MATH 311/521, FALL 2025 PRACTICE FINAL

DECEMBER 15

Each problem is worth 10 points.

Problem 1. Let $q_e(n)$ and $q_o(n)$ be the number of partitions of n into an even or odd number of distict parts. Give a proof of Euler's identity

$$q_e(n) - q_o(n) = \begin{cases} (-1)^j & n = \frac{3j^2 \pm j}{2} \\ 0 & \text{otherwise} \end{cases}.$$

Hence or otherwise, conclude the formal product identity

$$\phi(x) = \prod_{n=1}^{\infty}(1 - x^n) = 1 + \sum_{j=1}^{\infty}(-1)^j \left(x^{\frac{3j^2+j}{2}} + x^{\frac{3j^2-j}{2}}\right).$$

Solution. See the course text, p.448.

Problem 2.

a. Define the abscissa of convergence of a Dirichlet series $F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$.

b. Let $\mu(n)$ be the Möbius function of n, $d(n)$ the number of divisors of n, and $\sigma(n)$ the sum of the divisors of n. Express $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$, $\sum_{n=1}^{\infty} \frac{d(n)}{n^s}$, $\sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s}$ as Euler products, and in terms of $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, and determine the abscissa of convergence of each series.

c. (Extra credit) Recall that a finite abelian group is isomorphic to a group of form $\bigoplus_p \mathbb{Z}/p^{a_1}\mathbb{Z} \oplus \mathbb{Z}/p^{a_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{a_k}\mathbb{Z}$ where $a_1 \geq a_2 \cdots \geq a_k > 0$. How many isomorphism classes of abelian groups of order p^k exist for p prime? Let $q(n)$ be the number of isomorphism classes of abelian groups of order n. Express $\sum_{n=1}^{\infty} \frac{q(n)}{n^s}$ as an Euler product and in terms of the Riemann zeta function.

Solution. a. The abscissa of absolute convergence of a Dirichlet series is a real number c so that $\sum_n |a_n|/n^s$ converges for $s > c$ and diverges for $s < c$.

b. All three functions are multiplicative, so the Euler products are determined on prime powers. For μ, $\mu(p) = -1$ and $\mu(p^k) = 0$ for $k \geq 2$, so $\sum_n \frac{\mu(n)}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right) = \zeta(s)^{-1}$. The abscissa of absolute convergence is 1 as it is for ζ (which is determined by the p-test for series). We have $d(p^k) = k+1$ so $\sum_n \frac{d(n)}{n^s} = \prod_p \left(\sum_{k=0}^{\infty} \frac{k+1}{p^{ks}}\right) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-2} = \zeta(s)^2$. The abscissa of absolute convergence is again 1 from the theorem on products of series. We have $\sigma(p^k) = p^k + p^{k-1} + \cdots + 1 = \frac{p^{k+1}-1}{p-1}$ so the Euler product is given by

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

Since $n \leq \sigma(n) \leq d(n)n$, the abscissa of absolute convergence is 2.

c. We have $q(p^k) = p(k)$, the number of partitions of k. It follows

$$\sum_{k=0}^{\infty} \frac{q(p^k)}{p^{ks}} = \sum_{k=0}^{\infty} \frac{p(k)}{p^{ks}} = \prod_{k=1}^{\infty} \left(1 - p^{ks}\right)^{-1}$$

and thus the Dirichlet series is $\prod_{n=1}^{\infty} \zeta(ns)$. The abscissa of absolute convergence is one.

Problem 3. The Bernoulli numbers (B_k) are defined by

$$\frac{x}{e^x-1} = 1 - \frac{x}{2} + \sum_{k=1}^{\infty}(-1)^{k+1}B_k\frac{x^{2k}}{(2k)!}.$$

a. Calculate B_1, B_2, B_3.

b. Take logarithmic derivatives in the product $\sin z = z\prod_{n=1}^{\infty}\left(1-\frac{z^2}{n^2\pi^2}\right)$ to conclude

$$z\cot z = 1 + 2\sum_{n=1}^{\infty}\frac{z^2}{z^2-n^2\pi^2} = 1 - 2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{z^{2k}}{n^{2k}\pi^{2k}}.$$

c. Prove $\zeta(2k) = \frac{2^{2k-1}\pi^{2k}}{(2k)!}B_k$.

