18.785 Number Theory **Fall 2025**

Problem Set #2 **Due: 09/19/2025**

These problems are related to Lectures 3–4. 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 solve one (but not both) of Problems 1–2, and complete the survey, Problem 3. 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. Warmup (0 points)

These warmup exercises do not need to be written up.

(a) Let I, J, K be nonzero ideals in a noetherian (not necessarily Dedekind) domain. Show that $I \div (J + K) = (I \div J) \cap (I \div K)$.

(b) Let p be a prime. Prove that there are exactly four (unital) commutative rings of cardinality p^2. Which arise as A/I for some discrete valuation ring A and ideal I?

Problem 1. Characterizing Dedekind domains (98 points)

Recall that we defined a Dedekind domain to be an integrally closed noetherian domain of dimension at most one, or equivalently, a noetherian domain whose localizations at nonzero prime ideals are discrete valuation rings (see Proposition 2.9); let (D) denote either of these equivalent conditions. In Lecture 3 we proved that every Dedekind domain A enjoys the following properties:

(a) Each nonzero prime ideal of A is invertible.

(b) Each nonzero ideal of A is a (finite) product of prime ideals.

(c) *To contain is to divide*: for all ideals $J \supseteq I$ we have $J|I$.

(d) For each ideal I in A there exists a nonzero ideal J such that IJ is principal.

(e) The quotient A/I of A by any nonzero ideal I is a principal ideal ring.

(f) If a is a nonzero element of an ideal I then $I = (a, b)$ for some $b \in I$.

In this problem you will prove that for any integral domain A, each of the conditions above implies (D). As explained in Remark 2.15, for integral domains that are not necessarily noetherian, one defines fractional ideals as A-submodules I of the fraction field A for which there exists a nonzero $r \in A$ such that $rI \subseteq A$ (the definition of an invertible ideal is exactly the same).

You may prove these implications in any order (e.g. it suffices to just prove (a)⇒(b) in your answer for part **(a)** so long as you eventually prove (b)⇒(D)). You may want to first consider the case where A is a noetherian local domain.

(a) Prove (a)⇒(D).

(b) Prove (b)⇒(D). (Hint: show (b) implies that every invertible prime ideal is maximal by considering factorizations of $\mathfrak{p} + (a)$ and $\mathfrak{p} + (a^2)$ for some nonzero $a \in \mathfrak{p}$.)

(c) Prove (c)⇒(D).

(d) Prove (d)⇒(D).

(e) Prove (e)⇒(D).

(f) Prove (f)⇒(D).

(g) Show that the noetherian integral domain $A = \mathbb{Z}[\sqrt{-3}]$ of dimension one is *not* a Dedekind domain in two ways: show that it is not integrally closed and exhibit a nonzero prime ideal $\mathfrak{p}$ for which $A_{\mathfrak{p}}$ is not a DVR. Then give similarly explicit demonstrations that A does not satisfy each of the properties (a)-(f) above.

Problem 2. Fermat's last theorem (98 points)[1]

Recall that Fermat's Last Theorem (FLT) states that

$$x^n + y^n = z^n$$

has no integer solutions with $xyz \neq 0$ for $n > 2$. By removing common factors we may assume $\gcd(x, y, z) = 1$, and we may assume that n is a prime $p \geq 5$, since the cases $n = 3$ and $n = 4$ were proved by Euler and Fermat (respectively), and we can easily reduce to the case where either $n = p$ is prime or $n = 4$ (every solution with $n = ab$ also gives a solution with $n = a$ and $n = b$).

So let $p \geq 5$ be prime and suppose x, y, z are relatively prime integers for which

$$x^p + y^p = z^p$$

with $xyz \neq 0$, and let $\zeta_p \in \overline{\mathbb{Q}}$ denote a primitive pth root of unity (so $\zeta_p^p = 1$ but $\zeta_p \neq 1$). In order to simplify matters, we will make two further assumptions:

(1) $xyz \not\equiv 0 \bmod p$;

(2) the ring $\mathbb{Z}[\zeta_p]$ is a UFD.

You will prove below that under these assumptions, no such x, y, z can exist.

