18.785 Number Theory **Fall 2025**

Problem Set #9 **Due: 11/19/2025**

Description

These problems are related to Lectures 16–17. Your solutions should be written up in latex and submitted as a pdf-file to Gradescope by midnight on the date due.

Instructions: Solve Problem 0, then pick any combination of problems that sum to 100 points. Collaboration is permitted/encouraged, but you must identify your collaborators (including any LLMs you consulted) and any references you consulted outside the course syllabus. Include this information after the **Collaborators/Sources** prompt at the end of the problem set (if there are none, you should enter "none", do not leave it blank). Note that each student is expected to write their own solutions; it is fine to discuss problems with others, but your writing must be your own.

Problem 0.

These are warm-up problems that do not need to be turned in.

(a) In class we gave an elementary proof that $\vartheta(x) = O(x)$. Give a similarly elementary proof that $x = O(\vartheta(x))$ (both bounds were proved by Chebyshev before the PNT).

(b) Prove the Möbius inversion formula, which states that if f and g are functions $\mathbb{Z}_{\geq 1} \to \mathbb{C}$ that satisfy $g(n) = \sum_{d|n} f(d)$ then $f(n) = \sum_{d|n} \mu(d)g(n/d)$, where $\mu(n) := (-1)^{\#\{p|n\}}$ if n is squarefree and $\mu(n) = 0$ otherwise.

Problem 1. The zeta function of $\mathbb{F}_q[t]$ (49 points)

Recall that for a number field K, the Dedekind zeta function $\zeta_K(s)$ is defined by

$$\zeta_K(s) := \sum_I \mathrm{N}(I)^{-s},$$

where I ranges over nonzero ideals of $\mathcal{O}_K$ and $\mathrm{N}(I)$ is the absolute norm, which is just the cardinality of the residue field $\mathcal{O}_K/\mathfrak{p}$ when I is a prime ideal $\mathfrak{p}$.

The definition of $\mathrm{N}(\mathfrak{p}) := \#\mathcal{O}_K/\mathfrak{p}$ as the cardinality of the residue field makes sense in any global field and extends multiplicatively to all $\mathcal{O}_K$-ideals. In this problem you will investigate the zeta function $\zeta_q(s) := \sum_I \mathrm{N}(I)^{-s}$, where I ranges over nonzero ideals of the ring of integers $\mathcal{O}_K := \mathbb{F}_q[t]$ of the rational function field $K = \mathbb{F}_q(t)$.

Remark. The zeta function ζ_K of a global function field K defined in Problem 4 differs from the zeta function of its ring of integers $\mathcal{O}_K$, which is what we are considering here.

(a) Show that every nonzero $\mathcal{O}_K$-ideal has the form $I = (f)$, with $f \in \mathbb{F}_q[t]$ monic, and then $\mathrm{N}(I) = \#(\mathcal{O}_K/f\mathcal{O}_K) = q^{\deg f}$. Then prove that $\zeta_q(s) = \frac{1}{1-q^{1-s}}$ for $\mathrm{Re}(s) > 1$.

(b) Prove that $\zeta_q(s)$ has the Euler product

$$\zeta_q(s) = \prod_{\mathfrak{p}} (1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1},$$

valid for $\mathrm{Re}(s) > 1$.

(c) Prove that $\zeta_q(s)$ extends to a meromorphic function on $\mathbb{C}$ with a simple pole at $s = 1$ and no zeros. Give the residue of the pole at $s = 1$.

(d) Define a completed zeta function $Z(s) = G(s)\zeta_q(s)$, where $G(s)$ is a suitably chosen meromorphic function, so that $Z(s)$ satisfies the functional equation

$$Z(s) = Z(1 - s)$$

with simple poles at $s = 0, 1$ and no other poles.

(e) Let a_d denote the number of irreducible monic polynomials in $\mathbb{F}_q[t]$ of degree d. Using (a) and (b), prove that

$$\sum_{d|n} da_d = q^n.$$

and use this to derive an explicit formula for a_n.

