Quadratic Number Theory
Exercise Solutions

J. L. Lehman

Section 0.1. Linear Equations and Congruences.

(1) (a) $679 = 23 \cdot 29 + 12$.
(b) $-782 = 57 \cdot -14 + 16$.
(c) $-3216 = 67 \cdot -48 + 0$.

(2) Suppose that p divides ab, but that p does not divide a. If p is prime, then $\gcd(p, a) = 1$, since $\gcd(p, a)$ is a positive divisor of p but cannot equal p. Corollary 0.1.3 implies that then p divides b. If n is composite, then n has a positive divisor a other than 1 and n. In that case, $n = ab$ with $1 < a, b < n$. But now n divides ab but cannot divide a or b.

(3) Suppose that a and b both divide n. Then $n = bq$ for some integer q, so that a divides bq. If $\gcd(a, b) = n$, then Corollary 0.1.3 implies that a divides qd, say $qd = ar$ for some integer r. But now $nd = (bq)d = b(qd) = b(ar) = (ab)r$, and ab divides nd.

(4) If a and b are not both zero and $d = \gcd(a, b)$, then $ab/d = a(b/d) = b(a/d)$ is a common multiple of a and b. (Note that b/d and a/d are integers if $d = \gcd(a, b)$.) If n is a common multiple of a and b, then Exercise 3 shows that ab/d divides n. So $m = |ab|/d$ is the (positive) least common multiple of a and b by definition.

(5) (a) $\gcd(504, 186) = 6 = 504 \cdot -7 + 186 \cdot 19$.
(b) $\gcd(1247, 913) = 1 = 1247 \cdot -41 + 913 \cdot 56$.
(c) $\gcd(1350, 1401) = 3 = 1350 \cdot -55 + 1401 \cdot 53$.

(6) (a) Since $\gcd(567, 98) = 7 = 567(-5) + 98(29)$, then $203 = 29 \cdot 7 = 567(-145) + 98(841)$. All solutions of $567x + 98y = 203$ have the form $\left(-145 + \frac{98}{7} \cdot q, 841 - \frac{567}{7} \cdot q\right) = (-145 + 14q, 841 - 81q)$ with q an arbitrary integer. (Other expressions for this general solution are possible. For instance, when $q = 1$, then $x = 9$ and $y = -50$. We can also write $(x, y) = (9 + 14q, -50 - 81q)$ as the general solution.)
(b) No solutions of $504x + 186y = 202$ exist, since $\gcd(504, 186) = 6$ does not divide 202.
(c) Here $204 = 34(6) = 34(504 \cdot -7 + 186 \cdot 19) = 504(-238) + 186(646)$. One expression for the general solution of $504x + 186y = 204$ is $(-238 + 31q, 646 - 84q)$.
(d) $(x, y) = (-112 + 913q, 153 - 1247q)$ is one expression for the general solution of $1247x + 913y = 25$.
(e) $(x, y) = (106 + 467q, -100 - 450q)$ is one expression for the general solution of $1350x + 1401y = 3000$.

(7) There are finitely many possible remainders on division of an integer by m, so there must be some repetition of those remainders for the infinite set of positive powers of a. So there must be integers $0 \leq r < s$ so that $a^s \equiv a^r \pmod{m}$. If $\gcd(a, m) = 1$, we can cancel r terms of a from this congruence, by the congruence cancellation property, without affecting the modulus, and conclude that $a^{s-r} \equiv 1 \pmod{m}$. But $t = s - r$ is positive.

(8) Let $t = \text{ord}_m(a)$, where a is relatively prime to m.
(a) If $n = tq$, then $a^n = (a^t)^q \equiv 1^q \equiv 1 \pmod{m}$. Conversely, if $a^n \equiv 1 \pmod{m}$ and we write $n = tq + r$ with $0 \leq r < t$, then $1 \equiv a^n \equiv (a^t)^q a^r \equiv 1^q a^r \equiv a^r \pmod{m}$. This contradicts the definition of t if r is positive, so we must conclude that $r = 0$, and then t divides n.
(b) If $\gcd(a, m) = 1$, then by the congruence cancellation property $a^s \equiv a^r \pmod{m}$ if and only if $a^{s-r} \equiv 1 \pmod{m}$. But by part (a), this is true if and only if t divides $s - r$, that is, $s \equiv r \pmod{t}$.

