1. Lecture 1

Problem 1 –
Completely classify the primes $p \equiv a \bmod m$ when $\gcd(a, m) > 1$.

Problem 2 –
Prove that there are infinitely many primes congruent to 2 mod 3.

Problem 3 –
Prove that there are infinitely many primes $p \equiv 5 \bmod 6$ by pure thought. (Do not lift your pen! Turn in a blank answer.)

Problem 4 –
Here is a reminder on how to prove that $x^2 \equiv -1 \bmod p$ has a solution if and only if $p = 2$ or $p \equiv 1 \bmod 4$.

(a) Show that $x^2 \equiv -1 \bmod 2$ has a solution.
(b) Suppose that $x^2 \equiv -1 \bmod p$ and p is an odd prime. Raise this equation to the $\frac{p-1}{2}$-power and thus show that $p \equiv 1 \bmod 4$.
(c) It remains to give the existence of a solution to $x^2 \equiv -1 \bmod 4$ when $p \equiv 1 \bmod 4$. For that, consider $x = \left(\frac{p-1}{2}\right)!$ and use Wilson's theorem.

Problem 5 –
Make a table of comparing the primes $p \equiv 1 \bmod 3$ and the primes $p \equiv 2 \bmod 3$. How does it compare to the table we had in class for the modulus 4?

Problem 6 –
Try to make precise the second part of Dirichlet's theorem. How likely do you think it is that a prime p is congruent to 1 mod 14? What about 13 mod 27?

Problem 7 –
Use a computer to find the first time the number of primes $p \equiv 3 \bmod 4$ are less than the primes $p \equiv 1 \bmod 4$.

Exercise –
The proofs of Dirichlet's theorem for $p \equiv 1, 3 \bmod 4$ actually give an algorithm for generating a list of primes congruent to 3 and 1 modulo 4. Write down the first twenty or so terms in these sequences. Do you think all the primes appear in one of these lists? Why or why not?

Exercise –
Try to prove Dirichlet's theorem for primes $p \equiv 2 \bmod 5$.

Exercise –
Find a fast computer and try to figure out how big you need N to be so that $\sum_{p \leq N} 1/p > 3$. Then compute $\sum_{n \leq N} 1/n$ for that same N.

Exercise (Calculus) –
Do you remember what a sequence $\{x_n\}$ of real or complex numbers is? If not, ask someone (me for instance). Once you've done that, also find out what it means to say $\lim_{n\to\infty} x_n = x$ and then compute the following limits, if they exist:

(a) $\lim_{n\to\infty} (-1)^n$.
(b) $\lim_{n\to\infty} \dfrac{(-1)^n}{n}$.
(c) $\lim_{n\to\infty} \left(1 + \dfrac{1}{2} + \cdots + \dfrac{1}{2^n}\right)$.

One definition of the number e is $e = \lim_{n\to\infty} \left(1 + \dfrac{1}{n}\right)^n$. Show that

$$e^x = \lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n.$$

Exercise (Calculus) –
Let i be a complex square root of -1. Explain why $\lim_{n\to\infty} i^n$ does not exist first using any definition and then by drawing a picture.

2. Lecture 2

Problem 8 –
Prove that if p is prime then $x^2 + x + 1 \equiv 0 \bmod p$ has a solution if and only if $p = 3$ or $p \equiv 1 \bmod 3$.

Problem 9 –
Prove Dirichlet's theorem for the modulus 8 (we did $p \equiv 1 \bmod 8$ in class).

Problem 10 –
Let's generalize the lemma in class about solutions to $x^4 + 1 \equiv 0 \bmod p$.

(a) Let m be an integer. Recall that a primitive root modulo[1] m is an integer g co-prime to m such that $g, g^2, \ldots, g^{\phi(m)}$ are distinct modulo m. Primitive roots exist if and only if $m = 2, 4, p^r$ or $2p^r$ where p is an odd prime and $r \geq 1$. Make a complete list of primitive roots for the first dozen primes.
(b) Let p be an odd prime and $g \bmod p$ be a primitive root. Show that $g^{\frac{p-1}{2}} \equiv -1 \bmod p$.
(c) Suppose that $p \equiv 1 \bmod 8$. Show that $x^4 + 1 \equiv 0 \bmod p$ has a solution.
(d) Let $n \geq 1$ and p be an odd prime. Show that $x^{2^n} \equiv -1 \bmod p$ has a solution if and only if $p \equiv 1 \bmod 2^{n+1}$. Can you conclude Dirichlet's theorem for m a power of 2 and $a = 1$ now?

Problem 11 –
In class I said that $a^2 \equiv 1 \bmod m$ is a necessary and sufficient condition for there to exist a "Euclidean" proof of Dirichlet's theorem for $a \bmod m$ (though I didn't make that precise).

(a) Show that $a^2 \equiv 1 \bmod 24$ for all integers a relatively prime to 24.
(b) Prove that 24 is the largest integer for which the previous statement holds. (Hint: you might want to consider primitive roots and the Chinese remainder theorem). Make a list of all the other $m \geq 24$ for which the previous statement holds. Have you proven Dirichlet's theorem for those $m < 24$? Try some of the proofs for the m you haven't settled yet.

Problem 12 –
If $f(x)$ is a polynomial then set $P(f) = \{\text{primes } p\colon f(x) \equiv 0 \bmod p \text{ has a solution}\}$.

(a) Compute $P(f)$ if $f(x) = mx + b$ is a linear polynomial.
(b) Show that $P(f) \neq \varnothing$ if f is non-constant (Hint: when is $x = 0$ a solution to $f(x) \equiv 0 \bmod p$?)
(c) Show that $P(f)$ is infinite if f is non-constant (Hint: try first the case where $f(0) = 1$ and mimic Euclid's proof).
(d) A stronger statement is true: if g and f are both non-constant then $P(f) \cap P(g)$ is also infinite. Prove this for some pairs of quadratic polynomials f and g.

Problem 13 –
Remember that an infinite sum $\sum_{n=0}^{\infty} a_n$ with $a_n \in \mathbf{R}$ or $a_n \in \mathbf{C}$ converges if the limit

$$\lim_{N\to\infty} \left(\sum_{n=0}^{N} a_n \right) = \lim_{N\to\infty} a_0 + a_1 + \cdots + a_N$$

exists. We say that the infinite sum $\sum_{n=0}^{\infty} a_n$ converges *absolutely* if $\sum_{n=0}^{\infty} |a_n|$ converges.

(a) Do you remember how to write down Taylor series expansions? Write down the Taylor series expansion of e^x. Explain carefully why the sum absolutely converges for all $x \in \mathbf{R}$.
(b) Now replace x by z and realize that your previous conclusion still holds. This means we have a function $z \mapsto e^z$ of a complex variable z.
(c) Do the previous two exercises for the trigonometric functions sin and cos.
(d) Let $\theta \in \mathbf{R}$. Compute the expansions $e^{i\theta}$, $\cos(\theta)$ and $\sin(\theta)$ to show that $e^{i\theta} = \cos(\theta) + i\sin(\theta)$ makes sense in terms of Taylor series expansions (so I'm not completely crazy).

[1]This is a different notion than a primitive nth root of unity in the complex numbers. A primitive root here is a generator for the multiplicative group $(\mathbf{Z}/m\mathbf{Z})^\times$, if it exists. A primitive nth root of unity is essentially a generator for the additive group $\mathbf{Z}/n\mathbf{Z}$ (which always exists).

3. Lecture 3

Problem 14 –
Compute the first ten cyclotomic polynomials.

Problem 15 –
Prove the following lemma we had in class: if $n > 1$ then $\Phi_n(0) = 1$.

Problem 16 –
Find roots to $\Phi_5(z) \equiv 0 \bmod p$ for the first five primes $p \equiv 1 \bmod 5$.

Problem 17 –
Prove Eisenstein's criterion for irreducibility: Suppose that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbf{Z}[x]$ is a polynomial and p is any prime number such that $p \nmid a_n$, $p \mid a_i$ if $i < n$ and $p^2 \nmid a_0$. Then $f(x)$ is irreducible. (Hint: factor $f(x)$ into two factors and then reduce the equation modulo p.)

