to the Legendre symbol.

4.2 July 26, 2023

We will now prove the generalization of this sums.

Theorem 4.1: Dirichlet's Theorem on Primes in Arithmetic Progressions

If $\gcd(a, m) = 1$, then there are infinitely many primes that are a mod m.

We look for ideas to prove this theorem. The idea is to use Dirichlet characters and think about $L(s, \chi) = \sum_n \frac{\chi(n)}{n}$. We can use logs, and add/subtract combinations of these to pick out a mod m primes.

Question How should we isolate the a mod m congruence class using characters?

Recall that the Dirichlet character mod m is a function $\chi : U_m \to \mathbb{C}$ that is multiplicative and nonzero. We extend this to $\mathbb{Z}$ by setting $\chi(a) = 0$ if $\gcd(a, m) \neq 1$.

We now prove some conjectures that may be helpful to prove the theorem.

Claim

The set of Dirichlet characters mod m forms a group with the operation $*$ such that $(\chi_1 * \chi_2)(a) = \chi_1(a)\chi_2(a)$.

Proof. Note that $*$ is a binary operation on the set of Dirichlet characters. Let $\mathbb{D}_m$ be the set of Dirichlet characters mod m. We first prove that $\chi_1 * \chi_2$ is a Dirichlet character.

$$\begin{aligned}(\chi_1 * \chi_2)(ab) &= \chi_1(ab)\chi_2(ab)\\ &= \chi_1(a)\chi_1(b)\chi_2(a)\chi_2(b)\\ &= \chi_1(a)\chi_2(a)\chi_1(b)\chi_2(b)\\ &= (\chi_1 * \chi_2)(a) \cdot (\chi_1 * \chi_2)(b),\end{aligned}$$

so $\chi_1 * \chi_2$ is also a Dirichlet character. Associativity is inherited from the associativity of multiplication in $\mathbb{C}$. The identity element is χ_e such that

$$\chi_e(a) = \begin{cases} 1 & \gcd(a, m) = 1 \\ 0 & \gcd(a, m) \neq 1. \end{cases}$$

For inverses, if $\chi \in \mathbb{D}_m$, define χ^{-1} as

$$\chi^{-1}(a) = \begin{cases} \chi(a)^{-1} & \chi(a) \neq 0 \\ 0 & \chi(a) = 0. \end{cases}$$

To prove that χ^{-1} is actually a Dirichlet character, we need to prove that $\chi^{-1}(ab) = \chi^{-1}(a)\chi^{-1}(b)$.

If $\gcd(ab, m) \neq 1$, then $\chi(ab) = 0$, and $\chi^{-1}(ab) = 0$. If $\gcd(ab, m) = 1$, then since $\chi(ab) \neq 0$,

$$\begin{aligned}\chi^{-1}(ab) &= \chi(ab)^{-1}\\ &= \chi(b)^{-1}\chi(a)^{-1}\\ &= \chi(a)^{-1}\chi(b)^{-1} && (\chi \text{ is commutative})\\ &= \chi^{-1}(a)\chi^{-1}(b),\end{aligned}$$

χ^{-1} is multiplicative, and it is a Dirichlet character. Therefore, $\mathbb{D}_m$ is a group. ■

Problem Set 11

Good Ideas Revived

Problem 1

If $\sum_{n=1}^{\infty} a_n$ converges, then for any real number $r > 0$, there exists $N \in \mathbb{N}$ such that $\left| \sum_{n=N}^{\infty} a_n \right| < r$.

Problem 2

Consider the following argument that $\sum \frac{1}{p}$ diverges. Assume it converges, and consider

$$\left(\sum_{p<N} \frac{1}{p} \right)^k .$$

Then sum over k to get a piece of harmonic series (the part that includes integers whose prime factors are all less than N). Summing over k, we also got a geometric series. Does this idea work?

Modify this idea slightly by considering

$$\left(\sum_{p>N} \frac{1}{p} \right)^k$$

instead. Can you use this to prove that the sum of the reciprocals of the primes diverges?

