Math 514a: Algebraic Number Theory / Fall 2025
Homework assignment #1
Suggested due date: September 16, 2025

Edit 9/16/25: Added hint for (5b).
This homework set is a bit of a choose-your-own-adventure. There are three types of problems: A, B, and C.

- **Problems of type A are in blue.** These should be completely straightforward and/or review. Definitely do them if this material is new to you! On the other hand, if one of these is completely obvious to you, it's ok to skip it.
- **Problems of type B are in black.** These are a little more meaty. These are the main problems for the course, and everyone should work on them.
- **Problems of type C are in purple.** These are either more challenging or a little outside the main scope of the course. Do these last, if you're all set with A and have already done B.

(Open to suggestions of other forms of typesetting for differentiation; certainly do let me know if the colors are difficult to see.)

(1) **Legendre symbol review:** Fix an odd prime p. For an integer a recall that we set

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \text{ is a nonzero square modulo } a, \\ -1 & \text{if } p \text{ is a nonsquare modulo } a. \end{cases}$$

(a) In class we showed that $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}$ modulo p. Recall this argument. In particular, this implies that $(\frac{-1}{p}) \equiv 1$ if and only if $p \equiv 1 \mod 4$.

More generally, for $d \mid (p-1)$ show that $a^{\frac{p-1}{d}} \equiv 1$ if and only if a is a d^{th} power modulo p. How many distinct d^{th} powers are there modulo p?
Same question if $\gcd(d, p-1) = 1$.

(b) Show that $(\frac{\cdot}{p})$ is a totally multiplicative function $\mathbb{Z} \to \{0, 1, -1\}$. That is, $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$ for all $a, b \in \mathbb{Z}$.

Show that $(\frac{\cdot}{p})$ is a quadratic Dirichlet character modulo p (look up definitions if necessary).

To compute $(\frac{a}{p})$ quickly, by multiplicativity it suffices to know $(\frac{2}{p})$ and *quadratic reciprocity:* for odd primes p, q, we have $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}}$. Both of these were studied by Gauss and have elementary proofs. Proceed as follows.

(a) **Gauss's Lemma:** Given a relatively prime to p and each $k = 1, 2, \ldots, \frac{p-1}{2}$ define $r_k \in \{1, \ldots, \frac{p-1}{2}\}$ and $\varepsilon_k = \pm 1$ by $ak \equiv \varepsilon_k r_k$ modulo p. Show that $(\frac{a}{p}) = (-1)^n$, where n is the number of $\varepsilon_1, \ldots, \varepsilon_{\frac{p-1}{2}}$ that are negative.

(*Hint*: Show that the r_k are distinct and compare $\prod_k ak$ to $\prod_k \varepsilon_k r_k$.)

(b) Show that $\varepsilon_k = (-1)^{\left\lfloor \frac{2ak}{p} \right\rfloor}$ in (1a) above[(i)], so that for a prime to p we have $(\frac{a}{p}) = (-1)^m$, where $m = \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{2ak}{p} \rfloor$.

(c) Show that $(\frac{2}{p}) = 1$ iff $p \equiv \pm 1$ modulo 8. In other words, $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

(d) Show that for odd, positive, relatively prime a, b, we have

$$\sum_{k=1}^{\frac{b-1}{2}} \left\lfloor \frac{ak}{b} \right\rfloor + \sum_{k=1}^{\frac{a-1}{2}} \left\lfloor \frac{bk}{a} \right\rfloor = \frac{a-1}{2} \cdot \frac{b-1}{2}.$$

(*Hint*: Consider the rectangle in the plane with sides parallel to the axes and one diagonal going from the origin to $(\frac{a}{2}, \frac{b}{2})$. Count the interior lattice points.)

(e) Show that for odd, positive, relatively prime a, b, the parity of $\sum_{k=1}^{\frac{b-1}{2}} \lfloor \frac{ak}{b} \rfloor$ is the same as the parity of $\sum_{k=1}^{\frac{b-1}{2}} \lfloor \frac{2ak}{b} \rfloor$.

Alternatively, for a odd and prime to p, use the fact that $(\frac{2}{p})(\frac{a}{p}) = (\frac{2a+2p}{p}) = \left(\frac{(a+p)/2}{p}\right)$ along with (1b) and (1c) to get rid of the 2 in (1b) and conclude that $(\frac{a}{p}) = (-1)^M$, where $M = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor$.

(f) **Quadratic reciprocity:** for distinct odd primes $p,\ q$, we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}}.$$

In other words, $(\frac{p}{q}) \neq (\frac{q}{p})$ iff $p \equiv q \equiv 3 \mod 4$.

We will give alternate proofs of both the $(\frac{2}{p})$ statement and quadratic reciprocity this semester by considering prime splitting in cyclotomic fields.

(2) **A bit of algebra review:** Let A be a domain.

Recall that a nonzero, nonunit element a of A is an *irreducible* element if any factorization $a = bc$ in A if trivial: that is, one of b, c is a unit. Under the same assumptions a is a *prime* element if $a \mid bc$ for $b, c \in A$ implies that $a \mid b$ or $a \mid c$.