(f) Prove the prime number theorem for $\mathbb{F}_q[t]$, which states that

$$a_n = \frac{q^n}{n} + O\left(\frac{1}{n}q^{n/2}\right).$$

Remark. The error term in (f) is comparable to the error term in the PNT under the Riemann hypothesis (replace q^n with x); note that the analog of the Riemann hypothesis for $\zeta_q(s)$ is (vacuously) true, by (c).

(g) Let $S(n)$ be the set of monic polynomials of degree n in $\mathbb{F}_q[t]$, and let $I(n)$ be the subset of polynomials in $S(n)$ that are irreducible. Show that $\#I(n)/\#S(n) \sim \frac{1}{n}$. Now let $R(n)$ be the subset of polynomials in $S(n)$ that have no roots in $\mathbb{F}_q$. Give an asymptotic estimate for $\#R(n)/\#S(n)$.

(h) Let $Q(n)$ denote the subset of $S(n)$ consisting of squarefree polynomials. Prove $\lim_{n\to\infty} \#Q(n)/\#S(n) = 1/\zeta_q(2)$ and derive an asymptotic estimate for this limit.

(i) For nonzero $f \in \mathcal{O}_K$ define Φ via $\Phi(f) := \#(\mathcal{O}_K/f\mathcal{O}_K)^\times$. Prove the following

1. $\Phi(f) = \mathrm{N}(f)\prod_{p|f}(1 - \mathrm{N}(p)^{-1})$, where p ranges over the irreducible factors of f.
2. For all $f, g \in \mathcal{O}_K$ with $(f, g) = 1$ we have $g^{\Phi(f)} \equiv 1 \bmod f$.

Problem 2. Bernoulli numbers (49 points)

For integers $n \geq 0$, the *Bernoulli polynomials* $B_n(x) \in \mathbb{Q}[x]$ are defined as the coefficients of the exponential generating function

$$E(t, x) := \frac{te^{tx}}{e^t - 1} = \sum_{n\geq 0} \frac{B_n(x)}{n!}t^n.$$

The *Bernoulli numbers* $B_n \in \mathbb{Q}$ are defined by $B_n = B_n(0)$.

(a) Prove that $B_0(x) = 1$, $B_n'(x) = nB_{n-1}(x)$, and $B_n(1) = B_n(0)$ for $n \neq 1$, and that these properties uniquely determine the Bernoulli polynomials.

(b) Prove that $B_n(x+1) - B_n(x) = nx^{n-1}$ and

$$B_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} B_k(x) y^{n-k}.$$

Use this to show that B_k can alternatively be defined by the recurrence $B_0 = 1$ and

$$B_n = -\frac{1}{n+1} \sum_{k=0}^{n-1} \binom{n+1}{k} B_k$$

for all $n > 0$, and show that $B_n = 0$ for all odd $n > 1$.

(c) Recall the hyperbolic cotangent function $\coth z := \frac{e^z + e^{-z}}{e^z - e^{-z}}$. Prove that

$$z \coth z = \sum_{n \geq 0} B_{2n} \frac{(2z)^{2n}}{(2n)!}.$$

(d) Show that $\cot z = i \coth iz$ and then derive (as Euler did) the identity

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

(e) Use (c) and (d) to prove that for all $n \geq 1$ we have

$$\zeta(2n) = (-1)^{n-1} \frac{(2\pi)^{2n} B_{2n}}{2 \cdot (2n)!},$$

and then use the functional equation to prove that for all $n \geq 1$ we have

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}.$$

(f) Prove (rigorously!) that for any integer $n > 1$ the asymptotic density of integers that are *n-power free* (not divisible by p^n for any prime p) is $1/\zeta(n)$ and compute this density explicitly for $n = 2, 4, 6$.