Gauss Sums

Definition 4.2: General Gauss Sum

Define the **general Gauss sum** mod an odd prime p to be:

$$g_p(a) = \sum_{t=1}^{p-1} \left(\frac{t}{p} \right) \omega^{\alpha t}$$

where $(\frac{t}{p})$ is the usual Legendre symbol and $\omega = e^{2\pi i/p}$ is a p-th root of unity.

Problem 3

How is this more general Gauss sum related to the previous definition?

Problem 4

If we set $g = g_p(1)$ to be the Gauss sum defined on Pset 10, then $g^2 = p^*$ where $p^* = p$ if $p \equiv 1 \mod 4$ and $p^* = -1$ if $p \equiv 3 \mod 4$.

Problem 5

For p and q odd primes, prove the law of quadratic reciprocity by computing g^q and q, where g is the Gauss sum mod p used in P4.

4.3 July 27, 2023

Claim

If U_m is cyclic, then $\mathbb{D}_m$ is cyclic.

Proof. Let g be a generator of U_m, and let $u = g^k$. Define

$$\psi : u \mapsto \chi_u, \text{ where } \chi_u(a) = e^{\frac{2\pi i}{\varphi(m)} \log_g^u \log_g^a} = e^{\frac{2\pi i k}{\varphi(m)} \log_g^a}.$$

Then $\chi_u(g) = e^{\frac{2\pi i k}{\varphi(m)}}$, which makes $\mathbb{D}_m$ cyclic. ■

Question Is ψ an isomorphism?

Claim

If U_m is cyclic, then the three groups $(U_m, \times)$, $(\mathbb{D}_m, *)$, and ($\varphi(m)$th roots of unity, $\times$) are isomorphic to each other.

Proof. ψ is a bijection. Since $U_m = \{g, g^2, \ldots, g^{\varphi(m)}\}$ are different, χ_g, χ_{g^2}, …, $\chi_{g^{\varphi(m)}}$ all behave differently, and they are different. But also, any element of $\mathbb{D}_m$ must take g to a $\varphi(m)$th root of unity, so we've covered all possibilities.

To check if ψ is an isomorphism, suppose $u_1 = g^{k_1}$, and $u_2 = g^{k_2}$. Then

$$\begin{aligned}\psi(u_1 u_2)(g) &= e^{\frac{2\pi i(k_1+k_2)}{\varphi(m)}} \\ &= e^{\frac{2\pi i k_1}{\varphi(m)}} e^{\frac{2\pi i k_2}{\varphi(m)}} = \big(\psi(u_1) * \psi(u_2)\big)(g).\end{aligned}$$

So ψ is an isomorphism. ■

Claim

$$\sum_{\chi \in \mathbb{D}_m} \chi(a) = \begin{cases} 0 & a \not\equiv 1 \mod m \\ \varphi(m) & a \equiv 1 \mod m \end{cases}$$

Proof. Fix a, and assume $\mathbb{D}_m$ is cyclic. Suppose χ_g is a generator. Then $\mathbb{D}_m = \{\chi_g, \chi_g^2, \cdots, \chi_g^{\varphi(m)}\}$. So

$$\sum_{\chi \in \mathbb{D}_m} \chi(a) = \sum_{i=1}^{\varphi(m)} \chi_g^i(a) = \begin{cases} \sum_{i=1}^{\varphi(m)} w^i & \text{where } w \text{ is the } \varphi(m)\text{th roots on unity} \\ 0 & \gcd(a,m) \neq 1. \end{cases}$$

If $a \equiv 1 \mod m$, then $\chi_g(a) = 1$. But also, if $\chi(a) = 1$ for all $\chi \in \mathbb{D}_m$, then a must be 1 mod m. So if $a \not\equiv 1 \mod m$, $\chi_g(a) \neq 1$, otherwise $\chi_g^i(a) = 1$ for $1 \leq i \leq \varphi(m)$. Since $\chi_g(a)$ is a root of $\chi^{\varphi(m)} - 1 = (\chi - 1)(\chi^{\varphi(m)-1} + \chi^{\varphi(m)-2} + \cdots + \chi + 1) = 0$, $\chi_g(a)$ should be a root of $\chi^{\varphi(m)-1} + \chi^{\varphi(m)-2} + \cdots + \chi + 1$, and thus is the sum we want. This is indeed $\varphi(m)$ when $a \equiv 1 \mod m$, and 0 otherwise. ■

Problem Set 12

Dirichlet Characters

Definition 4.3: Primitive Dirichlet Character

We call a Dirichlet character **primitive** if it is not trivial and does not "come from" a character mod d for a proper divisor d of m.

