E. Dummit's Math 4527 ~ Number Theory 2, Spring 2024 ~ Homework 8, due Fri Mar 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. Identify all pages containing each problem when submitting the assignment.

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

1. (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.

---

2. Find all solutions (x,y,z) to the Diophantine equation $x^2+y^2=z^7$ where x and y are relatively prime.

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

3. Prove that the only solution to the Diophantine equation $y^2=x^3-8$ is $(x,y)=(2,0)$. [Hint: There are two different cases according to whether y is even or odd.]

---

4. 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.]

---

5. The goal of this problem is to explore some results about integers of the form x^2+Dy^2. Say that an integer D is "integrally representable" (non-standard terminology) if it is true that any integer n that can be written in the form x^2+Dy^2 for rational numbers x,y then it can be written in that form for integers x,y.

   (a) Prove that $D=1$ is integrally representable. (For example, $5=(22/13)^2+(19/13)^2=2^2+1^2$.)

   (b) Prove that $D=2$ is integrally representable. (For example, $3=(5/3)^2+2(1/3)^2=1^2+2\cdot 1^2$.)

   (c) Prove that $D=3$ is integrally representable. (For example, $13=(25/7)^2+3(2/7)^2=1^2+3\cdot 2^2$.)

   (d) Prove that $D=14$ is not integrally representable.

   (e) Suppose $D\equiv 3 \pmod{4}$ and $D+1$ is not a square. Prove that D is not integrally representable.

---

6. Suppose I is a nonzero ideal of $R = \mathcal{O}_{\sqrt{D}}$. The goal of this problem is to show that R/I is finite and its cardinality is $N(I)$. (Indeed, $N(I)$ is often just defined to be the cardinality of R/I, rather than as the nonnegative generator of $I \cdot \overline{I}$.)

   (a) Suppose I has prime ideal factorization $I = P_1^{a_1} \cdots P_n^{a_n}$. Show that R/I is isomorphic to $(R/P_1^{a_1}) \times \cdots \times (R/P_n^{a_n})$ and that $N(I) = N(P_1^{a_1}) \cdots N(P_n^{a_n})$.

   (b) Suppose a is any positive integer. Show that the cardinality of $R/(a)$ is a^2.

   (c) Suppose $Q = P^n$ is a power of a prime ideal. If $P = (p)$ for a prime integer p, show that $\#(R/Q) = N(Q)$.

   (d) Suppose $Q = P^n$ for some prime ideal P with $P\overline{P} = (p)$ and p prime; note that we are *not* assuming that $\overline{P} \neq P$. Show that all of the quotients R/P, P/P^2, ... , P^{n-1}/P^n, $P^n/(P^n\overline{P})$, ... , $(P^n\overline{P}^{n-1})/(P^n\overline{P}^n)$ have cardinality greater than 1, and that the product of their cardinalities is the cardinality of $R/(P^n\overline{P}^n)$. Conclude that all of these cardinalities must equal p and deduce that $\#(R/Q) = N(Q)$.

   (e) Show that R/I has cardinality $N(I)$ for any nonzero ideal I.

---

7. [Challenge] 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 $\sum_{a=0}^{p-1} e^{2\pi i a(s-t)/p} = \begin{cases} p & \text{if } s \equiv t \pmod{p} \\ 0 & \text{if } s \not\equiv t \pmod{p} \end{cases}$ 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 5(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: $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{(p-1)(q-1)/4}$.