The first assumption is not necessary, your proof can be extended to remove this assumption. This was the basis of Lamé's "proof" of FLT in 1847, which relied on (2); unfortunately (2) holds only for $p \leq 19$. Kummer later generalized Lamé's argument to many cases where $\mathbb{Z}[\zeta_p]$ is not a UFD; Kummer's argument applies whenever the order of the ideal class group of the ring of integers of $\mathbb{Q}(\zeta_p)$ is not divisible by p, which is expected to hold for infinitely many p (the set of so-called *regular* primes is believed to be infinite but this is not known).

For the sake of concreteness, let us fix an embedding of $\mathbb{Q}(\zeta_p)$ in $\mathbb{C}$ by defining $\zeta_p := e^{2\pi i/p}$, and for any $z \in \mathbb{Q}(\zeta_p) \subseteq \mathbb{C}$, let $\bar{z}$ denote its complex conjugate. If S is a set, then $a \equiv b \bmod S$ means $a - b \in S$.

[1] This problem is adapted from [1, I, Ex.17-27] but corrects/clarifies a number of minor issues there.

(a) Show that $\zeta_p^i - \zeta_p^j$ properly divides p in the ring $\mathbb{Z}[\zeta_p]$ for any $i \not\equiv j \bmod p$.

(b) Show that if a non-unit $\alpha \in \mathbb{Z}[\zeta_p]$ divides $x + y\zeta_p^i$ then it does not divide $x + y\zeta_p^j$ for any $j \not\equiv i \bmod p$.

(c) Show that $x + y\zeta_p^i = u_i \alpha_i^p$ for some $\alpha_i \in \mathbb{Z}[\zeta_p]$ and $u_i \in \mathbb{Z}[\zeta_p]^\times$.

(d) Prove that $1 + t + \cdots + t^{p-1}$ is irreducible in $\mathbb{Q}[t]$; conclude that $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ is a basis for $\mathbb{Z}[\zeta_p]$ as a $\mathbb{Z}$-module.

(e) Show that in any commutative ring A we have $\alpha^p + \beta^p \equiv (\alpha + \beta)^p \bmod pA$ for all $\alpha, \beta \in A$.

(f) Let $\alpha \in \mathbb{Z}[\zeta_p]$. Show (1) $\alpha^p \equiv a \bmod p\mathbb{Z}[\zeta_p]$ for some $a \in \mathbb{Z}$, (2) $\alpha^p \equiv \bar{\alpha}^p \bmod p\mathbb{Z}[\zeta_p]$, (3) $p \notin \mathbb{Z}[\zeta_p]^\times$, and (4) if $u \in \mathbb{Z}[\zeta_p]^\times$ then $u/\bar{u} \neq -\zeta_p^i$ for any i.

(g) Show that if $\alpha \in \overline{\mathbb{Q}}^\times$ is an algebraic integer whose Galois conjugates all lie in the unit disk in $\mathbb{C}$ then α is a root of unity.

(h) Show that if $u \in \mathbb{Z}[\zeta_p]^\times$ then $u/\bar{u} = \zeta_p^i$ for some i.

(i) Show that if $x + y\zeta_p \equiv u\alpha^p \bmod p\mathbb{Z}[\zeta_p]$ with $u \in \mathbb{Z}[\zeta_p]^\times$, then for some $0 \leq j \leq p-1$ we must have $x + y\zeta_p \equiv (x + y\zeta_p^{-1})\zeta_p^j \bmod p\mathbb{Z}[\zeta_p]$.

(j) Show that $x + y\zeta_p \equiv (x + y\zeta_p^{-1})\zeta_p^j \bmod p\mathbb{Z}[\zeta_p]$ only if $j \equiv 1 \bmod p$.

(k) Show that if $x + y\zeta_p \equiv x\zeta_p + y \bmod p\mathbb{Z}[\zeta_p]$ then $x \equiv y \bmod p$.

(l) Assuming $\mathbb{Z}[\zeta_p]$ is a UFD, show $x^p + y^p = z^p$ has no solutions with $xyz \not\equiv 0 \bmod p$.

Problem 3. 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			

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

Collaborators/sources:

References

[1] Dino Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics **9**, American Mathematical Society, 1996.