Problem 1

Consider the Dirichlet characters mod 8 and mod 4. Notice how the non-trivial Dirichlet character mod 4 induces one of the characters mod 8. Which one? Write a careful definition of what it means to be primitive (maybe starting with what it means to not be primitive).

Problem 2

Which moduli m have *all* Dirichlet characters? That is, every Dirichlet character mod m only takes on the values 0, ± 1.

Problem 3

Every real Dirichlet character has the form

$$\chi_0 \chi_4^{\epsilon_1} \chi_8^{\epsilon_2} \prod_{p \in S} \left(\frac{\cdot}{p}\right)$$

where $\cdot$ is the input and the operation is $*$, χ_0 is the trivial character mod m, χ_4 is the nontrivial character mod 4, χ_8 is the character mod 8 with $\chi_8(n) = 1$ if $n \equiv \pm 1$ mod 8 and $\chi_8(n) = -1$ if $n \equiv \pm 3$ mod 8, $\epsilon_i = 0$ or 1, and S is a finite (or empty) set of primes.

Problem 4

Compute $L(1, \chi)$ for each of the Dirichlet characters mod 8.

Gauss Sums and L-functions

Definition 4.4: Even More General Gauss Sum

Define the **even more general Gauss sum** mod a prime p and χ a character to be:

$$g_p(a, \chi) = \sum_{t=1}^{p-1} \chi(t)\omega^{\alpha t}$$

where $\omega = e^{2\pi i/p}$ is a p-th root of unity.

Problem 5

If χ is not the trivial character, then $|g_p(a, \chi)| = \sqrt{p}$.

Problem 6

Setting $\omega = e^{2\pi i/p}$, compute

$$\sum_{k=1}^{p-1} \omega^{ak}\omega^{-nk}$$

for fixed a and n. Write a formula for the function

$$f_a(n) = \begin{cases} 1 & \text{if } a \equiv n \mod p \\ 0 & \text{otherwise.} \end{cases}$$

Problem 7

If χ is not the trivial character, then

$$L(1, \chi) = -\frac{1}{p}\sum_{k=1}^{p-1} g_p(k, \chi)\log(1 - \omega^k).$$

Hint: First rewrite $L(s, \chi)$ for $s > 1$ by grouping terms according to their residue class mod p. Then take the limit as $s \to 1^+$.

5 Week 5

5.1 July 31, 2023

We now want to prove that

$$\sum_{\chi \in \mathbb{D}_m} \chi(a) = \begin{cases} 0 & a \not\equiv 1 \mod m \\ \varphi(m) & a \equiv 1 \mod m \end{cases}$$

in general cases, even when $\mathbb{D}_m$ is not cyclic.

Proof. Take any character ψ. Then $\chi(a) = \psi(a)\psi^{-1}(a)\chi(a)$, so

$$\sum_{x \in \mathbb{D}_m} \chi(a) = \psi(a) \sum_{x \in \mathbb{D}_m} \psi^{-1}(a)\chi(a) = \psi(a) \sum_{x \in \mathbb{D}_m} \chi(a).$$

This implies that either $\psi(a) \neq 1$ and $\sum_{x \in \mathbb{D}_m} \chi(a) = 0$, or $\psi(a) = 1$ for all $\psi \in \mathbb{D}_m$. $\psi(a) = 1$ for all $\psi \in \mathbb{D}_m$ means $a \equiv 1 \mod m$ and hence $\sum_{x \in \mathbb{D}_m} \chi(a) = \varphi(m)$. So we are done. ■

Then we have two questions.

Question Does $\psi(a) = 1$ for all $\psi \in \mathbb{D}_m$ implies that $a \equiv 1 \mod m$?

