E. Dummit's Math 4527 ~ Number Theory 2, Spring 2025 ~ Homework 10 Solutions

---

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

   - For $17x^2 - 83xy - 24y^2$, apply $T^2$ to obtain $\boxed{17x^2 - 15xy - 122y^2}$. This form is reduced.
   - For $16x^2 - 70xy + 77y^2$, apply $T^2$ to obtain $16x^2 - 6xy + y^2$. Apply $S$ to obtain $x^2 + 6xy + 16y^2$. Apply $T^{-3}$ to obtain $\boxed{x^2 + 7y^2}$. This form is reduced.
   - For $77x^2 - 56xy + 10y^2$, apply $S$ to obtain $10x^2 + 56xy + 77y^2$. Apply $T^{-3}$ to obtain $10x^2 - 4xy - y^2$. Apply $S$ to obtain $-x^2 + 4xy + 10y^2$. Apply $T^2$ to obtain $\boxed{-x^2 + 14y^2}$. This form is reduced.

---

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 $\Delta = -3$.

   - Here $\gcd(a, a', (b + b')/2) = \gcd(1, 1, (1 + 1)/2) = 1$ so we can compose directly.
   - Then we take $A = aa'$, $B$ to be the unique integer in $(-A, A]$ satisfying $B \equiv b \pmod{2a}$, $B \equiv b' \pmod{2a'}$, and $B^2 \equiv \Delta \pmod{4aa'}$, and $C = (B^2 - \Delta)/(4A)$.
   - We obtain $A = 1 \cdot 1 = 1$, $B \equiv 1 \pmod 2$, $B \equiv 1 \pmod 2$, and $B^2 \equiv -3 \pmod 4$, so that $B = 1$, and then $C = (B^2 - \Delta)/(4A) = 1$.
   - Thus, the Dirichlet composition of $x^2 + xy + y^2$ and $x^2 + xy + y^2$ is $\boxed{x^2 + xy + y^2}$ which is reduced.

   (b) The forms $2x^2 + 7y^2$ and $3x^2 - 2xy + 5y^2$ of discriminant $\Delta = -56$.

   - Here $\gcd(a, a', (b + b')/2) = \gcd(2, 3, (0 - 2)/2) = 1$ so we can compose directly.
   - Then we take $A = aa'$, $B$ to be the unique integer in $(-A, A]$ satisfying $B \equiv b \pmod{2a}$, $B \equiv b' \pmod{2a'}$, and $B^2 \equiv \Delta \pmod{4aa'}$, and $C = (B^2 - \Delta)/(4A)$.
   - We obtain $A = 2 \cdot 3 = 6$, $B \equiv 0 \pmod 4$, $B \equiv -2 \pmod 6$, and $B^2 \equiv -56 \pmod{24}$, so that $B = 4$, and then $C = (B^2 - \Delta)/(4A) = 3$.
   - Thus, the Dirichlet composition of $2x^2 + 7y^2$ and $3x^2 - 2xy + 5y^2$ is $6x^2 + 4xy + 3y^2$. This form is not reduced, but applying $S$ yields $3x^2 - 4xy + 6y^2$ and then $T$ yields the reduced $\boxed{3x^2 + 2xy + 5y^2}$.

   (c) The forms $4x^2 + 3xy + 5y^2$ and $3x^2 + xy + 6y^2$ of discriminant $\Delta = -71$.

   - Here $\gcd(a, a', (b + b')/2) = \gcd(4, 3, (1 + 3)/2) = 1$ so we can compose directly.
   - We obtain $A = 2 \cdot 3 = 12$, $B \equiv 3 \pmod 8$, $B \equiv 1 \pmod 6$, and $B^2 \equiv -71 \pmod{24}$, so that $B = -5$, and then $C = (B^2 - \Delta)/(4A) = 2$.
   - Thus, the Dirichlet composition of $4x^2 + 3xy + 5y^2$ and $3x^2 + xy + 6y^2$ is $12x^2 - 5xy + 2y^2$. This form is not reduced, but applying $S$ yields $2x^2 + 5xy + 12y^2$ and then $T^{-1}$ yields the reduced $\boxed{2x^2 + xy + 9y^2}$.