(a) Show that $a \in A$ is prime if and only if (a) is a nonzero prime ideal of A.

(b) Show that $a \in A$ is irreducible if and only if (a) is maximal among nonzero proper principal ideals of A.

(c) Show that prime elements are always irreducible.

(d) Give an example of a domain A and an irreducible of A that is not prime.

Recall that A is *noetherian* if every ideal is finitely generated (equivalently, if every nondecreasing chain of ideals in A eventually stabilizes), and A is a *UFD (unique*

[(i)] More generally, given positive a, b, with b odd, write $a = bq + \varepsilon r$ with $0 \leq r < \frac{b}{2}$ and $\varepsilon = \pm 1$. Then $\varepsilon = (-1)^{\left\lfloor \frac{2a}{b} \right\rfloor}$.

factorization domain) if every nonzero nonunit element of A factors into a product of irreducible elements, uniquely up to units and reordering.

(e) Show that in a UFD, irreducible elements are prime.

In fact, irreducible $\iff$ prime close to characterizes a UFD.

(f) Show that if A is noetherian, then every nonzero nonunit factors as a product of irreducibles.

(g) Show that a noetherian domain where every irreducible is prime is a UFD.

More definitions around the chain of reasoning: A is a *PID (principal ideal domain)* if every ideal of A is principal, and A is a *Euclidean domain* if there exists a function $d : A\backslash\{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ so that for every $a, b \in A$ with $b \neq 0$ there is $q, r \in A$ with $a = bq + r$ and $r = 0$ or $d(r) < d(b)$.[(ii)]

(h) Show that if A is Euclidean then it is a PID.

You may assume that d additionally satisfies $d(a) \leq d(ab)$ for all nonzero $b \in A$. Given an ideal $\mathfrak{a}$ of A take an element g of J with $d(g)$ minimal, and show that g generates $\mathfrak{a}$.

More generally, show that you can replace the Euclidean function d by $\tilde{d}$ which satisfies the additional condition above. For example, set $\tilde{d}(a) := \min_{b \neq 0} d(ab)$ and prove that A is still $\tilde{d}$-Euclidean.

The converse to the statement in (2h) is false: see Theorem 22 of Keith Conrad's blurb on Euclidean domains for an example of a PID that is not a Euclidean domain.

(i) Show that if A is a PID then it is a UFD.

(j) The converse to (2i) is also false. Give an example of a UFD that is not a PID.

(3) **Arithmetic of Gaussian integers:** Recall that $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$ with norm function $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ defined by $N(a + bi) = a^2 + b^2 = |a + bi|^2_{\mathbb{C}}$.

(a) Show that N is totally multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$.

(b) Show that $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $N(\alpha) = 1$.
Conclude that the only units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

(c) Show that if $N(\pi)$ is prime in $\mathbb{Z}$, then π is prime in $\mathbb{Z}[i]$.

(d) Show that if p a prime of $\mathbb{Z}$ factors in $\mathbb{Z}[i]$, then $p = N(\pi)$ for some $\pi \in \mathbb{Z}[i]$.

(e) For $\alpha = a + bi$, let $\bar{\alpha} = a - bi$ be the *conjugate* of α. Show that α and $\bar{\alpha}$ are not associates unless α is in $\mathbb{Z}$ or α is of the form $\pm a \pm ai$ for some $a \in \mathbb{Z}$ (that is, α is an associate of a rational integer multiple of $1 + i$).

(f) In class we gave a geometric argument that $\mathbb{Z}[i]$ is norm-Euclidean. In fact, we did a little bit more: we showed that, given $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, we can find $q, r \in \mathbb{Z}[i]$ with $\alpha = \beta q + r$ and $N(r) \leq \frac{N(\beta)}{2}$. Give an *algebraic* proof of this statement.

[(ii)] To specify the function d, we might also say that A is *d-Euclidean*.

(One way to start is to divide $\alpha\bar{\beta}$ by $N\beta = \beta\bar{\beta}$, componentwise in $\mathbb{Z}$.)

(g) In class we showed that a prime p is expressible as a sum of two squares if and only if $p \equiv 1$ modulo 4. Use factorization in $\mathbb{Z}[i]$ to determine which natural numbers are expressible as sums of two squares.

(4) **Generalizing the Gaussian integer story:** First, consider $\mathbb{Z}[\sqrt{-2}]$.

(a) Define a totally multiplicative norm on $\mathbb{Z}[\sqrt{-2}]$. Identify the units of $\mathbb{Z}[\sqrt{-2}]$.

(b) Show that $\mathbb{Z}[\sqrt{-2}]$ is norm-Euclidean (you can do this either algebraically or geometrically), and hence a PID.

(c) Show that $(\frac{-2}{p}) = 1$ iff $p \equiv 1, 3$ modulo 8. (Use (1c).)

(d) Give a full description of how primes of $\mathbb{Z}$ factor in $\mathbb{Z}[\sqrt{-2}]$. Explain everything.

