Hints for exercises in chapter 12

Exercise 12.1.3. Suppose that d is a fundamental discriminant and $[a, b, c]$ is an imprimitive form of discriminant d. If $h|(a, b, c)$, then $h^2|d$, so that $h = 2$. But then $D = d/h^2 \equiv 0$ or $1 \pmod 4$, a contradiction. Now suppose that d is not a fundamental discriminant. Then there exists a prime p such that $d = p^2 D$, where $D \equiv 0$ or $1 \pmod 4$. There is always a form g of discriminant D and so pg is an imprimitive form of discriminant d.

Exercise 12.1.4(c). Study the right-hand side of (12.1.2).

Exercise 12.1.5. Take determinants of both sides.

Exercise 12.1.6. First note that $b \equiv d \mod 2$, and that if $b = 2k + \delta$ with δ the least residue of $d \pmod 2$, then the change of variable $x \to x - ky$ shows that $[1, b, c] \sim [1, \delta, A]$, the principal form. The value of A must be $(\delta - d)/4$, so that the discriminant is $d = b^2 - 4c$.

Exercise 12.4.1. One example is $d = -171$. We begin by noting that $|b| \le a \le \sqrt{171/3} = \sqrt{57} < 8$ and b is odd. If $b = \pm 1$, then $ac = (1 + 171)/4 = 43$ with $a \le c$ so that $a = 1$. If $b = \pm 3$, then $ac = (9 + 171)/4 = 45$ with $a \le c$ so that $a = 1, 3, 5$ and $1 < |b|$. If $b = \pm 5$, then $ac = (25 + 171)/4 = 49$ with $a \le c$ so that $a = 1, 7$ and $1 < |b|$. If $b = \pm 7$, then $ac = (49 + 171)/4 = 55$ with $a \le c$ so that $a = 1, 5$ which are both $< |b|$, so we are left with $[1, 1, 43]$, $[3, 3, 15]$, $[5, 3, 9]$, $[5, -3, 9]$, $[7, 5, 7]$, and $[3, 3, 15]$ which is imprimitive.

Exercise 12.4.2. These are the smallest negative fundamental discriminants of class numbers 1 to 8:
For $d = -3$ we have $[1, 1, 1]$. For $d = -15$ we have $[1, 1, 4]$, $[2, 1, 2]$.
For $d = -23$ we have $[1, 1, 6]$, $[2, \pm 1, 3]$.
For $d = -39$ we have $[1, 1, 10]$, $[2, \pm 1, 5]$, $[3, 3, 4]$.
For $d = -47$ we have $[1, 1, 12]$, $[2, \pm 1, 6]$, $[3, \pm 1, 4]$.
For $d = -87$ we have $[1, 1, 22]$, $[2, \pm 1, 11]$, $[3, 3, 8]$, $[4, \pm 3, 6]$.
For $d = -71$ we have $[1, 1, 18]$, $[2, \pm 1, 9]$, $[3, \pm 1, 6]$, $[4, \pm 3, 5]$.
For $d = -95$ we have $[1, 1, 24]$, $[2, \pm 1, 12]$, $[3, \pm 1, 8]$, $[4, \pm 1, 6]$, $[5, 5, 6]$.

Exercise 12.4.3. These are the smallest even negative fundamental discriminants of class numbers 1 to 6: For $d = -4$ we have $[1, 0, 1]$; for $d = -20$ we have $[1, 0, 5]$, $[2, 2, 3]$; for $d = -56$ we have $[1, 0, 14]$, $[2, 0, 7]$, $[3, \pm 2, 5]$; for $d = -104$ we have $[1, 0, 26]$, $[2, 0, 13]$, $[3, \pm 2, 9]$, $[5, \pm 4, 6]$.

Exercise 12.5.3. Use Rabinowicz's criterion, and quadratic reciprocity.

Exercise 12.6.1. Prove and use the inequality $am^2 + bmn + cn^2 \ge am^2 - |b| \max\{|m|, |n|\}^2 + cn^2$.