(g) Prove that for all integer $n, N > 1$ we have

$$\sum_{m=0}^{N-1} (m+x)^{n-1} = \frac{B_n(N+x) - B_n(x)}{n}.$$

Use this to deduce Faulhaber's formula

$$P_n(N) := \sum_{m=1}^{N-1} m^n = \frac{1}{n+1} \sum_{k=0}^{n} \binom{n+1}{k} B_k N^{n+1-k}$$

for summing nth powers. Compute the polynomials $P_n(N)$ explicitly for $n = 2, 3, 4$.

Problem 3. Arithmetic functions and Dirichlet series (49 points)

Recall that an *arithmetic function* is a function $a\colon \mathbb{Z}_{\geq 1} \to \mathbb{C}$; we say that $a \neq 0$ is *multiplicative* if $a(mn) = a(m)a(n)$ holds for all relatively prime m, n, and *totally multiplicative* if this holds for all m, n. Below are some examples; as usual, p denotes a prime, p^e denotes a (nontrivial) prime power, and $d|n$ indicates that d is a positive divisor of n.

- $0(n) = 0,\ \ 1(n) = 1,\ \ \mathrm{id}(n) := n,\quad e(n) := 0^{n-1}$;
- $\tau(n) := \#\{d|n\},\quad \sigma(n) := \sum_{d|n} d$;
- $\omega(n) := \#\{p|n\},\ \ \Omega(n) := \#\{p^e|n\},\ \ \phi(n) := \#(\mathbb{Z}/n\mathbb{Z})^\times$;
- $\lambda(n) := (-1)^{\Omega(n)},\ \ \mu(n) := (-1)^{\omega(n)} \cdot 0^{\Omega(n)-\omega(n)},\quad \mu^2(n) := \mu(n)^2$.

The set of all arithmetic functions forms a $\mathbb{C}$-vector space that we denote $\mathcal{A}$. Associated to each arithmetic function is a *Dirichlet series* $\sum_{n\geq 1} a_n n^{-s}$ defined by

$$D_a(s) := \sum_{n\geq 1} a(n)n^{-s}$$

The *Dirichlet convolution* $a * b$ of arithmetic functions a and b is defined by

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

For $k \in \mathbb{Z}_{\geq 0}$ we use f^{*k} to denote the k-fold convolution $f * \cdots * f$, with $f^{*0} := e$.

(a) For arithmetic functions a and b prove that $D_{a*b} = D_a D_b$, and show that endowing $\mathcal{A}$ with a multiplication defined by Dirichlet convolution makes $\mathcal{A}$ a $\mathbb{C}$-algebra that is isomorphic to the $\mathbb{C}$-algebra of Dirichlet series (with the usual multiplication).

(b) Show that $\mathcal{A}$ is a local ring with unit group $\mathcal{A}^\times = \{f \in \mathcal{A} : f(1) \neq 0\}$ and maximal ideal $\mathcal{A}_0 = \{f \in \mathcal{A} : f(1) = 0\}$. Prove that the set of multiplicative functions $\mathcal{M}$ forms a subgroup of $\mathcal{A}_1 := \{f \in \mathcal{A} : f(1) = 1\} \subseteq \mathcal{A}^\times$. Is this also true of the set of totally multiplicative functions?

(c) Prove the following identities $\mu * 1 = e$, $\phi * 1 = \mathrm{id}$, $\mu * \mathrm{id} = \phi$, $1 * 1 = \tau$, $\mathrm{id} * 1 = \sigma$. Use $\mu * 1 = e$ to give a one-line proof of the Möbius inversion formula.

(d) For $k \in \mathbb{Z}_{\geq 1}$ define $\tau_k(n) := \sum_{n_1 n_2 \cdots n_k = n} 1$, so $\tau_1 = 1$ and $\tau_2 = \tau = 1 * 1$. Prove that $\tau_k = 1^{*k}$, and $D_{\tau_k}(s) = \zeta(s)^k$, where $\zeta(s) = \sum_{n\geq 1} n^{-s}$ is the Riemann zeta function.

