E. Dummit's Math 4527 ~ Number Theory 2, Spring 2025 ~ Homework 10, due Tue Apr 1st.

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. Find reduced quadratic forms equivalent to $17x^2 - 83xy - 24y^2$, $16x^2 - 70xy + 77y^2$, and $77x^2 - 56xy + 10y^2$.

---

2. Find the reduced Dirichlet composition of each pair of binary quadratic forms:
   (a) The forms $x^2 + xy + y^2$ and $x^2 + xy + y^2$ of discriminant $\Delta = -3$.
   (b) The forms $2x^2 + 7y^2$ and $3x^2 - 2xy + 5y^2$ of discriminant $\Delta = -56$.
   (c) The forms $4x^2 + 3xy + 5y^2$ and $3x^2 + xy + 6y^2$ of discriminant $\Delta = -71$.
   (d) The forms $4x^2 + 3xy + 5y^2$ and $2x^2 + xy + 9y^2$ of discriminant $\Delta = -71$.

---

3. For each discriminant Δ, find all reduced quadratic forms of discriminant Δ. For negative Δ, also compute the class number.
   (a) $\Delta = 12$.
   (b) $\Delta = 13$.
   (c) $\Delta = -24$.
   (d) $\Delta = -23$.
   (e) $\Delta = 40$.
   (f) $\Delta = -163$.

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

4. Suppose D is a squarefree integer congruent to 2 or 3 modulo 4. As you showed on homework 8, the prime 2 ramifies in $\mathcal{O}_{\sqrt{D}}$, so that $(2) = P^2$ for a prime ideal P.
   (a) Suppose $D < -2$. Show that P is not a principal ideal. [Hint: Consider the norm of a generator.]
   (b) Suppose $D < -2$. Show that the class number of $\mathcal{O}_{\sqrt{D}}$ is even.
   (c) Now suppose that $D > 2$ and that D is divisible by a prime congruent to 5 modulo 8. Show again that the class number of $\mathcal{O}_{\sqrt{D}}$ is even.

---

5. Let r be a nonzero nonunit in $\mathcal{O}_{\sqrt{D}}$ and suppose the prime factorization of the ideal (r) is $(r) = P_1 P_2 \cdots P_n$ where each P_i is a prime ideal.
   (a) Show that the product of the ideal classes $[P_1], [P_2], \ldots, [P_n]$ is the identity element in the class group.
   (b) If r is reducible in $\mathcal{O}_{\sqrt{D}}$ show that there is a nonempty proper sublist of the ideal classes $[P_1], [P_2], \ldots, [P_n]$ whose product is equal to the identity element in the class group.
   (c) Suppose there is a nonempty proper sublist of the ideal classes $[P_1], [P_2], \ldots, [P_n]$ whose product equals the identity element in the class group. Show that r is reducible.
   (d) Conclude that r is irreducible if and only if $(r) = P_1 P_2 \cdots P_n$ where no nonempty proper sublist of the ideal classes $[P_i]$ has product equal to the identity element in the class group.

---

6. The goal of this problem is to prove that if $\mathcal{O}_{\sqrt{D}}$ has class number 2 then for each nonzero nonunit r with two irreducible factorizations $s = x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m$ we have $m = n$. In other words, although $\mathcal{O}_{\sqrt{D}}$ does not have unique factorization, the *number* of terms in a factorization is still unique.

   (a) Suppose $\mathcal{O}_{\sqrt{D}}$ has class number 2. Show that all non-principal ideals of $\mathcal{O}_{\sqrt{D}}$ lie in the same ideal class, and the product of any two non-principal prime ideals is principal.

   (b) Suppose $\mathcal{O}_{\sqrt{D}}$ has class number 2 and that r is irreducible in $\mathcal{O}_{\sqrt{D}}$. Show that (r) is either a prime ideal or the product of two non-principal prime ideals. [Hint: Use 5(d).]

   (c) Suppose $\mathcal{O}_{\sqrt{D}}$ has class number 2 and that s is a nonzero nonunit with an irreducible factorization $s = x_1 x_2 \cdots x_n$ and prime ideal factorization $(s) = P_1 P_2 \cdots P_k Q_1 Q_2 \cdots Q_l$ where each P_i is principal and each Q_i is non-principal. Show that l must be even and that $n = k + l/2$. Deduce that any two irreducible factorizations of s have the same number of elements.

   Remark: If the class number of $\mathcal{O}_{\sqrt{D}}$ is greater than 1, then $\mathcal{O}_{\sqrt{D}}$ does not have unique factorization of elements. The point here is that even when the class number is greater than 1, some aspects of unique factorization still remain in $\mathcal{O}_{\sqrt{D}}$. In fact, by studying the various non-unique factorizations of different elements, one can (with substantial effort) actually reconstruct the full ideal class group.