   (d) The forms $4x^2 + 3xy + 5y^2$ and $2x^2 + xy + 9y^2$ of discriminant $\Delta = -71$.

   - Here $\gcd(a, a', (b + b')/2) = \gcd(4, 3, (1 + 3)/2) = 1$ so we cannot compose directly.
   - However if we apply $S$ to the second form we get $9x^2 - xy + 2y^2$ which will allow us to compose since now $\gcd(4, 9, (3 + (-1))/2) = 1$.
   - We obtain $A = 4 \cdot 9 = 36$, $B \equiv 3 \pmod 8$, $B \equiv -1 \pmod{18}$, and $B^2 \equiv -71 \pmod{108}$, so that $B = 35$, and then $C = (B^2 - \Delta)/(4A) = 9$.
   - Thus, the Dirichlet composition of $4x^2 + 3xy + 5y^2$ and $9x^2 - xy + 2y^2$ is $36x^2 + 35xy + 9y^2$. This form is not reduced, but applying $S$ yields $9x^2 - 35xy + 3y^2$, applying $T^2$ yields $9x^2 + xy + 2y^2$, and finally applying $S$ yields the reduced form $\boxed{2x^2 - xy + 9y^2}$.

---

3. For each discriminant $\Delta$, find all reduced quadratic forms of discriminant $\Delta$. For negative $\Delta$, also compute the class number.

(a) $\Delta = 12$.

- For $f = ax^2 + bxy + cy^2$ with $b^2 - 4ac = \Delta = 12$ we have $b$ even and $|a| \leq \frac{1}{2}\sqrt{\Delta} = \sqrt{3} \approx 1.732$, so $a = \pm 1$ and $b = 0$. So if $a = 1$ then $c = (b^2 - 12)/(4a) = -3$ while if $a = -1$ then $c = 3$.
- This yields the reduced forms $\boxed{x^2 - 3y^2}$ and $\boxed{-x^2 + 3y^2}$.

(b) $\Delta = 13$.

- For $f = ax^2 + bxy + cy^2$ with $b^2 - 4ac = \Delta = 13$ we have $b$ odd and $|a| \leq \frac{1}{2}\sqrt{\Delta} = \frac{1}{2}\sqrt{13} \approx 1.8028$, so $a = \pm 1$ and $b = 1$. Then if $a = 1$ then $c = (b^2 - 13)/(4a) = -3$ while if $a = -1$ then $c = 3$.
- This yields the reduced forms $\boxed{x^2 + xy - 3y^2}$ and $\boxed{-x^2 + xy + 3y^2}$.

(c) $\Delta = -24$.

- For $f = ax^2 + bxy + cy^2$ with $b^2 - 4ac = \Delta = -24$ we have $b$ even and $|a| \leq \sqrt{-\Delta/3} = \sqrt{8} \approx 2.8284$, so $a = \pm 1$ or $\pm 2$ and then $b = 0$ or $b = 2$.
- If $a = 1$ then $b = 0$ and $c = (b^2 + 24)/(4a) = 6$, while if $a = -1$ then $b = 0$ and $c = -6$.
- If $a = 2$ and $b = 0$ then $c = 3$, while if $a = -2$ and $b = 0$ then $c = -3$.
- Finally, $a = \pm 2$ with $b = 2$ do not yield integral values of $c$.
- So we obtain four reduced forms: $\boxed{x^2 + 6y^2}$, $\boxed{-x^2 - 6y^2}$, $\boxed{2x^2 + 3y^2}$, $\boxed{-2x^2 - 3y^2}$.
- There are two reduced positive-definite quadratic forms, so since all reduced forms for a fixed $\Delta < 0$ are inequivalent, the class number is $\boxed{2}$.

(d) $\Delta = -23$.

