18.785 Number Theory **Fall 2025**

Problem Set #1 **Due: 09/12/2025**

These problems are related to Lectures 1–2. Your solutions should be written up in latex (please do not submit handwritten solutions) and submitted as a PDF to Gradescope before midnight on the date due. You can use the latex source for this problem set as a template, and are welcome to use the latex environment of your choice (I personally use Overleaf and Texmaker, but there are many other options).

Instructions: First solve the warm up problems; these do not need to be formally written up or turned in. Then pick any three of Problems 1–4 to solve and write up your answers in latex. Finally, complete Problem 5, which is a short survey whose answers will help shape future problem sets and lectures. 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). 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. Warm up (0 points)

These warm up exercises do not need to be written up or turned in, they are provided simply to help you check your understanding.

(a) Prove the nonarchimedean "triangle equality": if $|\cdot|$ is a nonarchimedean absolute value on a field k and $|x| \neq |y|$ then $|x+y| = \max(|x|,|y|)$.

(b) Let K be a global field (a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$). Show that if K has characteristic zero then there is only one way to embed $\mathbb{Q}$ in K but when K has positive characteristic there are infinitely many different ways of embedding $\mathbb{F}_p(t)$ in K. In particular, show that the field $K := \operatorname{Frac}\Big(\mathbb{F}_p[x,y]/(y^2-x^3-x-1)\Big)$ can be viewed as both a degree 2 extension of $\mathbb{F}_p(x)$ and a degree 3 extension of $\mathbb{F}_p(y)$, but that the isomorphism $\mathbb{F}_p(x) \simeq \mathbb{F}_p(y)$ does not commute with the inclusions.

(c) Write down a monic polynomial $f \in \mathbb{Z}[x]$ with $\sqrt{2}+\sqrt{3}$ as a root.

Problem 1. Absolute values on $\mathbb{Q}$ (32 points)

(a) Prove that an absolute value $|\cdot|$ on a field k is nonarchimedean if and only if $|n| \leq 1$ for all $n \in \mathbb{Z}_{>0}$ (note $n := 1 + \cdots + 1 \in k$). (**Hint**: use the binomial theorem.)

(b) Prove Ostrowski's Theorem: every nontrivial absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime $p \leq \infty$. (**Hint**: if $|b| > 1$ for some $b \in \mathbb{Z}_{>1}$, let $|b| = b^\alpha$ and show there is a $C > 0$ such that $|n| \leq Cn^\alpha$ for all $n \in \mathbb{Z}_{\geq 1}$, and by applying this to powers deduce $|n| \leq n^\alpha$ for all $n \in \mathbb{Z}_{\geq 1}$. Now prove $|n| \geq n^\alpha$ for all $n \in \mathbb{Z}_{\geq 1}$ by fixing n, choosing s so $b^s \leq n < b^{s+1}$, using $|n| \geq |b^{s+1}| - |b^{s+1}-n|$ to show that $|n| \geq cn^\alpha$ for some $c > 0$ that does not depend on n, and apply to powers again.)

(c) Prove the product formula for $\mathbb{Q}$: show that $\prod_{p \leq \infty} |x|_p = 1$ for all $x \in \mathbb{Q}^\times$.

Problem 2. Absolute values on $\mathbb{F}_q(t)$ (32 points)

For each prime $\pi \in \mathbb{F}_q[t]$ and any nonzero $f \in \mathbb{F}_q[t]$, let $v_\pi(f)$ be the largest integer n for which $\pi^n | f$, equivalently, the largest n for which $f \in (\pi^n)$. For each $f/g \in \mathbb{F}_q(t)^\times$ define

$$v_\pi(f/g) := v_\pi(f) - v_\pi(g),$$

and let $v_\pi(0) := \infty$; also define $\deg 0 := -\infty$ and $\deg(f/g) := \deg f - \deg g$.

(a) For each prime $\pi \in \mathbb{F}_q[t]$, define $|r|_\pi := (q^{\deg \pi})^{-v_\pi(r)}$ for all $r \in \mathbb{F}_q(t)$. Show that $|\cdot|_\pi$ is a nonarchimedean absolute value on $\mathbb{F}_q(t)$.

(b) Define $|r|_\infty := q^{\deg r}$, for all $r \in \mathbb{F}_q(t)$. Prove that $|\cdot|_\infty$ is a nonarchimedean absolute value on $\mathbb{F}_q(t)$.

(c) Determine the residue field of $\mathbb{F}_q(t)$ with respect to $|\cdot|_\pi$; the residue field is the quotient of the valuation ring $\{x \in \mathbb{F}_q(t) : |x|_\pi \le 1\}$ by its unique maximal ideal.