Problem 18 –
Show that $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$. Use Eisenstein's criterion to show that $\Phi_p(x)$ is irreducible (consider changing variables to $u = x + 1$).

Problem 19 –
Prove the following identities:

(a) $\Phi_n(x) = x^{\phi(n)}\Phi_n(1/x)$.
(b) If p is prime and $r \geq 1$ then $\Phi_{p^r}(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = \Phi_p(x^{p^{r-1}})$ (this implies $\Phi_{p^r}(x)$ is also irreducible[2]).
(c) If n is odd then $\Phi_{2n}(x) = \Phi_n(-x)$.
(d) If $m = p_1^{r_1} \cdots p_s^{r_s}$ then $\Phi_m(x) = \Phi_{p_1 \cdots p_s}(x^{p_1^{r_1-1} \cdots p_s^{r_s-1}})$.

Problem 20 –
As mentioned in the footnote, the cyclotomic polynomials $\Phi_n(x) \in \mathbf{Z}[x]$ are all irreducible.

(a) Show that if $p \equiv 1 \bmod n$ then $\Phi_n(x) \bmod p \in \mathbf{F}_p[x]$ has a complete set of roots modulo p.
(b) Write down all the primes $p \leq 19$ and factor $\Phi_8(x) \bmod p$ when you can. Do you think $\Phi_8(x)$ is ever irreducible modulo p?
(c) Do the previous exercise for Φ_6, Φ_{12} as well.
(d) Find a prime p where $\Phi_9(x)$ is irreducible modulo p, if you can.

Problem 21 –
Consider the fifth cyclotomic polynomial $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ and let $\Psi_5(x) = x^2 + x - 1$.

(a) Show $\Psi_5(x) \equiv 0 \bmod p$ has a solution if and only if $p \equiv 1, 4 \bmod 5$ (or $p = 5$).
(b) Show that we have the relation $x^2 \cdot \Psi_5(x + x^{-1}) = \Phi_5(x)$.
(c) Show that if $p \equiv 1 \bmod 5$ (or $p = 5$) then $\Phi_5(x) \bmod p \in \mathbf{F}_p[x]$ factors into four linear factors. Try to show if $p \equiv 4 \bmod 5$ then $\Phi_5(x) \bmod p$ factors into two quadratic irreducible factors[3]. What about $p = 5$?
(d) Try to study $\Phi_5(x) \bmod p$ for small primes $p \equiv 2, 3 \bmod 5$. What do you think?

Exercise –
Repeat[4] the previous exercise for $p = 7$ and then show that there are infinitely many primes $p \equiv 6 \bmod 7$.

Exercise (Preview) –
If $f(z)$ is a complex function consider the limit

$$\lim_{w \to z} \frac{f(z) - f(w)}{z - w} \tag{0.1}$$

if it exists. It is important to note: for the limit to exist, it must converge, and *be equal*, for *all sequences* of points $w \to z$. Now consider (0.1) for the function $f(z) = \overline{z}$. Show the limit does not exist at $z = 0$ by computing it over two sequences $w \to 0$:

(a) Taking $w \to 0$ with $w = t$ with $t \in \mathbf{R}$ approaching 0.
(b) Taking $w \to 0$ with w of the form it with $t \in \mathbf{R}$ approaching zero.

Draw a picture to illustrate what is happening. Do you think we should call $z \mapsto \overline{z}$ a differentiable function?

[2]For all n, $\Phi_n(x)$ is irreducible but Eisenstein's criterion won't get you there
[3]Hint: you might start by considering the polynomial $T^2 - yT + 1 \in \mathbf{F}_p[T]$ where y is a root modulo p of $\Psi_5(x)$.
[4]You'll want to generalize (b) first, and then go prove the analog of (a).

4. Lecture 4

Problem 22 –
Here is another proof that the harmonic series diverges.

(a) If $n \geq 1$, set
$$x_n = \frac{1}{2^n} + \cdots + \frac{1}{2^{n+1}-1}$$
Show that $x_n \geq \frac{1}{2}$ for all $n \geq 1$.

(b) Show that $\sum_n \frac{1}{n} = 1 + \sum_{n\geq 1} x_n$. Conclude that the harmonic series $\sum_n \frac{1}{n}$ diverges.

Problem 23 –
Compute the infinite sum $\displaystyle\sum_{m=2}^{\infty} \frac{1}{m(m-1)}$.

Problem 24 –
We will use the Taylor series for $\arctan(x)$ in the next lecture[5].

(a) Show (or remind yourself why) $\arctan(x) = \displaystyle\int_0^x \frac{1}{1+t^2}\, dt$.

(b) Show that for each $N \geq 0$ and every x we have
$$\arctan(x) = \left(\sum_{n=0}^{N} (-1)^n \frac{x^{2n+1}}{2n+1}\right) + (-1)^{N+1} \int_0^x \frac{t^{2N+2}}{1+t^2}\, dt.$$
(Hint: consider how to compute the geometric series for $\frac{1}{1+t^2}$ and then integrate.)

(c) Let's consider the second sum in the previous part. Since $\frac{1}{1+t^2} \leq 1$ for all t, show that if $x \leq 1$ then
$$\lim_{N\to\infty} \int_0^x \frac{t^{2N+2}}{1+t^2}\, dt = 0.$$
Conclude that if $x \leq 1$ then
$$\arctan(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{2n+1}.$$

(d) Calculate the infinite sum
$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots$$

Problem 25 –
There is a famous proof due to Erdős that $\sum 1/p$ diverges. Rather than transcribe that proof for you (you should find it and read it yourself), here is another proof which apparently is due to J. Clarkson (appeared in Proc. Amer. Math. Soc., 1966).

Suppose that $\sum_p 1/p$ converges. Order the primes $p_1 < p_2 < \cdots$ and choose an N so large that $\sum_{i=N+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}$. We will reach a contradiction.

(a) Let $M = p_1 \ldots p_N$. Show that for each $n \geq 1$, the prime factors of $1+nM$ are among $p_{N+1}, p_{N+2}, \ldots$.

(b) Show that for every $n \geq 1$ there exists a j such that $\frac{1}{1+nM}$ is one of the terms appearing in the expansion of in the expansion of
$$\left(\sum_{i>N} \frac{1}{p_i}\right)^j = \left(\frac{1}{p_{N+1}} + \frac{1}{p_{N+2}} + \cdots\right)^j$$
and thus
$$\sum_{n=1}^{\infty} \frac{1}{1+nM} \leq \sum_{j=1}^{\infty} \left(\sum_{i>N} \frac{1}{p_i}\right)^j$$

(c) Use your assumption and the previous step to gain a contradiction.

[5]In lecture I will not be this delicate about the issue at $x = 1$ but since the final result relies on that, it is best if we do this for homework

5. Lecture 5

Problem 26 –
We proved again in class that there are infinitely many primes $p \equiv 3 \bmod 4$ by computing the Dirichlet density using the computation for primes $p \equiv 1 \bmod 4$. Instead of looking at $\log \zeta(s) + \log L(s)$ consider $\log \zeta(s) - \log L(s)$ and use it to compute the density of prime $p \equiv 3 \bmod 4$ directly.

Exercise (An important message) –
Inf Problems 27 below there are infinite sums indexed by sets which are not the integers. I ask you to explain how you will compute the sum but one might worry that your choice is going to effect the outcome (what if two of you choose two different ways of forming the sum?). Luckily we have the following important fact that you are free to use now and forever:

> Fact: If $\sum_{i=0}^{\infty} x_i$ is an *absolutely* convergent sum then you can compute it by rearranging the terms in any way you like.

In particular, if all the x_i are non-negative real numbers and $\sum_i x_i$ converges then any order of summation computes the same value. Here is some silly example to show what can go wrong.

(a) Show that the sum $\sum_{n=1}^{\infty} \frac{(-1)^n}{n}$ is convergent, but not absolutely, and compute its value.
(b) Show that there is a way to rearrange the sequence $\{(-1)^n/n\}$ so that the corresponding infinite sum becomes *divergent*.