- For $f = ax^2 + bxy + cy^2$ with $b^2 - 4ac = \Delta = -23$ we have $b$ odd and $|a| \leq \sqrt{-\Delta/3} = \sqrt{23/3} \approx 2.8284$, so $a = \pm 1$ or $\pm 2$ and then $b = \pm 1$.
- If $a = 1$ then $b = 1$ and $c = (b^2 + 23)/(4a) = 6$, while if $a = -1$ then $b = 1$ and $c = -6$.
- If $a = 2$ and $b = \pm 1$ then $c = 3$, while if $a = -2$ and $b = \pm 1$ then $c = -3$.
- So we get six forms: $\boxed{x^2 + xy + 6y^2}$, $\boxed{-x^2 + xy - 6y^2}$, $\boxed{2x^2 + xy + 3y^2}$, $\boxed{2x^2 - xy + 3y^2}$, $\boxed{-2x^2 - xy - 3y^2}$, $\boxed{-2x^2 + xy - 3y^2}$.
- There are three reduced positive-definite quadratic forms, so as in (c), the class number is $\boxed{3}$.

(e) $\Delta = 40$.

- For $f = ax^2 + bxy + cy^2$ with $b^2 - 4ac = \Delta = 40$ we have $b$ even and $|a| \leq \frac{1}{2}\sqrt{\Delta} = \frac{1}{2}\sqrt{40} \approx 3.1623$, so $a = \pm 1, \pm 2, \pm 3$ and $b = 0, \pm 2$.
- If $a = 1$ then $b = 0$ and $c = (b^2 - 40)/(4a) = -10$ while if $a = -1$ then $b = 0$ and $c = 10$.
- If $a = \pm 2$ and $b = 0$ then $c = \mp 5$ while if $b = \pm 2$ then $c = (b^2 - 40)/(4a) = \mp 9/2$ is not integral.
- If $a = \pm 3$ and $b = 0$ then $c = \mp 10/3$ is not integral, while if $b = \pm 2$ then $c = \mp 3$. Since then $|a| = |c|$ we must also demand $b \geq 0$.
- So we get six forms $\boxed{x^2 - 10y^2}$, $\boxed{-x^2 + 10y^2}$, $\boxed{2x^2 - 5y^2}$, $\boxed{-2x^2 + 5y^2}$, $\boxed{3x^2 + 2xy - 3y^2}$, $\boxed{-3x^2 + 2xy + 3y^2}$.

(f) $\Delta = -163$.

- For $f = ax^2 + bxy + cy^2$ with $b^2 - 4ac = \Delta = -163$ we have $b$ odd and $|a| \leq \sqrt{-\Delta/3} = \sqrt{163/3} \approx 7.3711$, so $a = \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7$ and $b = \pm 1, \pm 3, \pm 5$.
- If $a = \pm 1$ then $b = 1$ and $c = (b^2 + 163)/(4a) = 41$, while if $a = -1$ then $b = 1$ and $c = -41$.
- Then $a = \pm 2$ requires $b = \pm 1$ but $c = 164/\pm 8$ is not integral.
- If $a = \pm 3$ then either $b = \pm 1$ or $\pm 3$ but $c = 164/\pm 12$ or $172/\pm 12$ is not integral.
- If $a = \pm 5$ then $b^2 \in \{1, 9, 25\}$ but $c = (b^2 + 163)/(4a)$ is 164/20, 172/20, or 198/20 is not integral.
- Finally, if $a = \pm 7$ then $b^2 \in \{1, 9, 25, 49\}$ but again $c^2 = (b^2 + 163)/(4a)$ is 164/28, 172/28, 198/28, or 212/28 and none of these are integers.
- So in fact there are just two reduced forms: $\boxed{x^2 + xy + 41y^2}$ and $\boxed{-x^2 - xy - 41y^2}$.
- There is one reduced positive-definite quadratic form, so the class number is $\boxed{1}$.

---

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.]

   - If $P$ were principal, then since its norm is 2, its generator would necessarily have norm 2.
   - However, there are no such elements in $\mathcal{O}_{\sqrt{D}}$, since $a^2 + |D|\, b^2 = 2$ has no solutions for $D \neq -1, -2$.