(d) Describe the valuation ring $R := \{x \in \mathbb{F}_q(t) : |x|_\infty \le 1\}$ and its unique maximal ideal $\mathfrak{m}$. Then determine the residue field of $\mathbb{F}_q(t)$ with respect to $|\cdot|_\infty$.

(e) Prove Ostrowski's theorem for $\mathbb{F}_q(t)$: every nontrivial absolute value on $\mathbb{F}_q(t)$ is equivalent to $|\cdot|_\infty$ or $|\cdot|_\pi$ for some prime $\pi \in \mathbb{F}_q[t]$.

More precisely, show that if $\|\cdot\|$ is a nontrivial absolute value on $\mathbb{F}_q(t)$, either $\|t\| > 1$ and $\|\cdot\| \sim |\cdot|_\infty$, or $\|t\| \le 1$ and $\|\cdot\| \sim |\cdot|_\pi$ for some prime $\pi \in \mathbb{F}_q[t]$.

In view of (e), we regard ∞ as a "prime" of $\mathbb{F}_q(t)$ and let π range over both monic irreducible polynomials in $\mathbb{F}_q[t]$ and ∞.

(f) Prove the product formula for $\mathbb{F}_q(t)$: show that $\prod_\pi |r|_\pi = 1$ for every $r \in \mathbb{F}_q(t)^\times$.

Problem 3. Quadratic fields (32 points)

Let $K = \mathbb{Q}(\sqrt{d})$ with $d \ne 0, 1$ a squarefree integer, and let $\mathfrak{p}$ be a nonzero prime ideal of the ring of integers $\mathcal{O}_K$ that does not contain the integer $2d$.

(a) Give explicit generators for $\mathcal{O}_K$ as a $\mathbb{Z}$-module.

(b) Determine the index of $\mathbb{Z}[\sqrt{d}]$ in $\mathcal{O}_K$ as a function of d.

(c) Show that $\mathfrak{p}$ can be written in the form (p, α), with $(p) = \mathfrak{p} \cap \mathbb{Z}$ and $\alpha \in \mathcal{O}_K$.

(d) Show that $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_q$ where $q = [\mathcal{O}_K : \mathfrak{p}]$ is either p or p^2, with $\mathfrak{p} = (p, \alpha)$. Give an explicit criterion in terms of p and d for when the two cases occur.

(e) Determine the number of equivalence classes of archimedean absolute values of $\mathbb{Q}(\sqrt{d})$ as a function of d.

Problem 4. The Euler ϕ-function. (32 points)

Let A denote $\mathbb{Z}$ or $\mathbb{F}_p[t]$, and let $|\cdot|$ denote $|\cdot|_\infty$ (the standard archimedean absolute value on $\mathbb{Q}$ or the nonarchimedean absolute value of $\mathbb{F}_p(t)$ defined in Problem 2). Recall that $a \perp b$ means $(a,b) = A$. Throughout this problem, we assume $a, b \in A$ are nonzero, and understand "$a \bmod b$" to mean the image of a under the quotient map $A \to A/(b)$.

(a) Prove that $A/(a)$ is a ring with $|a|$ elements.

Define the Euler ϕ-function $\phi\colon A_{\neq 0} \to \mathbb{Z}_{>0}$ by $\phi(a) := \#(A/(a))^\times$.

(b) Prove $\phi(ab) = \phi(a)\phi(b)$ if $a \perp b$ and $\phi(a^n) = |a|^{n-1}(|a| - 1)$ for a prime and $n \geq 1$.

(c) Prove that $\phi(a) = |a| \prod_{q|a}(1 - |q|^{-1})$, where q ranges over primes.

(d) Prove that for $a \perp b$ we have $a^{\phi(b)} \equiv 1 \bmod b$.

(e) Prove that if b is prime then $\prod_{0<|a|<|b|} a \equiv \begin{cases} +1 \bmod b & \text{if } A = \mathbb{Z}; \\ -1 \bmod b & \text{if } A = \mathbb{F}_p[t]. \end{cases}$

(f) Let $a \perp b$ with b prime and let $r \geq 2$ divide $|b| - 1$. Show that $a \bmod b$ is an rth power if and only if $a^{(|b|-1)/r} \equiv 1 \bmod b$, and $\#\{c^r : c \in (A/(b^n))^\times\} = \phi(b^n)/r$.

Problem 5. Survey (4 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 time you spent on each problem to the nearest half hour.

	Interest	Difficulty	Time
Problem 1			
Problem 2			
Problem 3			
Problem 4			

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

Collaborators/Sources: