E. Dummit's Math 4527 ~ Number Theory 2, Spring 2021 ~ Homework 12, due Thu Apr 15th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Either staple the pages of your assignment together and write your name on the first page, or paperclip the pages and write your name on all pages.

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. Calculate:
   (a) Calculate the cubic residue symbols $\left[\frac{4+\sqrt{-3}}{11}\right]_3$, $\left[\frac{2\sqrt{-3}}{4+\sqrt{-3}}\right]_3$, and $\left[\frac{2+\sqrt{-3}}{7+2\sqrt{-3}}\right]_3$. Which elements are cubic residues and which are not?
   (b) Find the primary associates of the primes $2+\sqrt{-3}$ and $7+2\sqrt{-3}$ in $\mathcal{O}_{\sqrt{-3}}$, and then verify cubic reciprocity for these associates.
   (c) Calculate the quartic residue symbols $\left[\frac{5+i}{7}\right]_4$, $\left[\frac{2i}{6+i}\right]_4$, and $\left[\frac{-2+i}{7-2i}\right]_4$. Which elements are quartic residues? Which elements are quadratic residues?
   (d) Find the primary associates of the primes 11 and $7+2i$ in $\mathbb{Z}[i]$, and then verify quartic reciprocity for these associates.

Part II: Solve the following problems. Justify all answers with rigorous, clear arguments.

2. If R is a (commutative) ring with 1, the characteristic of R is defined to be the smallest positive integer n for which $\underbrace{1+1+\cdots+1}_{n \text{ terms}} = 0$, or 0 if there is no such positive integer n.
   (a) Find the characteristics of $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}[i]/(7)$, $\mathbb{Z}[i]/(2+i)$, and $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$. [Note that $(1,1)$ is the multiplicative identity in the last ring.]
   (b) If R is an integral domain, prove that its characteristic is always either 0 or a prime number.
   (c) Let R be a commutative ring of prime characteristic p. Prove that for any $a, b \in R$, the "freshman's binomial theorem" $(a+b)^p = a^p + b^p$ is actually correct. Deduce that the map $\varphi : R \to R$ given by $\varphi(a) = a^p$ is actually a ring homomorphism (this map is called the Frobenius endomorphism and turns out to be quite important in many contexts).
   (d) Let p be an integer prime congruent to 3 modulo 4. If $z = a + bi \in \mathbb{Z}[i]$, prove that $z^p \equiv \overline{z} \pmod{p}$. [Note that this was mentioned but not proven in class.]

---

3. In class, we proved cubic and quartic reciprocity using properties of Gauss sums. The goal of this problem is to give a self-contained proof of quadratic reciprocity using Gauss sums. So let p, q be distinct odd integer primes and let $\chi_p(a) = \left(\frac{a}{p}\right)$ be the Legendre symbol modulo p. Recall that the Gauss sum of a multiplicative character χ is defined to be $g_a(\chi) = \sum_{t=1}^{p-1} \chi(t) e^{2\pi i a t/p} \in \mathbb{C}$.
   (a) Show that $g_a(\chi_p) = \left(\frac{a}{p}\right) g_1(\chi_p)$ for any integer a. [Hint: If $p|a$, count the number of quadratic residues. For other a, reindex the sum.]
   (b) Let $S = \sum_{a=0}^{p-1} g_a(\chi_p) g_{-a}(\chi_p)$. Show that $S = \left(\frac{-1}{p}\right)(p-1) g_1(\chi)^2$. [Hint: Use (a), making sure to separate $a = 0$ and $a \neq 0$.]

(c) Show that if p does not divide a, then $\sum_{a=0}^{p-1} e^{2\pi i a(s-t)/p} = \begin{cases} p & \text{if } s = t \\ 0 & \text{if } s \neq t \end{cases}$ for any integers s and t.