   (b) Suppose $D < -2$. Show that the class number of $\mathcal{O}_{\sqrt{D}}$ is even.

   - From (a) we know that the ideal class $[P]$ is not trivial. However, its square is $[P^2] = [(2)]$ which is the trivial class.
   - Thus, $[P]$ is an element of order 2 in the class group of $\mathcal{O}_{\sqrt{D}}$. Then by Lagrange's theorem, the order of the class group (i.e., the class number) must be divisible by 2.

   (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.

   - If the prime ideal $P$ with $P^2 = (2)$ were principal then its generator $a + b\sqrt{D}$ would necessarily have norm $\pm 2$, meaning that there is an integer solution to $a^2 - Db^2 = \pm 2$.
   - However, if $q \equiv 5 \pmod 8$ divides $D$, then reducing mod $q$ yields $a^2 \equiv \pm 2 \pmod q$, but this is a contradiction because 2 and $-2$ are both quadratic nonresidues modulo $q$.
   - Thus $P$ is a nonprincipal ideal whose square is principal, so as in (b) the ideal class $[P]$ has order 2, and so the order of the class group 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.

   - The product $[P_1][P_2] \cdots [P_n]$ equals the ideal class of $(r)$, which is the trivial class since $(r)$ is principal.

   (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.

   - Suppose that $r = bc$ where neither $b$ nor $c$ is a unit. Then each of the ideals $(b)$ and $(c)$ has a nontrivial prime factorization, and the product of the respective prime ideals yields the factorization of $(r)$.
   - But by the logic in (a), the subset corresponding to the prime factorization of $(b)$ has product equal to the identity element of the class group. This gives a nonempty proper subset of $[P_1], [P_2], \ldots, [P_n]$ 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.

   - Suppose there were some nonempty proper subset $S$ of $\{1, 2, \ldots, n\}$ such that $\prod_{i \in S} [P_i]$ is the identity element in the class group. This means $\prod_{i \in S} P_i$ is a principal ideal, say $(b)$, and $b$ is not a unit because $S$ is nonempty.
   - Then since $\prod_{i=1}^n P_i = [\prod_{i \in S} P_i][\prod_{i \notin S} P_i]$ and both $\prod_{i=1}^n P_i$ and $[\prod_{i \in S} P_i]$ are principal, the remaining term $[\prod_{i \notin S} P_i]$ must also be principal: thus $\prod_{i \notin S} [P_i]$ is a principal ideal also, say $(c)$: note that $c$ is not a unit since $S$ is a proper subset.
   - Then $(r) = (b)(c)$ hence $r = ubc$ for some unit $u$ and some nonunits $b$ and $c$. This means $r$ is reducible as claimed.

   (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.

   - This is just the contrapositive of (b) and (c) put together.

---

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.

   - By hypothesis, since $\mathcal{O}_{\sqrt{D}}$ has class number 2, the class group is a cyclic group $\{e, g\}$ of order 2 where $e$ is the identity and $g$ is the element of order 2. The two ideal classes therefore consist of (i) the trivial class $e$ of principal ideals, and (ii) the nontrivial class $g$ which must consist of all of the nonprincipal ideals.
   - So in particular, all the nonprincipal ideals lie in the same ideal class.
   - Furthermore, if $Q_i$ and $Q_j$ are nonprincipal, then both ideal classes $[Q_i]$ and $[Q_j]$ equal $g$, so that $[Q_i Q_j] = [Q_i][Q_j] = g^2 = e$, so $Q_i Q_j$ lies in the trivial class hence 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).]

   - By 5(d), an element $r$ is irreducible if and only if $(r) = P_1 P_2 \cdots P_n$ where no nonempty proper subset of the ideal classes $[P_i]$ has product equal to the identity element in the class group.
   - Since the class group consists only of $e$ and $g$, the ideal classes $[P_i]$ on the list cannot have $e$ or $gg$ as a proper subset, so there is at most one $e$ and at most two $g$s, and we cannot have both. Furthermore the product must be $e$ so there are an even number of $g$s.
   - This leaves only the possibilities of $e$ and $gg$. In the first case $(r)$ is the product of a single principal prime ideal (so that $(r)$ is itself prime) and in the second case $(r)$ is the product of two non-principal prime ideals.