Question Does $a \equiv 1 \mod m$ implies $\sum_{x \in \mathbb{D}_m} \chi(a) = \varphi(m)$?

We answer to the question by proving that U_m is isomorphic to $\mathbb{D}_m$, even if U_m is non cyclic.

Theorem 5.1

$\mathrm{U}_m \cong \mathbb{D}_m$.

Example 10

Take $U_{15} = U_3 \times U_5$. 2 is a generator in both U_3 and U_5. Since

$$11 \equiv \begin{cases} 2 & \mod 3 \\ 1 & \mod 5 \end{cases} \quad \text{and } 7 \equiv \begin{cases} 1 & \mod 3 \\ 2 & \mod 5, \end{cases}$$

U_{15} is generated by 11 and 7, i.e. $U_{15} = 11^k 7^l$ for $0 \leq k \leq 1$ and $0 \leq l \leq 3$.

Proof. Let $m = 2^t p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. Then, $U_m = U_{2^t} \times U_{p_1^{k_1}} \times \cdots \times U_{p_s^{k_s}}$.

- if $t = 1$, then U_2 is generated by 1.
- if $t = 2$, then U_4 is generated by 3.
- if $t > 2$, then since 3 has order 2^{t-2}, and -1 is not a power of 3, U_{2^t} is generated by 3 and -1.

Also, we can find generators of each $U_{p_i^{k_i}}$ because $U_{p_1^{k_1}}$, $U_{p_2^{k_2}}$, ..., $U_{p_s^{k_s}}$ are cyclic. Finally, the mapping

$$\begin{aligned} \chi &\mapsto \big(\chi(g_1),\, \chi(g_2),\, \ldots,\, \chi(g_s)\big) \\ &\mapsto \big(e^{\frac{2\pi i l_1}{\varphi(p_1^{k_1})}},\, e^{\frac{2\pi i l_2}{\varphi(p_2^{k_2})}},\, \ldots,\, e^{\frac{2\pi i l_s}{\varphi(p_s^{k_s})}}\big) \\ &\mapsto g_1^{l_1} g_2^{l_2} \cdots g_s^{l_s} \end{aligned}$$

implies that $\mathbb{D}_m$ is isomorphic to U_m. ■

Then for the second question, since $U_m \cong \mathbb{D}_m$, $\mathbb{D}_m$ has $\varphi(m)$ elements, so $\sum_{x \in \mathbb{D}_m} \chi(a) = \varphi(m)$. For the first question, if $a \not\equiv 1 \mod m$, then there exists l_1, l_2, ..., $l_r \neq 0$ such that $a = g_1^{l_1} g_2^{l_2} \cdots g_r^{l_r}$. If we take the character that has

$$\chi(g_j) = \begin{cases} 1 & j \neq i \\ e^{\frac{2\pi i}{\varphi(p_i^{k_i})}} & j = i \end{cases}$$

then $\chi(a) \neq 1$. So finally we have

Theorem 5.2

$$\sum_{\chi \in \mathbb{D}_m} \chi(n) = \begin{cases} \varphi(m) & n \equiv 1 \mod m \\ 0 & \text{otherwise} \end{cases}$$

Theorem 5.3

$$\sum_{\chi \in \mathbb{D}_m} \chi(na^{-1}) = \begin{cases} \varphi(m) & n \equiv a \mod m \\ 0 & \text{otherwise.} \end{cases}$$

Problem Set 13

Primitive vs. Imprimitive Dirichlet Characters

Problem 1

If χ is a primitive character mod d and χ' is an imprimitive character mod $dk = m$ that is induced by χ, then how are $L(s, \chi)$ and $L(s, \chi')$ related?

Problem 2

Compute $g_m(a, \chi)$ for primitive characters mod 6, 8, 9, 10, 12, ... Any conjectures?