(d) Show that the sum S from part (b) is equal to $p(p-1)$. [Hint: Write $S = \sum_{a=0}^{p-1} \sum_{s=1}^{p-1} \sum_{t=1}^{p-1} \left(\frac{st}{p}\right) e^{2\pi i a(s-t)/p}$, then change summation order to sum over a first, move the Legendre symbol out, and use (c).]

(e) Let $p^* = \left(\frac{-1}{p}\right) p$. Show that the Gauss sum $g_1(\chi_p)$ has $g_1(\chi_p)^2 = p^*$. Deduce that $g_1(\chi_p)$ is an element of the quadratic integer ring $\mathcal{O}_{\sqrt{p^*}}$.

Now let p and q be distinct odd primes and let $g = g_1(\chi_p) \in \mathcal{O}_{\sqrt{p^*}}$ be the quadratic Gauss sum.

(f) Show that $g^{q-1} \equiv \left(\frac{p^*}{q}\right) \pmod{q}$. [Hint: Use (e).]

(g) Show that $g^q \equiv g_q(\chi_p) \equiv \left(\frac{q}{p}\right) g \pmod{q}$. [Hint: Use 2(c) and (a).]

(h) Conclude that $\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g \pmod{q}$, and deduce that $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$.

(i) Deduce the law of quadratic reciprocity: $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) (-1)^{(p-1)(q-1)/4}$.

---

4. Let F be a field. A discrete valuation on F is a surjective function $v : F^\times \to \mathbb{Z}$ such that $v(ab) = v(a) + v(b)$ for all $a, b \in F$ and $v(a+b) \geq \min(v(a), v(b))$ for all $a, b \in F^\times$ with $a + b \neq 0$. The set $R = \{r \in F^\times : v(r) \geq 0\} \cup \{0\}$ is called the valuation ring of v. By convention we also set $v(0) = \infty$.

(a) If v is a discrete valuation on F and $r \in F$ is a root of unity (i.e., has $r^n = 1$ for some n), show that $v(r) = 0$.

(b) If $F = \mathbb{Q}$ and p is prime, show that the map defined by $v(p^n \frac{x}{y}) = n$, where by assumption p does not divide x or y, is a discrete valuation on $\mathbb{Q}$. (This is known as the *p-adic valuation* on $\mathbb{Q}$.) What is the associated valuation ring?

(c) For any discrete valuation v with valuation ring R, show that R is an integral domain.

(d) Show that for any $r \in F^\times$, either r or $1/r$ is in R.

(e) Show that $x \in R$ is a unit of R if and only if $v(x) = 0$.

(f) Let $t \in R$ be a fixed element with $v(t) = 1$. If $x \in R$ is nonzero and $v(x) = n$, show that $x = ut^n$ for some unit $u \in R$.

(g) Let $t \in R$ be a fixed element with $v(t) = 1$. Show that every nonzero ideal of R is of the form (t^n) for some $n \geq 0$. [Hint: Let n be the smallest valuation of any nonzero element of I.]

(h) Conclude that R has a unique maximal ideal, and that every ideal of R is principal.

(i) Show that R is also a Euclidean domain. [Hint: Take the norm to be the valuation v.]

(j) If v is a discrete valuation on F, show that the distance function d defined via $d(x, y) = 2^{-v(x-y)}$ makes F into a metric space. In other words, show that it satisfies the properties that for all $x, y, z \in F$, (i) $d(x, y) \geq 0$ with equality if and only if $x = y$, (ii) $d(x, y) = d(y, x)$, and (iii) $d(x, z) \leq d(x, y) + d(y, z)$. [Hint: You might find it easier to show the ultrametric inequality $d(x, z) \leq \max(d(x, y), d(y, z))$ instead.]

- Remark: We may adapt the p-adic valuation from (b) into other fields, using arbitrary prime ideals from the ring of integers. For example, for the field of rational functions $F(x)$, another family of discrete valuations is the degree of vanishing at $x - r$ for a particular $r \in F$. The fact that the discrete valuation gives rise to a natural metric on F then allows bringing analysis into the discussion (convergence, Cauchy sequences, completions, and so forth).