   (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.

   - By (a) we have the product $[(s)] = [P_1][P_2] \cdots [P_k][Q_1][Q_2] \cdots [Q_l] = e^k g^l = g^l$, but since $(r)$ is principal, this product equals $e$, and so $l$ must be even.
   - For the second part, by (b) each $x_i$ factors either as a principal prime ideal $P_i$ or the product of two nonprincipal prime ideals $Q_i Q_j$. So each $P_i$ contributes one irreducible factor $x_i$ and each two $Q_j$ contribute one irreducible factor $x_j$. In total the number of irreducible factors is therefore always $k + l/2$, as desired.

**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 $p$.

   - Observe that the norm $N[\frac{a+b\sqrt{-D}}{2}] = (a^2 + Db^2)/4$ is either the square of an integer (when $b = 0$) or is at least $(1 + D)/4$ (when $b \neq 0$). Thus, if $p < (1 + D)/4$ is prime, $p$ cannot equal the norm of any element.
   - If $\mathcal{O}_{\sqrt{-D}}$ has class number 1, then the prime ideals dividing $(p)$ must be principal. But there are no elements of norm $p$ for $p < (1 + D)/4$ by the above, so any ideal of norm $p$ cannot be principal.
   - We conclude that there are no ideals of norm $p$: thus $p$ cannot split or ramify (since then the ideal factors would have norm $p$), so it must remain inert.
   - Finally, Dedekind-Kummer immediately yields that $p$ is inert if and only if $-D$ is a nonsquare modulo $p$ for odd primes $p$.

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

   - By (a) if $D < -7$ then 2 must be inert.
   - By Dedekind-Kummer, since the minimal polynomial of $\frac{1+\sqrt{-D}}{2}$ is $x^2 - x + \frac{1-D}{4}$, to be irreducible modulo 2 we need the constant term to be 1 mod 2, so $-D \equiv -3 \bmod 8$.
   - Likewise, if $-D < -11$ then by (a) we also need 3 to be inert, which again by the above occurs when $-D \equiv -2 \pmod 3$.
   - Then $-D \equiv -3 \pmod 8$ and $-D \equiv -2 \pmod 3$ which are together equivalent to $-D \equiv -19 \pmod{24}$.

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

   - Suppose instead that $D$ is composite. Then from Dedekind-Kummer, any prime divisor of $D$ ramifies hence by (b) must be less than $(1 + D)/4$.
   - But $D$ is squarefree and composite, so it must have at least two such prime divisors. But then their product would be at least $(\frac{1+D}{4})(\frac{5+D}{4})$ which exceeds $D$ when $-D < -11$, since $(\frac{1+D}{4})(\frac{5+D}{4}) > D$ for $D > 5 + 2\sqrt{5} \approx 9.47$.

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

   - By (a) if $D < -27$ then 5 and 7 must be inert.
   - By Dedekind-Kummer, this requires $-D$ to be a nonsquare modulo 5 and modulo 7, which means $-D$ is congruent to 1 or 4 modulo 5 and to 3, 5, or 6 modulo 7.
   - Putting these together with $-D \equiv -19 \pmod{24}$ using the Chinese remainder theorem, we obtain six residue classes for $-D$ modulo $24 \cdot 5 \cdot 7 = 840$: these are $-43, -67, -163, -403, -547, -667$.

   (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.