Solution. a. Write

$$\begin{aligned}\frac{x}{e^x-1} + \frac{x}{2} &= \frac{x}{2}\frac{e^{\frac{x}{2}}+e^{-\frac{x}{2}}}{e^{\frac{x}{2}}-e^{-\frac{x}{2}}}\\ &= \frac{1+(\frac{x}{2})^2/2!+(\frac{x}{2})^4/4!+(\frac{x}{2})^6/6!+...}{1+(\frac{x}{2})^2/3!+(\frac{x}{2})^4/5!+(\frac{x}{2})^6/7!+...}\\ &= 1 + B_1x^2/2! - B_2x^4/4! + B_3x^6/6! + ...\end{aligned}$$

Matching up powers of x in

$$\begin{aligned}&1+\left(\frac{x}{2}\right)^2/2!+\left(\frac{x}{2}\right)^4/4!+\left(\frac{x}{2}\right)^6/6!+...\\ &=\left(1+\left(\frac{x}{2}\right)^2/3!+\left(\frac{x}{2}\right)^4/5!+\left(\frac{x}{2}\right)^6/7!+...\right)\\ &\times\left(1+B_1x^2/2!-B_2x^4/4!+B_3x^6/6!+...\right)\end{aligned}$$

gives

$$\begin{aligned}\frac{1}{2^2 2!} &= \frac{1}{2^2 3!} + \frac{B_1}{2!}\\ \frac{1}{2^4 4!} &= \frac{1}{2^4 5!} + \frac{B_1}{2^2 3! 2!} - \frac{B_2}{4!}\\ \frac{1}{2^6 6!} &= \frac{1}{2^6 7!} + \frac{B_1}{2^4 5! 2!} - \frac{B_2}{2^2 3! 4!} + \frac{B_3}{6!}\end{aligned}$$

or $B_1 = \frac{1}{6}, B_2 = \frac{1}{30}, B_3 = \frac{1}{42}$.

b. $\log \sin z = \log z + \sum_n \log(1 - \frac{z^2}{n^2\pi^2})$ so

$$\frac{\cos z}{\sin z} = \frac{1}{z} - \sum_n \frac{\frac{2z}{n^2\pi^2}}{1 - \frac{z^2}{n^2\pi^2}}.$$

The first formula for $z \cot z$ follows, and the second is reached on expanding the geometric series for $\frac{1}{1-\frac{z^2}{n^2\pi^2}}$.

c. In the previous expression, execute the sum over n to collect

$$z \cot z = 1 - 2\sum_{k=1}^{\infty} \frac{z^{2k}}{\pi^{2k}}\zeta(2k).$$

We now match this up with $\frac{x}{e^x-1} + \frac{x}{2}$ at $x = 2iz$,

$$\frac{x}{e^x - 1} + \frac{x}{2} = \frac{x}{2}\frac{e^{\frac{x}{2}} + e^{-\frac{x}{2}}}{e^{\frac{x}{2}} - e^{-\frac{x}{2}}} = z \cot z,$$

so

$$1 + \sum_{k=1}^{\infty}(-1)^{k+1}\frac{(2iz)^{2k}}{(2k)!}B_k = 1 - 2\sum_{k=1}^{\infty} \frac{z^{2k}}{\pi^{2k}}\zeta(2k).$$

Equating coefficients on z^{2k} gives $\zeta(2k) = \frac{2^{2k-1}\pi^{2k}}{(2k)!}B_k$.