Problem 27 –
Let $\mathbf{F}_p[x]$ be the polynomial ring in the variable x over the integers modulo p. Recall that $\mathbf{F}_p[x]$ behaves just like the integers: every non-zero element $f \in \mathbf{F}_p[x]$ factors into a product of irreducible polynomials, uniquely up to units. The units in $\mathbf{F}_p[x]$ are just the non-zero constants.

(a) Prove the previous statement: the units in $\mathbf{F}_p[x]$ are the non-zero constants.
(b) For $f \in \mathbf{F}_p[x]$ define its *norm* to be $\mathrm{N}(f) := p^{\deg f}$. For example, if c is a constant then $\mathrm{N}(c) = 1$ and for each $n \geq 0$, $\mathrm{N}(x^n) = p^n$. Show that $\mathrm{N}(fg) = \mathrm{N}(f)\mathrm{N}(g)$.
(c) Compute $\#\{f \in \mathbf{F}_p[x] \colon \mathrm{N}(f) = p^n\}$ for each $n = 0, 1, 2, \ldots$
(d) We now define a new zeta function by

$$\zeta_{\mathbf{F}_p[x]}(s) = \sum_{f \text{ monic}} \frac{1}{\mathrm{N}(f)^s}.$$

Explain what the sum means and how you will compute it (it isn't indexed by integers).
(e) Discuss the algebraic analogy between summing over the *monic* f in the definition of $\zeta_{\mathbf{F}_p[x]}(s)$ and summing over positive integers $n \geq 1$ in the definition of $\zeta(s) = \sum_{n \geq 1} n^{-s}$.
(f) Show that the $\zeta_{\mathbf{F}_p[x]}(s)$ converges for $s > 1$ and then compute $\zeta_{\mathbf{F}_p[x]}(s)$ *explicitly* as a function of p^{-s}.
(g) Show that $\zeta_{\mathbf{F}_p[x]}(s)$ has an Euler product expression for $s > 1$ given by

$$\zeta_{\mathbf{F}_p[x]}(s) = \prod_{g \text{ monic irred.}} \left(\frac{1}{1 - \frac{1}{\mathrm{N}(g)^s}} \right)$$

Make sure you explain how you are computing the product.
(h) Prove that there are infinitely many irreducible polynomials in $\mathbf{F}_p[x]$.

Problem 28 (Calculus) –
There is a funny technique called "summation by parts" that we are going to use later in the course, so I am putting it here now. I also used it in the lecture via its application to Abel's theorem.

(a) Let $a_0, a_1, \ldots$ and $s_0, s_1, \ldots$ be sequences of real or complex numbers. For each $N > 0$ show that[6]

$$a_0 s_0 + \sum_{i=1}^{N} a_i (s_i - s_{i-1}) = a_N s_N - \sum_{i=1}^{N} s_{i-1}(a_i - a_{i-1}).$$

(b) If z_i is a sequence then let $\mathrm{d}(z_i) = z_i - z_{i-1}$. Re-write the previous formula in terms of $\sum a_i \mathrm{d}(s_i)$ and $\sum s_{j+1} \mathrm{d}(a_j)$ and then discuss why summation by parts is a good name.

[6] If my indices are off fix them accordingly.

Exercise (Bonus calculus, Abel's theorem) –
Let $f(x)$ be an infinite series $f(x) = \sum_{k=0}^{\infty} b_k x^k$ that converges on $|x| < 1$. Assume that $\sum b_k$ converges. We want to show $\lim_{x\to 1^-} f(x) = \sum b_k$. This is usually called Abel's theorem and we used it in class to calculate $\arctan(1)$ as the infinite sum $1 - 1/3 + 1/5 - 1/7 + \cdots$. It has an amusing analog for complex series but we won't need it explicitly.

(a) Fix $|x| < 1$ and define

$$f_N(x) = b_0 + b_1 x + \cdots b_N x^N = \sum_{i=0}^{N} b_i x^i,$$

$$s_N = b_0 + b_1 + \cdots + b_N = \sum_{i=0}^{N} b_i.$$

Show that

$$f_N(x) = s_N x^N - \sum_{j=0}^{N-1} s_j (x^{j+1} - x^j) = s_N x^N - (x-1) \sum_{j=0}^{N-1} s_j x^j.$$

and thus show that

$$f(x) = (1-x) \sum_{j=0}^{\infty} s_j x^j$$

(b) Let $s = \lim_{j\to\infty} s_j = \sum b_k$. Show that if $|x| < 1$ then

$$f(x) - s = (1-x) \sum_{j=0}^{\infty} (s_j - s) x^j.$$

(c) Remember our goal is to show that $f(x) \to s$ as $x \to 1^-$. If $\varepsilon > 0$ is chosen then show that we can choose N so large that

$$|f(x) - s| \leq \left[(1-x) \sum_{j=0}^{N} |s_j - s| \, x^j \right] + \varepsilon$$

for *every single* x. This is a very important idea in analysis: N is chosen to give this estimate for all x at once. Informally, if N had to depend on x then what could go wrong as we take $x \to 1^-$ (see the next step) is that the N could keep getting bigger and bigger, eventually turning into some unwieldy infinite sum[7].

(d) Conclude from the previous part that $\lim_{x\to 1^-} f(x) = s$.

(e) Using the discussion in class about computing $\arctan(1)$ as an infinite sum, show that

$$\ln(2) = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots = \sum_{n=0}^{\infty} (-1)^n \frac{1}{n+1}.$$

[7] To spiritually see what can go wrong when trying to make two estimates at once, consider the number 2^{n-m} and compute

$$\lim_{m\to\infty} \lim_{n\to\infty} 2^{n-m} \text{ and } \lim_{n\to\infty} \lim_{m\to\infty} 2^{n-m}.$$

You should get two (wildly) different answers. The issue here is that the various rate of convergence for one of the inner limits depends on the index of the outer limit and so it messes up our desire to compute the limit in either order. This isn't exactly the issue in the proof of Abel's theorem but it is a good approximation.

6. Lecture 6

Problem 29 –
If $x \neq 0$ is a real number let $f(x) = x\sin(1/x)$. This is continuous on $x \neq 0$, being a composition of continuous functions.

(a) Show that $f(x)$ extends to a continuous function at $x = 0$ and denote this function by $f(x)$ still.
(b) Is $f(x)$ differentiable at $x = 0$?
(c) Repeat the same two things for $g(x) = x^2\sin(1/x)$. Is $g(x)$ twice differentiable at $x = 0$?

Problem 30 –
We've seen the power series definitions of complex analytic functions e^z, $\cos z$ and $\sin z$. I even told you that by the rigidity of complex analytic functions, we know that $\cos^2 z + \sin^2 z = 1$.

(a) Show that $e^{iz} = \cos z + i\sin z$ for all $z \in \mathbf{C}$.
(b) Show that the functions $z \mapsto \cos z$ and $z \mapsto \sin z$ are *unbounded*.
(c) Show that the function $f(z) = z\sin(1/z)$ does not extend to a continuous function on $\mathbf{C}$.
(d) Does $z^n\sin(1/z)$ extend to a continuous function for any value of $n \geq 1$?

Problem 31 –
Show that the image of the function $z \mapsto e^z$ is $\mathbf{C}\backslash\{0\}$ and that e^z is not injective. Compare with its restriction to real numbers.

Problem 32 –
Show directly that if $P(z)$ is polynomial and $P(z) \neq 0$ for all $z \in U$ then $1/P(z)$ is an analytic function on U as well. Now try the analogous statement for all analytic functions (with the obvious hypotheses).

Problem 33 –
Here, n is an integer assume $n \geq 1$.

(a) If $s \in \mathbf{C}$, give a reasonable definition of n^s, show that $s \mapsto n^s$ is a complex analytic function and then compute $|n^s|$.
(b) Show that the complex function $\zeta(s) = \displaystyle\sum_{n=1}^{\infty} \frac{1}{n^s}$ converges on the open set $\mathrm{Re}(s) > 1$.