(e) Give a full characterization of which positive primes of $\mathbb{Z}$ are represented by the quadratic form $x^2 + 2y^2$.

Now, consider $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

(f) Define a norm, identify the units, and show that $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is norm-Euclidean.

(g) Describe fully how primes of $\mathbb{Z}$ factor in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Connect this to representations of primes by some quadratic form.

(5) **A real quadratic field:** Now consider $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} : a, b \in \mathbb{Z}\}$.

(a) Define a totally multiplicative norm N on $\mathbb{Z}[\sqrt{2}]$. What can you say about the norm of a unit of $\mathbb{Z}[\sqrt{2}]$?

(b) Show that every unit in $\mathbb{Z}[\sqrt{2}]$ is of the form $\pm(1 + \sqrt{2})^n$ for some $n \in \mathbb{Z}$. In particular, the group of units is a $\mathbb{Z}$-module of rank 1.
Edit 9/16/25: *Hint:* If there's a unit in $\mathbb{Z}[\sqrt{2}]^\times$ that's not in $U = \{\pm(1+\sqrt{2})^n\}$, scale it by elements of U to find a unit of the form $a + b\sqrt{2}$ with

$$1 < a + b\sqrt{2} < 1 + \sqrt{2}.$$

Invert to get a second inequality; add or subtract to bound a or b.
It may be useful to take cases depending on the sign of the norm.

(c) Show that $\mathbb{Z}[\sqrt{2}]$ is norm-Euclidean and hence a PID.

(d) How do primes of $\mathbb{Z}$ factor in $\mathbb{Z}[\sqrt{2}]$? Which primes of $\mathbb{Z}$ are represented by the quadratic form $x^2 - 2y^2$?

(6) **Rings of integers in quadratic fields:** Let K be a quadratic extension of $\mathbb{Q}$. Compute its ring of integers $\mathcal{O}_K$. (First show that $K = \mathbb{Q}(\sqrt{d})$ for some squarefree integer d; your answer will depend on d modulo 4, and you should find three cases.)

(7) **Minkowski's theorem:** A region D of $\mathbb{R}^n$ is said to be *convex* if whenever two points P, Q are in D, the entire line segment $\{tP + (1-t)Q : t \in [0,1]\}$ connecting P and Q is contained in D as well.[iii] We will call a region D of $\mathbb{R}^n$ (*centrally*) *symmetric* if $-P$ is in D whenever P is in D.

A *lattice* in $\mathbb{R}^n$ here will be a free $\mathbb{Z}$-module of rank n whose basis is an $\mathbb{R}$-basis for $\mathbb{R}^n$. The covolume $\operatorname{Covol} L$ of a lattice L is the volume of a *fundamental domain* of the lattice (the n-parallelepiped determined by a basis of the lattice).

(a) Prove **Minkowski's theorem**: Let L be a lattice in $\mathbb{R}^n$. If $D \subseteq \mathbb{R}^n$ is a convex, symmetric, measurable region with $\operatorname{Vol}(D) > 2^n \operatorname{Covol}(L)$, then D contains a nonzero point of L.

(First show that it suffices to assume that L is the standard lattice $\mathbb{Z}^n$ of $\mathbb{R}^n$. Translating D into a fundamental domain of the doubled lattice $2\mathbb{Z}^n$, show that volume considerations tell us that D contains two distinct points P, Q all whose coordinates differ by even integers.)

(b) **Four-square theorem for primes:** Use Minkowski's theorem to prove Lagrange's result that any prime is expressible as a sum of *four* squares.

(If p is an odd prime, show that one can find two integers a, b so that $a^2+b^2+1 \equiv 0$ modulo p (pigeonhole principle). Consider the region

$$D = \{(x,y,z,w) : x^2 + y^2 + z^2 + w^2 < 2p\} \subset \mathbb{R}^4$$

and the lattice $L \subset \mathbb{R}^n$ spanned by $(p,0,0,0)$, $(0,p,0,0)$, $(a,b,1,0)$, and $(-b,a,0,1)$. You'll have to derive or look up a formula for the volume of a 4-sphere.)

(c) Prove Lagrange's full result: every nonnegative integer is expressible as a sum of four squares.

(One convenient way to proceed is to put a multiplicative norm on the Hamiltonian quaternions $\mathbb{H}$. If $\alpha = a+bi+cj+dk \in \mathbb{H}$, let $\bar{\alpha} := a-bi-cj-dk$ and set $N\alpha := \alpha\bar{\alpha} = a^2+b^2+c^2+d^2$. Check that $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$ to establish multiplicativity. Restrict to $a, b, c, d \in \mathbb{Z}$.)

(8) **Transitivity of norm and trace:** Let $M/L/K$ be a finite tower of fields.

(a) Show that $\mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}$.
(b) Show that $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$.

[iii] I believe I said in class that is suffices to check midpoints, but that's false without additional assumptions: indeed, $\mathbb{Q} \subset \mathbb{R}$ is "midpoint-closed" but is not a convex set!