Problem 4. Prove a number n is coprime to q if $\sum_{d|\mathrm{GCD}(n,q)} \mu(d) = 1$, and that the sum is zero otherwise. Using this, prove

$$\#\{M \leq n < M+N, \mathrm{GCD}(n,q) = 1\} = \frac{\phi(q)}{q} N + O(2^{\omega(q)})$$

where ϕ is Euler's ϕ function and $\omega(q)$ is the number of distinct primes that divide q.

Solution. Let $m = \mathrm{GCD}(n, q)$. Then $\sum_{d|m} \mu(d)$ is 1 if $m = 1$ and 0 if $m > 1$. The count required now is

$$\sum_{M \leq n < M+N} \sum_{d|\mathrm{GCD}(n,q)} \mu(d) = \sum_{d|q} \mu(d) \sum_{M \leq dn < M+N} 1.$$

The last sum is $\frac{N}{d} + O(1)$ so the count is

$$N \sum_{d|q} \frac{\mu(d)}{d} + \sum_{d|q, \mu(d) \neq 0} O(1) = \frac{\phi(q)}{q} N + O(2^{\omega(q)}).$$

Problem 5. Let

$$\chi_4(n) = \begin{cases} 1 & n \equiv 1 \bmod 4 \\ -1 & n \equiv 3 \bmod 4 \\ 0 & \text{otherwise} \end{cases},$$

$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, $L(s, \chi_4) = \sum_{n=1}^{\infty} \frac{\chi_4(n)}{n^s}$. The Dedekind zeta function for $\mathbb{Q}(i)$ is

$$\zeta_{\mathbb{Q}(i)}(s) = \zeta(s)L(s, \chi_4) = \sum_{m=1}^{\infty} \frac{r(m)}{m^s}.$$

Prove $r(m) = \#\{x, y \in \mathbb{Z}, x \geq 0, y > 0, x^2 + y^2 = m\}$.

Proof. The norm of an integer $x + iy$ in $\mathbb{Z}[i]$ is $N(x + iy) = x^2 + y^2$. Since the units of $\mathbb{Z}[i]$ are $1, i, -1, -i$, every non-zero integer in $\mathbb{Z}[i]$ is associated by multiplication by unit to a unique representative $x+iy$ with $x \geq 0, y > 0$, so the count $\#\{x, y \in \mathbb{Z}, x \geq 0, y > 0, x^2 + n^2 = m\}$ is exactly the number of integers of $\mathbb{Z}[i]$ of norm m, taken modulo multiplication by units. (Remark: $\mathbb{Z}[i]$ is a principle ideal domain, so this is the same as the number of ideals of norm m in the ring of integers.) By our discussion of unique factorization into primes for $\mathbb{Z}[i]$, the primes of $\mathbb{Z}[i]$ are as follows: ramified primes $(1+i)$, with $(1+i)|2$, split primes $\pi\overline{\pi} = p$ when $p \equiv 1 \bmod 4$, these have norm p, and inert primes $p \equiv 3 \bmod 4$, which have norm p^2. As the norm is multiplicative, to gain an integer of norm

$$m = 2^a \prod_{p \equiv 1 \bmod 4} p^\alpha \prod_{q \equiv 3 \bmod 4} q^\beta$$

we must have $\beta = 2\beta'$ even and

$$x + iy = \epsilon(1 + i)^a \prod_{p \equiv 1 \bmod 4} \pi^{\alpha_1}\overline{\pi}^{\alpha - \alpha_1} \prod_{q \equiv 3 \bmod 4} q^{\beta'}$$

where ϵ is a unit and α_1 may be chosen in $\alpha + 1$ ways. This proves a theorem from early in the class on the number of ways of representing a number m as the sum of two squares. We now check that the Euler products match up. At 2 the local factor comes from ζ and is $(1 + 2^{-s} + 2^{-2s} + ...)$ which reflects that there is one way to express a power of 2 as a sum of two squares. At

$p \equiv 1 \bmod 4$ the local factor is

$$(1 + p^{-s} + p^{-2s} + ...)^2 = (1 + 2p^{-s} + 3p^{-2s} + 4p^{-3s} + ...)$$

which agrees with the number of choices of α_1, and at $p \equiv 3 \bmod 4$ this is $(1 - p^{-s} + p^{-2s} - p^{-3s} + ...)(1 + p^{-s} + p^{-2s} + ...) = (1 + p^{-2s} + p^{-4s} + p^{-6s} + ...)$ which again agrees.