---

7. The goal of this problem is to show there are very few imaginary quadratic integer rings with class number 1: as mentioned in class, the rings $\mathcal{O}_{\sqrt{-D}}$ for $-D = -1$, -2, -3, -7, -11, -19, -43, -67, -163 have class number 1. Now let $-D < 0$ be squarefree and suppose $\mathcal{O}_{\sqrt{-D}}$ has class number 1.

   (a) Let p be a prime such that $p < (1+D)/4$. Show that there are no elements of $\mathcal{O}_{\sqrt{-D}}$ of norm p. Deduce that p must be inert in $\mathcal{O}_{\sqrt{-D}}$, so that $-D$ is a nonsquare modulo p for odd p.

   (b) If $-D < -7$ show $-D \equiv -3 \pmod 8$, and if $-D < -11$ show that $-D \equiv -19 \pmod{24}$.

   (c) If $-D < -11$, show D must be prime. [Hint: Prime divisors of D ramify, hence exceed $(1+D)/4$.]

   (d) If $-D < -27$, show $-D$ is congruent to one of -43, -67, -163, -403, -547, -667 modulo 840.

   (e) Show that for $-1000 \leq -D < 0$, the only $\mathcal{O}_{\sqrt{-D}}$ of class number 1 are the nine values of D given above.

   Remark: If $-D < -1000$ then in order to have class number 1, by (a) all of the primes less than $(1+D)/4$ must be inert. There are already 52 odd primes less than 250, and taking the heuristic that each one has a 50% chance of being inert, we see a proportion of only $(1/2)^{52} \approx 2 \cdot 10^{-16}$ such D will be inert at all 52 of those primes! (And of course the larger $|D|$ is, the lower this heuristic probability will go.)

---

8. [Challenge] The goal of this problem is to establish the converse of problem 6 and complete the proof of the following theorem of Carlitz: $\mathcal{O}_{\sqrt{D}}$ has class number 2 if and only if $\mathcal{O}_{\sqrt{D}}$ does not have unique factorization but the number of terms in any irreducible factorization of a nonzero nonunit is unique.

   (a) Suppose $\mathcal{O}_{\sqrt{D}}$ has two distinct elements g, h of order 2 in its class group. Select distinct prime ideals P_1, P_2, P_3 with $[P_1] = g$, $[P_2] = h$, and $[P_3] = gh$. Show that the ideals P_1^2, P_2^2, P_3^2, and $P_1 P_2 P_3$ are all principal and that if $P_1^2 = (x_1)$, $P_2^2 = (x_2)$, $P_3^2 = (x_3)$, and $P_1 P_2 P_3 = (y_1)$ then x_1, x_2, x_3, y_1 are all irreducible and $x_1 x_2 x_3 = u y_1 \cdot y_1$ for some unit u. [Hint: For the irreducibility, use 5(d).]

   (b) Suppose $\mathcal{O}_{\sqrt{D}}$ has an element g of order $n \geq 3$ in its class group. Select distinct prime ideals P_1, P_2, P_3, P_4 with $[P_1] = g$, $[P_2] = g^2$, $[P_3] = g^{n-2}$, and $[P_4] = g^{n-1}$. Show that the ideals $P_1 P_4$, $P_2 P_3$, $P_1^2 P_3$, and $P_2 P_4^2$ are all principal, and that if $(x_1) = P_1 P_4$, $(x_2) = P_2 P_3$, $(y_1) = P_1^2 P_3$, and $(y_2) = P_2 P_4^2$ then x_1, x_2, y_1, y_2 are all irreducible and $x_1 x_1 x_2 = u y_1 \cdot y_2$ for some unit u.

   (c) Show that if the class number of $\mathcal{O}_{\sqrt{D}}$ is greater than 2, then there exists an element $r \in \mathcal{O}_{\sqrt{D}}$ with two irreducible factorizations of different lengths. Deduce that $\mathcal{O}_{\sqrt{D}}$ has unique factorization length but not unique factorization if and only if its class number is 2.

   Remark: For the purposes of this problem you may assume that there exist (infinitely many) prime ideals lying in each possible ideal class. This fact is not trivial to prove and is the analogue of Dirichlet's theorem on primes in arithmetic progressions for quadratic integer rings; it follows from a more general result known as the Chebotarev density theorem, which says that the prime ideals are (asymptotically) uniformly distributed among all the ideal classes in the class group.