Exercise 12.6.2(b). Use the smallest values properly represented by each form.

Exercise 12.6.5(c). Use exercise 12.6.2(e).

Exercise 12.6.7(c). Given a solution B, let $C = (B^2 - d)/4A$ and then $[A, B, C]$ represents A properly (by $(1, 0)$). Find reduced $f \sim [A, B, C]$ and use the transformation matrix to find the representation as in (b).

Exercise 12.8.1. Prove this one prime factor of A at a time and then use the Chinese Remainder Theorem. For each prime p, try $f(1, 0)$, $f(0, 1)$, and then $f(1, 1)$.

Exercise 12.8.2 If $f = [a, r, u]$, then the transformation $x \to x+ky, y \to y$ yields that $f \sim [a, b, c]$ where $b = r + 2ka$; that is, we can take b to be any value $\equiv r \pmod{2a}$. Similarly if $F = [A, s, v]$, then we can take b to be any value $\equiv s \pmod{2A}$. Such a b exists by the Chinese Remainder Theorem provided $r \equiv s \pmod 2$, and r and s have the same parity as the discriminants of f and F.

Exercise 12.11.3. Now $d = b^2 - 4ac = B^2 - 4AC$, and so if $p|4aA$, then $(d/p) = 0$ or 1. We will now prove that there are rational points on the curve $aAu^2 = v^2 - dw^2$, by using Legendre's version of the local-global principle. There are obviously real solutions with $u = 0$. If odd prime p divides aA but not d, then we have seen that $(d/p) = 1$. If odd prime p divides d but not aA, then $(aA/p) = (a/p)(A/p) = \sigma_f(p)\sigma_F(p) = 1$. Finally we have the case in which p divides a and d. Hence p divides b, and $p^1 \| d$ as d is fundamental, and so $p \nmid (a/p)c$. So writing $a = pa', b = pb', d = pD$ we have $D = p(b')^2 - 4a'c$ which implies that $(-a'cD/p) = 1$. We also have $(Ac/p) = \sigma_f(p)\sigma_F(p) = 1$, and so $(-a'AD/p) = (-a'cD/p)(Ac/p) = 1$ as needed. Dividing through by u we have $aA = t^2 - d\gamma^2$ for some rationals t, γ; letting $t = 2a\alpha + b\gamma$ we deduce that $A = f(\alpha, \gamma)$ for some $\alpha, \gamma \in \mathbb{Q}$. We can select any $\beta, \delta \in \mathbb{Q}$ for which $\alpha\delta - \beta\gamma = 1$ to obtain a transformation for f to a form $Ax^2 + b'xy + c'y^2$. We now let $x = X + kY, y = Y$ where k is chosen so that $2AK + b' = B$ to obtain a form $Ax^2 + Bxy + C'y^2$. Since both transformations have determinant 1, we see that $B^2 - AC' = d$ and so $C' = C$. Hence f and F are equivalent over the rationals.

Exercise 12.15.1(a). Use Euler's criterion and Corollary 7.5.2.

Exercise 12.15.3(c). Use exercise 12.15.2(c).

Exercise 12.18.2(a). If even $N = a^2 + b^2 + c^2 + d^2$ with $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$, then $N/2 = (\frac{a+b}{2})^2 + (\frac{a-b}{2})^2 + (\frac{c+d}{2})^2 + (\frac{c-d}{2})^2$. If $N \equiv 1 \pmod 4$ with $N = a^2 + b^2 + c^2 + d^2$, then we may let a be odd, the rest even. To obtain representations of $2N$ we have the first two squares as $(a+b)^2 + (a-b)^2$, the other two even. This yields back a and the choice of b and so it is a 1-to-3 map. We have a similar construction if $N \equiv 3 \pmod 4$.

Exercise 12.18.3(c). Use Legendre's Theorem (Theorem 12.5). (d) Let $u = a + b - c - d, v = a - b + c - d, w = a - b - c + d$, etc. (e) Be careful with the cases where $u = v$ etc.