(e) Define the exponential map $\exp\colon \mathcal{A} \to \mathcal{A}$ by

$$\exp(f) := \sum_{n=0}^{\infty} \frac{f^{*n}}{n!} = e + f + \frac{f * f}{2} + \cdots$$

Prove that exp defines a group isomorphism from $(\mathcal{A}_0, +)$ to $(\mathcal{A}_1, *)$ with inverse

$$\log(f) := \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(f - e)^{*n}}{n}.$$

(f) Define $\kappa(n)$ to be $1/k$ if $n = p^k$ is a prime power and 0 otherwise (for us 1 is not a prime power). Prove that $\exp \kappa = 1$, and deduce that $\exp(-\kappa) = \mu$ and $\exp(2\kappa) = \tau$.

(g) Prove that each $f \in \mathcal{A}_1$ has a unique square-root $g \in \mathcal{A}_1$ for which $g^{*2} = f$ that we denote $f^{*1/2}$. Prove that $1^{*1/2} = \exp(\kappa/2)$ and compute $\exp(\kappa/2)(n)$ for n up to 10.

Problem 4. The Weil conjectures for global function fields (49 points)

Let $K/\mathbb{F}_q(t)$ be a global function field, with $\mathbb{F}_q$ algebraically closed in K. The *divisor group* $\operatorname{Div} K$ is the free abelian group generated by the places of K; it consists of formal sums $\sum_P n_P P$ over $P \in M_K$ in which only finitely many $n_P \in \mathbb{Z}$ are nonzero. This is the same as the group of M_K-divisors we defined in Lecture 15, but here we view $\operatorname{Div} K$ as an additive group and use P to denote a place rather than v.

Corresponding to each $f \in K^\times$ we have a *principal divisor*

$$\operatorname{div}(f) := \sum_P \operatorname{ord}_P(f) P,$$

where $\operatorname{ord}_P \colon K^\times \to \mathbb{Z}$ is the discrete valuation corresponding to P, which we extend to $\operatorname{Div} K$ by defining $\operatorname{ord}_P(\sum_Q n_Q Q) = n_P$. Two divisors D_1 and D_2 are *linearly equivalent* if $D_1 - D_2$ is a principal divisor, and we write $D_1 \sim D_2$ to indicate this; this defines an equivalence relation on $\operatorname{Div} K$ and we use $[D]$ to denote the equivalence class of D.

The *degree* of a place P is the dimension of the residue field of the local field K_P as an $\mathbb{F}_q$-vector space; it extends to a group homomorphism $\deg \colon \operatorname{Div} K \to \mathbb{Z}$ whose kernel contains the subgroup of principal divisors (by the product formula); the corresponding quotient is denoted $\operatorname{Pic}^0 K$. The *norm* of a divisor D is defined by $\mathrm{N}(D) := q^{\deg D}$; when $D = P$ this is the cardinality of the residue field and if D is supported only on finite places this agrees with the absolute norm defined in Problem 1.

We partially order divisors by defining

$$D_1 \le D_2 \qquad \Longleftrightarrow \qquad \operatorname{ord}_P(D_1) \le \operatorname{ord}_P(D_2) \text{ for all } P \in M_K.$$

A divisor $D \ge 0$ is said to be *effective*. The *zeta function* of K is defined as a sum over effective divisors

$$\zeta_K(s) := \sum_{D \ge 0} \mathrm{N}(D)^{-s} = \sum_{D \ge 0} q^{-s \deg(D)}$$

The *Weil conjectures* (for global function fields) concern three properties of $\zeta_K(s)$:

- $\zeta_K(s)$ is a rational function of q^{-s}.
- There is a functional equation that relates $\zeta_K(1-s)$ and $\zeta_K(s)$.
- The zeros of $\zeta_K(s)$ all lie on the line $\operatorname{Re}(s) = 1/2$.