Problem 3

If χ is a primitive character mod m, then

$$L(1, \chi) = -\frac{1}{m} \sum_{k=1}^{m-1} g_m(k, \chi) \log(1 - \omega^{-k}) = -\frac{g_m(1, \chi)}{m} \sum_{k=1}^{m-1} \overline{\chi(k)} \log(1 - \omega^{-k}).$$

Numericals

Problem 4

Let χ_{-n} be the character $\chi_{-n}(a) = (\frac{-n}{a})$, where this means the usual Legendre symbol if a is an odd prime. For $a = 2$, we have

$$\left(\frac{m}{2}\right) = \begin{cases} 1 & \text{if } m \equiv 1 \mod 8 \\ -1 & \text{if } m \equiv 5 \mod 8 \\ 0 & \text{otherwise.} \end{cases}$$

and if a is a product of primes $a = p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_k^{\epsilon_k}$, we set $(\frac{m}{a}) = (\frac{m}{p_1})^{\epsilon_1} (\frac{m}{p_2})^{\epsilon_2} \cdots (\frac{m}{p_k})^{\epsilon_k}$. This is a character mod...?

Problem 5

Use a computer to calculate $L(1, \chi_{-n})$ for $n = 2, 5, 6, 10, 13, 14, 17$. Compare to $\pi/\sqrt{n}$.

Problem 6

Which $\mathbb{Z}[\sqrt{-n}]$ have unique prime factorization for $n = 2, 5, 6, 10, 13, 14, 17$?

5.2 August 2, 2023

To prove that there are infinitely many primes of $a \mod m$, we show that $\displaystyle\sum_{\substack{p\equiv a \mod m \\ p \text{ prime}}} \frac{1}{p}$ diverges.

Lemma

If $\gcd(a,m) = 1$, then $\displaystyle\sum_{\substack{p\equiv a \mod m \\ p \text{ prime}}} \frac{1}{p^s}$ should diverge as long as the sum of $L(1,\chi)$ is negative infinity for all the other characters.

Proof. We have

$$\sum_{\substack{p\equiv a \mod m \\ p \text{ prime}}} \frac{1}{p} = \frac{1}{\varphi(m)} \sum_{p \text{ prime}} \sum_{x\in\mathbb{D}_m} \frac{\chi(a^{-1}p)}{p^s}$$

$$= \frac{1}{\varphi(m)} \sum_{x\in\mathbb{D}_m} \sum_{p \text{ prime}} \frac{\chi(a^{-1}p)}{p^s}$$

$$= \frac{1}{\varphi(m)} \sum_{x\in\mathbb{D}_m} \chi(a^{-1}) \sum_{p \text{ prime}} \frac{\chi(p)}{p^s}$$

Recall that $L(s,\chi) = \displaystyle\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$. So

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

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

$$= \sum_{p \text{ prime}} \sum_{n=1}^{\infty} \frac{\chi(p^n)}{np^{ns}}$$

$$= \sum_{p \text{ prime}} \frac{\chi(p)}{p^s} + \sum_{p \text{ prime}} \sum_{n=2}^{\infty} \frac{\chi(p^n)}{np^{ns}}$$

We see that $\displaystyle\sum_{p\text{ prime}}\sum_{n=2}^{\infty}\frac{\chi(p^n)}{np^{ns}}$ is bounded because

$$\left|\sum_{p\text{ prime}}\sum_{n=2}^{\infty}\frac{\chi(p^n)}{np^{ns}}\right| \leq \sum_{p\text{ prime}}\sum_{n=2}^{\infty}\left|\frac{\chi(p^n)}{np^{ns}}\right| = \sum_{p\text{ prime}}\sum_{n=2}^{\infty}\frac{1}{np^{ns}} \leq \frac{\pi^2}{6}.$$