Problem 34 –
When defining integrals on the real line, we are aided by our intuition that one number is smaller than another. Is there an analog for some subsets of $\mathbf{C}$? A total order on $\mathbf{C}$ is a relation $z \succ w$ subject to the following axioms:

- If $z, w \in \mathbf{C}$ then exactly one of the following holds: $z = w$ or $z \succ w$ or $w \succ z$.
- If $z, w, x \in \mathbf{C}$ then $z \succ w$ implies $z + x \succ w + x$.
- If $z, w, x \in \mathbf{C}$ then $z \succ 0$ implies $zx \succ zw$.

Show that there is no total order on $\mathbf{C}$.

Problem 35 –
For each of the functions $f(z)$ below, show that $f(z)$ converges absolutely on $|z| < 1$ and then describe its behavior on the circle $|z| = 1$.

(a) $f(z) = \displaystyle\sum_{n\geq 1} nz^n$.
(b) $f(z) = \displaystyle\sum_{n\geq 1} z^n/n^2$.
(c) $f(z) = \displaystyle\sum_{n\geq 1} z^n/n$.

Problem 36 –
Let $R > 0$. Compute the path integral $\displaystyle\int_{|z|=R} z^n\, dz$ for all integers n. How does it depend on R?

Problem 37 –
Suppose that $f(z)$ is a continuous function on an open set $U \subset \mathbf{C}$ then an antiderivative $F(z)$ for $f(z)$ is another function defiend on U such that $F'(z) = f(z)$. Do you think that $\overline{z} \mapsto z$ has an antiderivative anywhere? How does this compare with the fundamental theorem of calculus?

7. Lecture 7

Problem 38 –
Show that if the origin does not lie in the region bounded by the circle $|z-w|=R$ then $\displaystyle\int_{|z-w|=R} \frac{1}{z}\,dz = 0$.

Problem 39 –
If $f(z)$ is a complex function, write it as $f(x,y) = u(x,y) + iv(x,y)$ where $z = x+iy$, $u(x,y) = \operatorname{Re} f(x+iy)$ and $v(x,y) = \operatorname{Im} f(x+iy)$. Thus we consider everything as a function of two real variables x and y.

(a) Show that if f is holomorphic then we have an equality of partial derviatives:
$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y} \qquad \text{and} \qquad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

(b) Suppose you know multivariable calculus (up to Green's theorem, or just look it up). Re-prove the Cauchy–Goursat theorem under the assumption that all the partial derivatives in the previous part are continuous (this is a stronger hypothesis than f just being holomorphic).

Problem 40 –
Suppose that $f(z)$ is an *analytic* function on an open set containing $z_0 \in \mathbf{C}$. Show that if $R > 0$ then
$$f(z_0) = \frac{1}{2\pi i} \int_{|z-z_0|=R} \frac{f(z)}{z-z_0}\,dz.$$
This is a good sanity check for the upcoming Cauchy integral formula.

Problem 41 –
One reason for developing path integrals is to justify certain calculations of real integrals. The goal of this problem is to discuss one such mild calculation. You may take for granted the "Gaussian integral" $\displaystyle\int_{-\infty}^{\infty} e^{-\pi x^2}\,dx = 1$. (This seems easiest to prove using methods of multi-variable calculus, though complex analytic proofs do exist via the "Γ-function"). A picture of the paths in (b)-(d) will be drawn in (on photo copies) below.

(a) Show that the function e^{-z^2} is analytic (and thus has an antiderivative) on all of $\mathbf{C}$.

(b) Let $[0,R]$ be the path in $\mathbf{C}$ connecting the origin to the point R on the real axis. Show that
$$\lim_{R\to\infty} \int_{[0,R]} e^{-z^2}\,dz = \frac{\sqrt{\pi}}{2}.$$

(c) Now let $\zeta_8 = e^{\pi i/4}$ be the primitive 8th root of unity with positive real and imaginary parts. Let S_R be the circular arc connecting the point R on the real axis to the point $R\zeta_8$ in the first quadrant. Show that
$$\lim_{R\to\infty} \int_{S_R} e^{-z^2}\,dz = 0.$$

(d) Let L_R be the straight line connecting the point $R\zeta_8$ in the first quadrant to the origin. Show that
$$\lim_{R\to\infty} \int_{L_R} e^{-z^2}\,dz = -\zeta_8 \int_0^{\infty} e^{-ix^2}\,dx.$$

(e) Compute $\displaystyle\int_0^{\infty} \sin(x^2)\,dx$ and $\displaystyle\int_0^{\infty} \cos(x^2)\,dx$.

Problem 42 –
We are going to have to deal with constructing new analytic functions out of old, so this exercise is meant to be a warning sign. I will continue with it during the next set.

(a) Let $f_n(x) = x^n$, for $0 \le x \le 1$ real. Show that for each x, $f(x) = \lim_{n\to\infty} f_n(x)$ exists but that $x \mapsto f(x)$ is not a continuous function. Express this as the disagreement of a double limit computed two different ways (e.g. see the second page of Homework 5).

(b) Thinking about the calculation of the limit implicit in (b) and the limit in (a), try to come up with a condition on a sequence of functions $\{f_n(x)\}$ defined on $[0,1]$ that would imply that $f(x) = \lim_{n\to\infty} f_n(x)$ defines a continuous function.

8. Lecture 8

Problem 43 –
The purpose of the next three exercises is to prove the fundamental theorem of algebra, since we don't have time lecture for this application. Let $r > 0$ be a real number, $z_0 \in \mathbf{C}$ and suppose that f is a holomorphic function on a disc that contains the circle $|z - z_0| = r$. Show that

$$\left|f^{(n)}(z_0)\right| \leq \frac{n!}{r^n} \cdot \max_{|z-z_0|=r} |f(z)| .$$

(Use the Cauchy formula for the coefficients of the Taylor series expansion of f at z_0).

Problem 44 –
Suppose that f is holomorphic on all of $\mathbf{C}$ and bounded, i.e. there exists a constant B such that $|f(z)| \leq B$ for each $z \in \mathbf{C}$. Show that f is constant. (Show that $f' = 0$ using the previous problem, you may use that $f' = 0$ if and only if f is a constant[8].)

Problem 45 –
Let $P(z) = a_n z^n + \cdots + a_1 z + a_0$ be a complex polynomial. Assume that $a_n \neq 0$.

(a) Show that there exists a real number $R > 0$ and a real number $c > 0$ such that if $|z| > R$ then $|P(z)| \geq c\,|z|^n$.
(b) Show that if $P(z)$ has no roots in $\mathbf{C}$ then $1/P(z)$ is a bounded holomorphic function.
(c) Show every non-constant polynomial has a complete set of roots in $\mathbf{C}$.

Problem 46 –
Suppose that $a_1, a_2, \ldots$ is a sequence of complex numbers which are bounded. Show that $\displaystyle\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ absolutely converges on $\mathrm{Re}(s) > 1$ and defines a holomorphic function there.

Problem 47 –
Suppose that $a_1, a_2, \ldots$ is a sequence of complex numbers and there exists a $c > 0$ such that for every $n \geq 1$, $|a_1 + \cdots + a_n| \leq c$. Show that $\displaystyle\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges to a holomorphic function[9] on $\mathrm{Re}(s) > 0$ (re-visit the sum by parts method from Lecture 5). Give an example where the sum is not absolutely convergent, somewhere.

Problem 48 –
Suppose that f is a non-vanishing holomorphic function on an open set U. Suppose also that U satisfies the property we had in class: it is connected by paths and the interior of any rectangle drawn in U is also in U.

(a) Show that there exists a holomorphic function $\log f$ on U such that $(\log f)'(z) = f'(z)/f(z)$ and $e^{\log f(z)} = f(z)$.
(b) Show that if L_f is any other holomorphic function on U such that $e^{L_f(z)} = f(z)$ then $L_f(z) = \log f(z) + 2\pi i m$ for some $m \in \mathbf{Z}$. (Hint: use the intermediate value theorem and the fact that U is connected by paths.)

We call $\log f(z)$ a logarithm for f on U. Because of part (c) there is no "the logarithm" but the ambiguity is concrete.