   - First we have $-D = -1, -2, -3, -7$. We have shown in class that $-D = -5, -6$ don't have class number 1. Then if $-D < -7$ then we must have $-D \equiv 1 \pmod 4$ and so $-D = -11$ works.
   - For $-D < -11$ we see $D$ must be prime and have $-D \equiv -19 \bmod 24$ by (b) and (c), so the next possible values are $-D = -19, -43, -67$.
   - Now by (d) any lower value must be congruent to one of $-43, -67, -163, -403, -547, -667$ modulo 840, which yield possible values $-43, -67, -163$ (which work) and also $-403, -547, -667, -883, -907$ above $-1000$.
   - But $403 = 13 \cdot 31$ and $667 = 23 \cdot 29$ are composite (impossible by (c)), while $-547$ is a square modulo 11 and both $-883$ and $-907$ are squares modulo 13 (impossible by (a)).
   - So in fact the only values that work are the ones listed in part (a).

**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 $P_1P_2P_3$ are all principal and that if $P_1^2 = (x_1)$, $P_2^2 = (x_2)$, $P_3^2 = (x_3)$, and $P_1P_2P_3 = (y_1)$ then $x_1, x_2, x_3, y_1$ are all irreducible and $x_1x_2x_3 = uy_1 \cdot y_1$ for some unit $u$. [Hint: For the irreducibility, use 5(d).]

   - We have $[P_1^2] = [P_1]^2 = g^2 = e$, $[P_2^2] = [P_2]^2 = h^2 = e$, $[P_3^2] = [P_3]^2 = (gh)^2 = g^2h^2 = e$, $[P_1P_2P_3] = [P_1][P_2][P_3] = (g)(h)(gh) = g^2h^2 = e$ so these ideals are principal.
   - By 4(d) since no nonempty proper sublist of $[P_1], [P_1]$ or $[P_2], [P_2]$ or $[P_3], [P_3]$ or $[P_1], [P_2], [P_3]$ has product equal to the identity we see $x_1, x_2, x_3, y_1$ are all irreducible.
   - Finally, $(x_1x_2x_3) = P_1^2P_2^2P_3^2 = (P_1P_2P_3)^2 = (y_1^2)$ so $x_1x_2x_3 = uy_1^2 = uy_1 \cdot y_1$ for some unit $u$.

   (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 $P_1P_4$, $P_2P_3$, $P_1^2P_3$, and $P_2P_4^2$ are all principal, and that if $(x_1) = P_1P_4$, $(x_2) = P_2P_3$, $(y_1) = P_1^2P_3$, and $(y_2) = P_2P_4^2$ then $x_1, x_2, y_1, y_2$ are all irreducible and $x_1x_1x_2 = uy_1 \cdot y_2$ for some unit $u$.

   - We have $[P_1P_4] = [P_1][P_4] = g^n = e$, $[P_2P_3] = [P_2][P_3] = g^n = e$, $[P_1^2P_3] = [P_1]^2[P_3] = g^n = e$, $[P_2P_4^2] = [P_2][P_4]^2 = g^{2n} = e$, so these ideals are all principal.
   - By 4(d) since no nonempty proper sublist of $[P_1], [P_4] = g, g^{n-1}$ or $[P_2], [P_3] = g^2, g^{n-2}$ or $[P_1], [P_1], [P_3] = g, g, g^{n-2}$ or $[P_2], [P_4], [P_4] = g^2, g^{n-1}, g^{n-1}$ has product equal to $e$, so $x_1, x_2, y_1, y_2$ are irreducible.
   - Finally, $(x_1x_1x_2) = (P_1P_4)^2(P_2P_3) = (P_1^2P_3)(P_4^2P_2) = (y_1y_2)$, so $x_1x_1x_2 = uy_1 \cdot y_2$ 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.

   - Suppose the class number of $\mathcal{O}_{\sqrt{D}}$ is $> 2$. If there is an element in the class group of order $n \geq 3$ then by (b) we obtain an element $r = x_1x_2x_3 = (uy_1)y_2$ with two factorizations of different lengths.
   - The only other possibility is that all nonidentity elements in the class group have order 2. Since the class number is $> 2$ there must be two distinct elements of order 2, and then by (a) we again obtain an element $r = x_1x_1x_2 = (uy_1)(y_1)$ with two factorizations of different lengths.
   - The last statement follows immediately from these observations along with the result of 6(c).

**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.

---