This tells us that

$$\begin{aligned}
&\frac{1}{\varphi(m)}\sum_{\chi\in\mathbb{D}_m}\chi(a^{-1})\log L(s,\chi) \\
&= \frac{1}{\varphi(m)}\sum_{\chi\in\mathbb{D}_m}\chi(a^{-1})\Bigg(\sum_{p\text{ prime}}\frac{\chi(p)}{p^s}+\sum_{p\text{ prime}}\sum_{n=2}^{\infty}\frac{\chi(p^n)}{np^{ns}}\Bigg) \\
&= \frac{1}{\varphi(m)}\sum_{\chi\in\mathbb{D}_m}\sum_{p\text{ prime}}\frac{\chi(a^{-1}p)}{p^s}+\frac{1}{\varphi(m)}\sum_{\chi\in\mathbb{D}_m}\chi(a^{-1})\sum_{p\text{ prime}}\sum_{n=2}^{\infty}\frac{\chi(p^n)}{np^{ns}} \\
&= \sum_{\substack{p\equiv a \mod m\\ p\text{ prime}}}\frac{1}{p^s}+\frac{1}{\varphi(m)}\sum_{\chi\in\mathbb{D}_m}\chi(a^{-1})\sum_{p\text{ prime}}\sum_{n=2}^{\infty}\frac{\chi(p^n)}{np^{ns}} \\
&= \sum_{\substack{p\equiv a \mod m\\ p\text{ prime}}}\frac{1}{p^s}+\big(\text{bounded stuff}\big)
\end{aligned}$$

because the second term is a finite sum of bounded terms, thus it is bounded. We will now prove that $L(s,\chi)$ diverges for $s=1$. We look at χ_e, the trivial character.

$$\chi_e(n)=\begin{cases}1 & \gcd(m,n)=1\\ 0 & \text{otherwise}\end{cases}$$

Then

$$\begin{aligned}
L(s,\chi_e) &= \prod_{p\text{ prime}}\left(1-\frac{\chi_e(p)}{p^s}\right)^{-1} \\
&= \prod_{p\nmid m}\left(1-\frac{1}{p^s}\right)^{-1}\prod_{p\mid m}\left(1-\frac{0}{p^s}\right)^{-1} \\
&= \prod_{p\nmid m}\left(1-\frac{1}{p^s}\right)^{-1}
\end{aligned}$$

This differs with $\displaystyle\zeta(s)=\prod_{p\text{ prime}}\left(1-\frac{1}{p^s}\right)^{-1}$ by $\displaystyle\prod_{p\mid m}\left(1-\frac{1}{p^s}\right)^{-1}$, which is a finite product since there are prime divisors of m. So

$$\lim_{s\to 1} L(s,\chi_e) = \infty$$

since $\log\zeta(s)$ diverges as $s \to 1^+$. Therefore, $\sum_{\substack{p\equiv a \mod m \\ p \text{ prime}}} \frac{1}{p^s}$ should diverge as long as the sum of $L(1,\chi)$ is negative infinity for all the other characters. ■

Problem Set 14

Expressing $L(1,\chi)$

Problem 1

On the last problem set, you showed that if χ is a primitive character mod m, then

$$L(1,\chi) = -\frac{1}{m}\sum_{k=1}^{m-1} g_m(k,\chi)\log(1-\omega^{-k}) = -\frac{g_m(1,\chi)}{m}\sum_{k=1}^{m-1}\overline{\chi(k)}\log(1-\omega^{-k}).$$

If the modulus is actually a prime p that is 3 mod 4, and $\chi(a) = (\frac{a}{p})$, can you simplify this expression for $L(1,\chi)$?

Numericals

Problem 2

Which primes p in $\mathbb{Z}$ are still prime in $\mathbb{Z}[\sqrt{-2}]$? Are 2, 3, 5, 7, 11, 13, 17 prime in $\mathbb{Z}[\sqrt{-2}]$?

Problem 3

Which primes p of $\mathbb{Z}$ can be written in the form $x^2 + 2y^2$?

Problem 4

Which primes p in $\mathbb{Z}$ are still prime in $\mathbb{Z}[\sqrt{-5}]$? Which primes p of $\mathbb{Z}$ can be written in the form $x^2 + 5y^2$?

Problem 5

A binary quadratic form is a polynomial of the form $Q(x,y) = ax^2 + bxy + cy^2$, where a, b, $c \in \mathbb{Z}$. How mant inequivalent quadratic forms have discriminant -8? What about -20? Here, two binary quadratic forms Q and Q' of discriminant D are equivalent if there exist R, U, S, $T \in \mathbb{Z}$ such that $Q(Rx+Sy, Tx+Uy) = Q'(x,y)$.