Problem 49 –
Let $U_1 = \mathbf{C} - \{x \in \mathbf{R} \colon x \leq 0\}$ and let $U_2 = \mathbf{C} - \{x \in \mathbf{R} \colon x \geq 0\}$.

(a) Convince yourself that U_1 and U_2 satisfy the hypotheses of the previous problem.
(b) Compute a logarithm for the function z on U_1 and then compute $\log(i)$ for this choice of logarithm.
(c) Compute a logarithm for the function z on U_2 and then compute $\log(i)$ for this choice of logarithm.
(d) Find the multiple of $2\pi i$ that your logarithms differ by on $V = \{z \in \mathbf{C} \colon \mathrm{Im}(z) > 0\}$.

---

[8] This is a property of functions on sets like $\mathbf{C}$ that cannot be disconnected by open sets. But for example if you take two disjoint open discs then the function that is 0 on one of them and 1 on the other is a non-constant holomorphic function whose derivative is zero.

[9] Added next day: You may have trouble justifying that it is holomorphic at this point. Don't worry about that.

9. Lecture 9

Problem 50 –
Suppose that $f_n(x) = \sqrt{x^2 + 1/n^2}$. We give an example of a limit of differentiable functions whose limit is not differentiable.

(a) Show that for each n, $f_n(x)$ is a differentiable function $\mathbf{R}$.
(b) Show that $|x| \leq f_n(x) \leq |x| + \frac{1}{n}$. Deduce that the limit
$$\lim_{n\to\infty} f_n(x) = |x|$$
converges at a rate independent of x.
(c) Is $z \mapsto \sqrt{z^2+1}$ holomorphic on $\mathbf{C}$? Why or why not?

Problem 51 –
(This should've been done a long time ago). Suppose that $z = x + iy$ and write also $z = re^{i\theta}$.

(a) Compute r and θ in terms of x and y. Now do the opposite.
(b) For each $X > 0$, draw a picture of the region
$$U = \left\{ z\colon \operatorname{Re}(z) > 0 \text{ and } \frac{|z|}{\operatorname{Re}(z)} < X \right\}$$
(c) Do you see that every $z \in \mathbf{C}$ with $\operatorname{Re}(z) > 0$ lies in some region U as in the previous part?

Problem 52 –
Suppose that $0 < a < b$ are two real numbers and let $z \in \mathbf{C}$ be such that $\operatorname{Re}(z) > 0$.

(a) Show $e^{-az} - e^{-bz} = z \displaystyle\int_a^b e^{-tz}\, dt$.
(b) Show that
$$\left|e^{-az} - e^{-bz}\right| \leq \frac{|z|}{\operatorname{Re}(z)}(e^{-a\operatorname{Re}(z)} - e^{b\operatorname{Re}(z)})$$
(c) Show that if n is an integer and $s \in \mathbf{C}$ then
$$\left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| \leq \frac{|s|}{\operatorname{Re}(s)}\left(\frac{1}{n^{\operatorname{Re}(s)}} - \frac{1}{(n+1)^{\operatorname{Re}(s)}}\right)$$

Problem 53 –
If $\pi = a + bi \in \mathbf{Z}[i]$ then remember we set $N(\pi) = a^2 + b^2 \in \mathbf{Z}$.

(a) Show that for every integer N there are at most finitely $\pi \in \mathbf{Z}[i]$ such that $N(\pi) \leq N$ and that if π and π' are associate[10] then $N(\pi) = N(\pi')$.
(b) Denote by $\mathbf{Z}[i]/\sim$ the elements of $\mathbf{Z}[i]$ up to associates. Make sense of the sum
$$\zeta_{\mathbf{Z}(i)}(s) := \sum_{\pi \in \mathbf{Z}[i]/\sim} \frac{1}{N(\pi)^s}.$$
Now show that it converges absolutely to a holomorphic function on $\operatorname{Re}(s) > 1$.
(c) Show that when $\operatorname{Re}(s) > 1$ then we have a factorization
$$\zeta_{\mathbf{Z}[i]}(s) = \zeta(s) \cdot L(s),$$
where $L(s) = \sum_n \chi_4(n)/n^s$ is the Dirichlet L-function we've seen in class (remember $\chi_4(n) = (-1)^{(n-1)/2}$). (You might want to prove a product formula for $\zeta_{\mathbf{Z}[i]}(s)$).

Problem 54 –
Let $(\mathbf{Z}/4\mathbf{Z})^\times$ be the set of units modulo 4 and let $\mathbf{C}^\times$ be the set of non-zero complex numbers

(a) Write down all the functions $\chi : (\mathbf{Z}/4\mathbf{Z})^\times \to \mathbf{C}^\times$ that satisfy the relationship $\chi(nm) = \chi(n)\chi(m)$.
(b) You maybe know what the Galois group $\operatorname{Gal}(\mathbf{Q}(i)/\mathbf{Q})$ of $\mathbf{Q}(i)$ over $\mathbf{Q}$ is, right? Discuss (with your friends, save the trees and save the trees, with your friends) your answer to part (a), the definitions of $\zeta(s)$ and $L(s)$ and the factorization in part (c) of the previous problem.

[10] Remember that means that π/π' is either ± 1 or $\pm i$.

10. Lecture 10

Problem 55 –
Suppose that G and H are groups and let $\widehat{(-)}$ denote the character group.

(a) Show that the map $\iota : G \hookrightarrow G \times H$ given by $g \mapsto (g, e_H)$ realizes G as a normal subgroup of $G \times H$. What is the quotient group?
(b) If χ is a character of $G \times H$ show that $\chi\big|_G(g) := \chi(\iota(g))$ defines a character of G.
(c) Construct an explicit isomorphism

$$\widehat{G} \times \widehat{H} \simeq \widehat{G \times H}.$$

(Note: I never said that G and H are finite. You'd better not count each side, in any case, since that would be circular with the next part[11]).
(d) Using what we said in class, show that if G is a finite abelian group then $\#G = \#\widehat{G}$.

Problem 56 –
Let G be a group, and $\widehat{\widehat{G}}$ be the character group of $\widehat{G}$. If $g \in G$ and $\chi \in \widehat{G}$, define $\varepsilon(g)(\chi) := \chi(g)$. Show that if G is abelian then

$$G \xrightarrow{\varepsilon} \widehat{\widehat{G}}$$

defines an injective group homomorphism. Show that if G is finite and abelian then ε is an isomorphism.

Problem 57 –
Write down the unique non-trivial character of $(\mathbf{Z}/3\mathbf{Z})^\times$ as a Legendre symbol.

Problem 58 –
Show that if χ is a character of $(\mathbf{Z}/m\mathbf{Z})^\times$ then χ is uniquely determined by the values $\chi(p \bmod m)$ where p runs through primes $p \nmid m$.

Problem 59 –
Write down all the characters of $(\mathbf{Z}/9\mathbf{Z})^\times$ and $(\mathbf{Z}/12\mathbf{Z})^\times$.

Problem 60 –
Write down an explicit character of $(\mathbf{Z}/42\mathbf{Z})^\times$ whose values on primes $p \neq 13$ is given by

$$p \mapsto \left(\frac{13}{p}\right).$$

Problem 61 –
Write down an explicit character of $(\mathbf{Z}/28\mathbf{Z})^\times$ whose values on primes $p \neq 7$ is given by

$$p \mapsto \left(\frac{7}{p}\right).$$

Problem 62 –
The definition of a character makes complete sense regardless of it G is abelian or finite or neither (see the first problem). However, in general one is interested in preserving certain extra structures. Re-define the characters of $\mathbf{R}$ to be

$$\widehat{\mathbf{R}} = \left\{\underline{\text{continuous}} \text{ characters } \chi : \mathbf{R} \to \mathbf{C}^\times\right\}.$$

(a) Show that if $\theta \in \mathbf{R}$ then $\psi_\theta(x) = e^{2\pi i x\theta}$ is an element of $\widehat{\mathbf{R}}$.
(b) When is ψ_θ the trivial character?
(c) Describe $\widehat{\mathbf{R}}$ as explicitly as you can (you will need to use the continuity assumption in a serious way at some point).