In this problem you will prove the first two; Weil proved the third in the 1940s, and a generalization to algebraic varieties of higher dimension conjectured by Weil was proved by Deligne in the 1970s.

Associated to each divisor $D \in \operatorname{Div} K$ is a *Riemann-Roch space*

$$L(D) := \{f \in K^\times : \operatorname{div}(f) \ge -D\} \cup \{0\},$$

which is an $\mathbb{F}_q$-vector space whose finite dimension we denote $\ell(D) \in \mathbb{Z}_{\ge 0}$. The degree $\deg D$ and dimension $\ell(D)$ of a divisor D depend only on the divisor class $[D]$ and are related by the following theorem (which you are not asked to prove).

Theorem (Riemann-Roch)**.** *Let K be a global function field. There is an integer $g \ge 0$ and divisor $C \in \operatorname{Div} K$ such that for all divisors $D \in \operatorname{Div} K$ we have*

$$\ell(D) = \deg(D) - g + 1 + \ell(C - D).$$

(a) Prove that $\ell(C) = g$ and $\deg(C) = 2g - 2$, and that for $\deg(D) \geq 2g - 2$ we have $\ell(D) = \deg(D) - g + 1$ unless $D \sim C$. Conclude that both the integer g (the *genus*) and the divisor class $[C]$ (the *canonical class*) are uniquely determined.

(b) Prove that for any $n \geq 0$ the number of effective divisors of degree n is finite, and the number of divisor classes of degree n is finite (so in particular, the group $\operatorname{Pic}^0 K$ of divisor classes of degree 0, is finite).

(c) Prove that for any divisor D the number of effective divisors in $[D]$ is $\frac{q^{\ell(D)}-1}{q-1}$.

(d) Prove that the sum defining $\zeta_K(s)$ converges on $\operatorname{Re}(s) > 1$ and we have an Euler product

$$\zeta_K(s) = \prod_P (1 - \mathrm{N}(P)^{-s})^{-1}.$$

(e) Let a_n be the number of effective divisors of degree n. Prove that

$$a_n = \sum_{\deg([D])=n} \frac{q^{\ell(D)} - 1}{q - 1},$$

where the sum is over the divisor classes of degree n, and show that if we define $Z_K(u) := \sum_{n \geq 0} a_n u^n$ then $\zeta_K(s) = Z_K(q^{-s})$ for $\operatorname{Re} s > 1$.

(f) Let $e\mathbb{Z} = \deg(\operatorname{Pic} K)$. Prove there is a polynomial $L_K \in \mathbb{Z}[u]$ of degree $2g$ for which

$$Z_K(u) = \frac{L_K(u^e)}{(1 - u^e)(1 - (qu)^e)},$$

and show that $L_K(0) = 1$ and $L_K(1) = \#\operatorname{Pic}^0 K$.

(g) For $n \geq 1$ let $K_n := K \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$. Show that $Z_{K_n}(u^n) = \prod_{i=1}^n Z_K(\zeta_n^i u)$, where $\zeta_n := e^{2\pi i/n}$, and use this to prove that we must have $e = 1$ in part (f).

(h) Prove that $Z_K(q^{-s})$ is meromorphic on $\mathbb{C}$ and thus provides an analytic continuation of $\zeta_K(s)$ to $\mathbb{C}$ with simple poles at $s = 0, 1$. Are these the only poles?

(i) Let $\xi_K(s) := q^{(g-1)s}\zeta_K(s)$. Prove that $\xi_K(s)$ satisfies the functional equation

$$\xi_K(1 - s) = \xi_K(s).$$

Problem 5. Survey (2 points)

Complete the following survey by rating each problem you attempted on a scale of 1 to 10 according to how interesting you found it (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found it (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			
Problem 3			
Problem 4			

Please feel free to record any additional comments you have on the problem sets and the lectures, in particular, ways in which they might be improved.

Collaborators/Sources