$\square$

Problem 6. Let $q = p^r$ be a power of a prime and let $\mathbb{F}_q$ be a finite field having q elements.

a. Prove $\mathbb{F}_q$ has characteristic p, that is, if $x \in \mathbb{F}_q$ then $p \cdot x = 0$ for all x, and hence conclude $\mathbb{F}_q$ has $\mathbb{F}_p$ as a subfield.
b. Conclude $\mathbb{F}_q^\times = \{a \in \mathbb{F}_q, a \neq 0\}$ is a multiplicative group, and hence conclude that for all $a \neq 0$, $a^{q-1} = 1$ in $\mathbb{F}_q$. Conclude $x^q - x = \prod_{a \in \mathbb{F}_q}(x - a)$ and that all fields of order q are isomorphic.
c. (Extra credit) For $a \in \mathbb{F}_q^\times$, let $\mathrm{ORD}(a)$ be the least positive n so that $a^n = 1$. For $d|q-1$ let $f(d) = \#\{a \in \mathbb{F}_q^\times : \mathrm{ORD}(a) = d\}$, $g(d) = \#\{a \in \mathbb{F}_q^\times : a^d = 1\}$. Prove $g(d) = \sum_{k|d} f(k)$ and thus $f(d) = \sum_{k|d} \mu(k)\frac{d}{k}$. Conclude $\mathbb{F}_q^\times$ has elements of order $q-1$, and hence is a cycle group.

Solution. a. Evidently $k \cdot 1 = 1 + 1 + ... + 1$ k times is eventually 0, since there are only finitely many elements in the field. The number must be a prime, or else the field would have a zero divisor, so $p \cdot 1 = 0$. The claim follows. The subfield may be taken to be the elements $0, 1, 2, ..., p-1$ defined this way.

b. Since there are not zero-divisors, multiplication by a non-zero $a \in \mathbb{F}_q^\times$ permutes the elements of $\mathbb{F}_q^\times$, so a has a multiplicative inverse. The associativity follows from the multiplication in the field, and a field always has a 1, so $\mathbb{F}_q^\times$ is a multiplicative group. Since the order of an element divides the order of a group, $a^{q-1} = 1$. In a field $x^q - x = 0$ has no more than q solutions, and there is division of polynomials with remainder, so $x^q - x$ has each field element as a root exactly once and these are all of the roots, this gives the factorization. We have $\mathbb{F}_q$ is a splitting field for $x^q - x$ over the subfield $\mathbb{F}_p$, which uniquely determines the field as $\mathbb{F}_p[x]/(Q(x))$ for an irreducible polynomial $Q(x)$ of degree r which necessarily divides $x^q - x$.

c. We evidently have $g(d) = \sum_{k|d} f(k)$, so the claim follows if we establish $g(d) = d$ by Möbius inversion. Obviously $a^d - 1$ has at most d solutions and when $d|(q-1)$, $x^{q-1} = 1$ has exactly $q-1$ solutions. The map $x \mapsto x^{\frac{q-1}{d}}$ on $\mathbb{F}_q^\times$ is at most $\frac{q-1}{d}$-to-1, and in fact has to be exactly this multiplicity for there to be enough roots of $x^{q-1} = 1$. The image provides the required d solutions to $x^d = 1$. Now $f(q-1) = (q-1)\sum_{k|q-1} \frac{\mu(k)}{k} > 0$.