[11] It is also certainly possible to deduce part (d) without using the classification of finite abelian groups. In fact, the logic is sometimes reversed. This might appear on a future homework.

11. Lecture 11

Problem 63 –
Let G and G' be groups.

(a) Suppose $\varphi : G' \to G$ is a homomorphism of groups. Describe a natural group homomorphism
$$\widehat{\varphi} : \widehat{G} \to \widehat{G'}.$$
When $G' = H \subset G$ is a subgroup, note that the map $\widehat{G} \to \widehat{H}$ on dual groups is the "restriction map".

(b) If G is a finite abelian group, show the restriction map $\widehat{G} \to \widehat{H}$ is surjective and show that there is a natural isomorphism of groups $\widehat{G/H} \simeq \ker(\widehat{G} \to \widehat{H})$. (Hint: (a) should give you a natural map $\widehat{G/H} \to \widehat{G}$.)

Problem 64 –
Let G be a finite abelian group of order n. In class we showed that
$$\sum_{g \in G} \chi(g) = \begin{cases} n & \text{if } \chi \neq \mathbf{1} \\ 0 & \text{otherwise.} \end{cases}$$
Using this, and the isomorphism $G \simeq \widehat{\widehat{G}}$ (the dual of the dual) from the previous homework, give another argument that
$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} n & \text{if } g \neq 1 \\ 0 & \text{otherwise.} \end{cases}$$

Problem 65 (How to find primes in a given congruence class) –
Let $m \geq 1$, p be a prime $p \nmid m$ and $a \in (\mathbf{Z}/m\mathbf{Z})^\times$. Show that
$$\frac{1}{\phi(m)} \sum_{\chi \in \widehat{(\mathbf{Z}/m\mathbf{Z})^\times}} \overline{\chi}(a)\chi(p) = \begin{cases} 1 & \text{if } p \equiv a \bmod m \\ 0 & \text{otherwise.} \end{cases}$$
Here, and below, $\overline{\chi} = \chi^{-1}$ is the inverse character to χ.

Problem 66 –
Suppose that G is a finite abelian group of order n and $f : G \to \mathbf{C}$ is a function. We define a new function $\widehat{f}$ on the dual group $\widehat{f} : \widehat{G} \to \mathbf{C}$ by
$$\widehat{f}(\chi) := \frac{1}{\sqrt{n}} \sum_{g \in G} f(g)\overline{\chi}(g).$$
Show that
$$f(g) = \frac{1}{\sqrt{n}} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi(g).$$

Problem 67 –
Let $\chi : (\mathbf{Z}/3\mathbf{Z})^\times \to \mathbf{C}^\times$ be the unique non-trivial Dirichlet character modulo 3. We will show $L(1, \chi) \neq 0$. Recall that
$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

(a) Let $g(x) = \dfrac{1-x}{1-x^3}$. Describe $g(x)$ as an absolutely convergent sum on $|x| < 1$.

(b) If $0 \leq x < 1$ let
$$f(x) = \int_0^x g(t)\, dt.$$
Write $f(x)$ as an absolutely convergent sum on $|x| < 1$.

(c) Show that the summation formula for $f(x)$ converges at $x = 1$ and that $f(x)$ extends to a continuous function on $[0, 1]$ with $f(1) = L(1, \chi)$.

(d) Now compute $L(1, \chi)$ by computing $\lim_{x \to 1^-} f(x)$ by using the definition of $f(x)$ as an integral (you might want to simply $g(x)$ into lowest terms).

12. Lecture 12

Problem 68 –
If n is an integer we define a number $\mu(n)$, and call μ the Möbius function. It is defined as follows:

- If n is not square-free then $\mu(n) = 0$;
- If n is the product of k primes then $\mu(n) = (-1)^k$ (the integer $n = 1$ has $k = 0$ prime factors).

(a) Show that $\mu(n)$ is multiplicative but not strictly multiplicative.
(b) Show that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1. \end{cases}$$

(c) Show that $\mu(n)$ is the sum of the primitive nth roots of unity in the complex plane, i.e.

$$\mu(n) = \sum_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} e^{\frac{2\pi i k}{n}}$$

(Hint: the right hand side is related to a certain coefficient of the nth cyclotomic polynomial $\Phi_n(x)$)

Problem 69 –
If $a : \mathbf{N} \to \mathbf{C}$ is a function and $r \geq 0$ then we say $a(n)$ has polynomial growth of order r if there exists a constant C such that

$$|a(n)| \leq Cn^r$$

for all $n \geq 1$. For example, $a(n)$ is bounded if and only if it has polynomial growth of order zero.

As a reality check, show that $a(n)$ has polynomial growth of order r if and only if there exists an integer n_0 and a constant C such that if $n \geq n_0$ then $|a(n)| \leq Cn^r$.

Problem 70 –
For each of the following functions $a(n)$, show it is polynomial growth of some order. Describe the order as explicitly as you can. Which ones are multiplicative? Completely multiplicative?

(a) The trivial function $\mathbf{1}(n) = 1$ for all n.
(b) The Möbius function $\mu(n)$ defined above.
(c) The Dirac function $\delta(1) = 1$ and $\delta(n) = 0$.
(d) The k-power map $\iota_k(n) = n^k$.
(e) The logarithm $\log(n)$ (your answer shouldn't depend on the base (why not?) but to fix ideas, log means the natural logarithm)
(f) The Euler ϕ-function $\phi(n)$.
(g) The k-power divisor function $\sigma_k(n) = \sum_{d|n} d^k$.
(h) $\Lambda(n)$ defined by

$$\Lambda(n) = \begin{cases} \log(p) & \text{if } n \text{ is a power of a prime } p, \\ 0 & \text{otherwise.} \end{cases}$$

(i) $\lambda(n) := (-1)^{\Omega(n)}$ where $\Omega(n)$ is the number of prime factors of n, counted with multiplicity (e.g $\Omega(1) = 0$, $\Omega(2) = 1$ and $\Omega(2^{10}) = 10$).

Problem 71 –
Suppose that $a, b : \mathbf{N} \to \mathbf{C}$ are two functions. We define their convolution product $a * b$ as the function on the natural numbers given by

$$(a * b)(n) = \sum_{d|n} a(d)b(n/d).$$

(a) Compute $\mathbf{1} * \mathbf{1}$, $\mu * \mathbf{1}$, $\iota_k * \mathbf{1}$, $\phi * \mathbf{1}$, $\Lambda * \mathbf{1}$ in terms of the functions above.
(b) Let $\mathbf{N}^{\mathbf{C}}$ be the set of functions $a : \mathbf{N} \to \mathbf{C}$. Show that if we equip $\mathbf{N}^{\mathbf{C}}$ with addition given pointwise and multiplication given by the convolution product then it becomes a commutative ring. What is the identity?
(c) Show that if $a \in \mathbf{N}^{\mathbf{C}}$ and $b(n) = \sum_{d|n} a(d)$ then $a = \mu * b$ (Möbius inversion).

Problem 72 –
Suppose $r \geq 0$.

(a) Show by example that if a, b are two functions with polynomial growth of order r then $a * b$ need not have polynomial growth of order r.

(b) But, do show that if a, b have polynomial growth of order r then $a * b$ has polynomial growth of order $r + \varepsilon$ for all $\varepsilon > 0$.

Problem 73 –
If $a : \mathbf{N} \to \mathbf{C}$ is a function then we define its Dirichlet series as in lecture with

$$D(a, s) = \sum_{n \geq 1} \frac{a(n)}{n^s}$$

as a formal power series (for the moment).

(a) Show that if $a(n)$ has polynomial growth of order r then $D(a, s)$ absolutely converges to a holomorphic function in the right half plane $\mathrm{Re}(s) > r + 1$ and if $a(n)$ is strictly multiplicative then $D(a, s)$ has an Euler product expansion

$$D(a, s) = \prod_p \frac{1}{1 - \frac{a(p)}{p^s}}$$

on $\mathrm{Re}(s) > r + 1$.

(b) Show that if a, b both have polynomial growth of order r then we have identities of holomorphic functions

$$D(a + b, s) = D(a, s) + D(b, s) \text{ and } D(a * b, s) = D(a, s)D(b, s).$$

on $\mathrm{Re}(s) > r + 1$. Be sure to justify why each function converges there (especially the Dirichlet series of the convolution!)

(c) Prove the following identities (and give the right half planes they are valid on)

$$\begin{aligned} D(\mathbf{1}, s) &= \zeta(s) \\ D(\mu, s) &= 1/\zeta(s) \\ D(\iota_k, s) &= \zeta(s - k) \\ D(\log, s) &= -\zeta'(s) \\ D(\phi, s) &= \zeta(s - 1)/\zeta(s) \\ D(\sigma_k, s) &= \zeta(s)\zeta(s - k) \\ D(\Lambda, s) &= -\zeta'(s)/\zeta(s) \\ D(\lambda, s) &= \zeta(2s)/\zeta(s). \end{aligned}$$

(The derivatives are derivatives with respect to s).

(d) Wax poetic about the failure of the $\log(n)$ to be multiplicative to the fact that $D(\log, s)$ is a derivative of an Euler product, not an Euler product itself.

(e) Do any of the Dirichlet series in part (c) extend to a region beyond their half plane of absolute convergence? (Note: the series could converge without the identity remaining valid.)

Problem 74 –
This is a continuation of the previous part.

(a) Fix $r \geq 0$ and suppose that a has polynomial growth of order r. Show that $D(a, s) = 0$ if and only if $a = 0$. (This is analogous the rigidity property of analytic functions that we saw.)

(b) Use Dirichlet series to show that if a has polynomial growth r then

$$\mu * (a * \mathbf{1}) = a.$$

13. Lecture 13

Problem 75 –
Let $\chi : (\mathbf{Z}/8\mathbf{Z})^\times \to \mathbf{C}^\times$ be the quadratic character whose values are given by $\chi(3) = \chi(5) = -1$. Finish the calculation of $L(1,\chi)$ that we started in class by evaluating

$$L(1,\chi) = \int_0^1 \frac{1-x^2}{1+x^4}\, dx.$$

Problem 76 –
Generalize the technique in Problem 75, or what we've done in class, to compute $L(1,\chi)$ when χ is the non-trivial character χ modulo 5 such that $\chi^2 = 1$.

Problem 77 –
Suppose that χ mod m is a Dirichlet character such that $\chi^2 = 1$. Discuss your expectation for the "shape" of $L(1,\chi)$ depending on whether $\chi(-1) = 1$ or $\chi(-1) = -1$.

Problem 78 –
Compare your answer in Problems 75 and 77 to integral solutions to the Pell equations $x^2 - 2y^2 = \pm 4$ and $x^2 - 5y^2 = \pm 4$. Find another quadratic character χ with $\chi(-1) = 1$, compute $L(1,\chi)$ and see if you can find a pattern. Can you come up with a good reason why it is important for $\chi(-1) = 1$, rather than $\chi(-1) = -1$?

Problem 79 –
If $m \geq 1$, show that the Dirichlet series $\sum_{\gcd(n,m)=1} n^{-s\phi(m)}$ and $\zeta_m(s)$ do not converge at $s = 1/\phi(m)$.

Problem 80 –
Let $\Phi_3(x) = x^2 + x + 1$ be the 3rd cyclotomic polynomial and let $\zeta_3(s)$ be the zeta function as in class.

(a) For each prime $p \nmid 3$, compute $f(p)$ and $g(p)$ with respect to the modulus 3, i.e. $f(p)$ and $g(p)$ appear in the pth Euler factor $(1 - p^{-f(p)s})^{g(p)}$ of $\zeta_3(x)$.

(b) Make a table that lists for each prime $p \nmid 3$, whether $\Phi_3(x) \bmod p \in \mathbf{F}_p[x]$ is irreducible or not and compare with (a).

Problem 81 –
And now for something completely different. If p is a prime, let $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ be the finite field with p elements.

(a) Show that if $a, b \in \mathbf{F}_p^\times$ are not squares then a/b is a square.

(b) If a is not a square, let $\sqrt{a}$ be a formal symbol satisfying $\sqrt{a}^2 = a$. Then set

$$\mathbf{F}_p(\sqrt{a}) = \left\{x + y\sqrt{a} \colon x, y \in \mathbf{F}_p\right\}.$$

Define addition and multiplication in the obvious way. Show that $\mathbf{F}_p(\sqrt{a})$ is a field of size p^2.

(c) Show that if $a, b \in \mathbf{F}_p^\times$ then $\mathbf{F}_p(\sqrt{a}) \simeq \mathbf{F}_p(\sqrt{b})$. Any field of size p^2 is of the form[12] $\mathbf{F}_p(\sqrt{a})$ and we write this common field as $\mathbf{F}_{p^2}$.

Problem 82 –
This is a generalization of Problem 80, and returns to Problem 21. Recall that the 5th cyclotomic polynomial is $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$.

(a) Make a table that lists for each prime $p \nmid 5$, the values $f(p)$ and $g(p)$ so that the pth Euler factor of the zeta function $\zeta_5(x)$ is $(1 - p^{-f(p)s})^{g(p)}$.

(b) Let $\Psi_5(x) = x^2 + x - 1$. Let $\alpha, \beta \in \mathbf{F}_{p^2}$ be two roots. Show that $\Phi_5(x) = (x^2 - \alpha x + 1)(x^2 - \beta x + 1)$.

(c) Show that $\alpha, \beta \in \mathbf{F}_p$ if and only if $p \equiv \pm 1 \bmod 5$.

(d) Show that if $p \equiv -1 \bmod 5$ then $x^2 - \alpha x + 1$ is irreducible over $\mathbf{F}_p$ and that if $p \equiv 2, 3 \bmod 5$ then $x^2 - \alpha x + 1$ is irreducible over $\mathbf{F}_{p^2}$ (Hint: A root z of $x^2 - \alpha x + 1$ is a 5th root of unity, but the multiplicative group $\mathbf{F}_p^\times$ (resp. $\mathbf{F}_{p^2}^\times$) has order $p - 1$ (resp. $p^2 - 1$)).

(e) Compare part (a) with the way $\Phi_5(x)$ factors over $\mathbf{F}_p$ into irreducible factors (for $p \nmid 5$).

Problem 83 –
Make a conjecture about the factorization of $\Phi_7(x)$ modulo p for primes $p \nmid 7$. Prove as much as you can. What about $\Phi_{11}(x)$? $\Phi_{13}(x)$?

---

[12] If $\mathbf{F}$ is any field extension of $\mathbf{F}_p$ with p^2 elements then $\mathbf{F}$ is a two-dimensional vector space over $\mathbf{F}_p$. Thus there exists $z \neq 0$ in $\mathbf{F}$, such that 1 and z are linearly independent, but $1, z$ and z^2 are linearly dependent. In particular, z must satisfy a quadratic equation over $\mathbf{F}_p$ and thus $\mathbf{F}$ is obtained by adjoining a square root.

14. Lecture 14

Problem 84 –
Prove the result mentioned and used in class: if $f(s) = \sum a_n n^{-s}$ is a Dirichlet series and it converges at $s = s_0$. Show that $f(s)$ converges and is a holomorphic function on $\mathrm{Re}(s) > \mathrm{Re}(s_0)$.

Problem 85 –
Show that

$$\log(1/(1-z)) = \sum_n \frac{z^n}{n}$$

is a logarithm for $f(z) = 1/(1-z)$ on the open disc $|z| < 1$. (By Problem 48 it's enough to check the series is holomorphic on $|z| < 1$ and exponentiates to give the correct answer and once you know the analyticity, it's enough to check on real numbers[13]).

Problem 86 –
The goal of this (long) problem is to show that if $\chi \bmod m$ is any Dirichlet character (*including* $\chi = \mathbf{1}_m$) and $s \neq 1$, but $\mathrm{Re}(s) = 1$ then $L(s,\chi) \neq 0$. It is an application of Landau's theorem and as a consolation for our pain, the case where $\chi = \mathbf{1}$, so $L(s,\chi) = \zeta(s)$, is an important step in the prime number theorem. There are also other proofs of that specific result. We let $\chi \bmod m$ be a Dirichlet character.

(a) Remind yourself how to make sense of $L(s, \mathbf{1}_m)$ when $s \neq 1$ but $\mathrm{Re}(s) > 0$ (remember the first thing we proved about $\zeta(s)$ was something about $\zeta(s) - 1/(s-1)$).

(b) Now suppose that $t \in \mathbf{R}$ is non-zero and we will consider complex numbers $1 + it$ lying on $\mathrm{Re}(s) = 1$. We know from class (or the previous part) that $L(1+it,\chi)$ is a finite number. Show that if $L(1+it,\chi) = 0$ then $L(1-it,\overline{\chi}) = 0$.

(c) Set

$$\Xi(s) = \zeta(s)^2 L(s+it,\chi) L(s-it,\overline{\chi})$$

and expand it out on $\mathrm{Re}(s) > 1$ as a Dirichlet series $\Xi(s) =: \sum_{n\geq 1} a_n n^{-s}$. That is, the a_n are defined as whatever shows up when you expand the products[14]. Show that if $L(1+it,\chi) = 0$ then $\Xi(s)$ extends to a holomorphic function on $\mathrm{Re}(s) > 0$.

(d) Landau's theorem is about Dirichlet series with nonnegative real coefficients, so the next four parts are to show that $\Xi(s)$ has that property. Show that $n \mapsto a_n$ is a multiplicative function of n. Is it strictly multiplicative? (Why should it be?) Deduce that it is enough to show that a_{p^r} is a real number ≥ 0 for each prime p and integer $r \geq 1$.

(e) Let $\varepsilon(p) = \chi(p)p^{-it}$ and $\overline{\varepsilon}(p) = \overline{\chi}(p)p^{it}$ be its conjugate. Go back and actually check that the a_{p^r} are defined explicitly as

$$1 + \frac{a_p}{p^s} + \frac{a_{p^2}}{p^{2s}} + \cdots = \left(\frac{1}{1-\frac{1}{p^s}}\right)^2 \left(\frac{1}{1-\frac{\varepsilon(p)}{p^s}}\right)\left(\frac{1}{1-\frac{\overline{\varepsilon}(p)}{p^s}}\right).$$

Make sure to justify your (re)ordering of the summations.

(f) Using the series expansion of $\log(1/(1-z))$ on $|z| < 1$, deduce that

$$1 + \frac{a_p}{p^s} + \frac{a_{p^2}}{p^{2s}} + \cdots = \exp\left(\sum_{k=1}^{\infty} \frac{2 + \varepsilon(p)^k + \overline{\varepsilon}(p)^k}{kp^{ks}}\right).$$

Show that that $2 + \varepsilon(p)^k + \overline{\varepsilon}(p)^k$ is a non-negative real number. (Here $\exp(z)$ means e^z).

(g) Conclude that for each prime p and $r \geq 1$, a_{p^r} is real and $a_{p^r} \geq 0$ for each r.

(h) Go back and actually expand out the exponential to see that $a_{p^2} \geq 1$ for each prime p.

(i) Show that the infinite series of real numbers $\sum_n a_n n^{-1/2}$ does not converge by comparing with $\sum_p a_{p^2}/p$ and thus $\sum 1/p$.

(j) Piece together all the previous parts to conclude that $L(1+it,\chi) \neq 0$. Carefully point out where you used $t \neq 0$, if you did at all.

---

[13] Why?

[14] By the way, why can you expand them and rearrange again?

15. Lecture 15

Problem 87 –
Find an explicit infinite list of primes p such that $x^2 - 35 \bmod p$ has no solution.

Problem 88 –
Suppose that ℓ is an odd prime. Show that the function $\chi_\ell(a) := (-1)^{\frac{\ell-1}{2}\cdot\frac{a-1}{2}}\left(\frac{a}{\ell}\right)$ defines a Dirichlet character modulo 4ℓ and it is the unique character modulo 4ℓ such that $\chi_\ell(p) = \left(\frac{\ell}{p}\right)$ for all primes $p \nmid 4\ell$.

Problem 89 –
Generalize the previous problem as follows. Show that if $d \in \mathbf{Z}$ is a non-zero square free integer (possibly negative) and $m = 4\,|d|$ then there exists a unique Dirichlet character χ_d mod m such that

$$\chi_d(p) = \left(\frac{d}{p}\right)$$

for all primes $p \nmid m$. Show that $\chi_d^2 = 1$ and $\chi_d \neq 1$ except if $d = 1$.

Problem 90 – (a) Suppose that $m \geq 1$ and $H \subset (\mathbf{Z}/m\mathbf{Z})^\times$ is a subgroup. Show that the set of primes p such that $p \in H$ has Dirichlet density $((\mathbf{Z}/m\mathbf{Z})^\times : H)^{-1}$.

(b) Let $a \in \mathbf{Z}$ be a non-square. Show that $\{p\colon x^2 \equiv a \bmod p\}$ is a set of Dirichlet density $\frac{1}{2}$ (you might consider $\ker(\chi_a)$?)

Problem 91 –
Suppose that p is an odd prime, $\zeta_p = e^{2\pi i/p}$ be a primitive pth root of unity and $\tau = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_p^a$. This is an example of a Gauss sum which you might have seen before. Our goal is to show $\tau^2 = p^*$ where $p^* = (-1)^{\frac{p-1}{2}}p$.

(a) First show that $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$ (either by hand or using orthogonality and $\left(\frac{a}{p}\right) = \chi_{p^*}$).

(b) Next show that

$$\tau^2 = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\sum_{b=1}^{p-1}\zeta_p^{(1+a)b}.$$

(c) Evaluate the inner sum as a geometric sum and show that $\tau^2 = p^*$.

Problem 92 –
Let $\mathbf{Q}(\zeta_m)$ be the mth cyclotomic field, i.e. the field obtained by adjoining a primitive mth root of unity to $\mathbf{Q}$. We will show that every quadratic extension of $\mathbf{Q}$ is contained within such a field. (This is special case of a deeper result known as Kroenecker–Weber).

(a) Show that $\sqrt{2} \in \mathbf{Q}(\zeta_8)$ and $\sqrt{-1} \in \mathbf{Q}(\zeta_4)$.

(b) If p is prime show that $p^* := (-1)^{\frac{p-1}{2}}p$ lies in $\mathbf{Q}(\zeta_p)$.

(c) Show that if d is a square-free integer then $\sqrt{d} \in \mathbf{Q}(\zeta_m)$ for some m and, more precisely, $\sqrt{d} \in \mathbf{Q}(\zeta_{|d|})$ if $d \equiv 1 \bmod 4$ and $\sqrt{d} \in \mathbf{Q}(\zeta_{4|d|})$ if $d \equiv 2, 3 \bmod 4$.

Problem 93 –
Let[15] p be an odd prime and let $p^* = (-1)^{\frac{p-1}{2}}p$. Fix also a primitive pth root of unity $\zeta_p = e^{2\pi i/p}$. Using ζ_p we define an isomorphism $(\mathbf{Z}/p\mathbf{Z})^\times \xrightarrow{\cong} \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ by sending j to $\sigma_j(\zeta_p) = \zeta_p^j$. Recall we also have a Dirichlet character χ_{p^*} defined modulo p.

(a) Let τ be as above. Show that $\sigma_b(\tau) = \chi_{p^*}(b^{-1})\tau$.

(b) Under the isomorphism above, we can make sense of $\chi_{p^*}(\sigma)$ for $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. Show that

$$\ker(\chi_{p^*}) = \{\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})\colon \sigma(\tau) = \tau\} = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}(\sqrt{p^*})).$$

(c) Show that $\mathbf{Q}(\sqrt{p^*})$ is the unique quadratic subfield of $\mathbf{Q}(\zeta_p)$. (Hint: how many quadratic characters of $(\mathbf{Z}/p\mathbf{Z})^\times$ are there?)

[15] You can also save this for after you learn more about Galois groups in the other advanced seminar.