(9) (a) Since $\gcd(23, 39) = 1 = 23 \cdot 17 + 39 \cdot -10$, then $18 \cdot 17 = 306 \equiv 33 \pmod{39}$ is the unique solution of $23x \equiv 18 \pmod{39}$.
(b) $\gcd(186, 504) = 6$ divides 246, so six solutions of $186x \equiv 246 \pmod{504}$ exist. Here $246 = 41 \cdot 6 = 41(504 \cdot -7 + 186 \cdot 19)$, using calculations from Exercise 5, thus every

solution of $186x \equiv 246 \pmod{504}$ has the form $x = 41 \cdot 19 + \frac{504}{6}q = 779 + 84q$ for some integer q. The distinct solutions in $\mathbb{Z}_{504}$ are 23, 107, 191, 275, 359, and 443.

(c) $\gcd(221, 247) = 13$ does not divide 19, so no solutions of $221x \equiv 19 \pmod{247}$ exist.

(d) Here $\gcd(221, 247) = 13 = 221 \cdot 9 + 247 \cdot -8$ divides $117 = 9 \cdot 13$. The solutions of $221x \equiv 117 \pmod{247}$ are given by $x = 9 \cdot 9 + \frac{247}{13}q = 81 + 19q$. Thirteen solutions are distinct in $\mathbb{Z}_{247}$: 5, 24, 43, 62, 81, 100, 119, 138, 157, 176, 195, 214, and 233.

(10) (a) Here $\gcd(13, 41) = 1 = 13 \cdot 19 + 41 \cdot -6 = 247 - 246$. So a simultaneous solution of $x \equiv 7 \pmod{13}$ and $x \equiv 29 \pmod{41}$ is given by $x = -246 \cdot 7 + 247 \cdot 29 = 5441$. This solution is unique modulo $13 \cdot 41 = 533$, that is, $x \equiv 5441 \equiv 111 \pmod{533}$.

(b) With $\gcd(63, 82) = 1 = 63 \cdot -13 + 82 \cdot 10$, the unique solution of $x \equiv 17 \pmod{63}$ and $x \equiv 14 \pmod{82}$ is congruent to $17 \cdot 82 \cdot 10 + 14 \cdot 63 \cdot -13$ modulo $63 \cdot 82 = 5166$. That is, $x \equiv 2474 \pmod{5166}$ is the unique solution of the pair of congruences.

(c) Using a calculation from Exercise 5, the unique solution of $x \equiv 374 \pmod{1247}$ and $x \equiv 821 \pmod{913}$ is given by $x \equiv 374 \cdot 913 \cdot 56 + 821 \cdot 1247 \cdot -41$ modulo $1247 \cdot 913 = 1138511$, that is $x \equiv 1055336 \pmod{1138511}$.

(11) If x simultaneously satisfies $ax \equiv c \pmod{m}$ and $bx \equiv d \pmod{m}$, then $b(ax) \equiv bc \pmod{m}$ and $a(bx) \equiv ad \pmod{m}$. So abx is congruent to both bc and ad modulo m, and so m must divide $ad - bc$. Conversely, suppose that $\gcd(a, b) = 1$ and that m divides $ad - bc$, say with $as + bt = 1$ and $ad - bc = mu$ for some integers s, t, and u. If $x = cs + dt$, then $ax = acs + adt = acs + (bc + mu)t = c(as + bt) + m(ut) \equiv c \pmod{m}$ and $bx = b(cs + dt) = (ad - mu)s + bdt = d(as + bt) + m(-us) \equiv d \pmod{m}$. That is, $ax \equiv c \pmod{m}$ and $bx \equiv d \pmod{m}$ have a simultaneous solution. If y is also a solution, then $a(x - y) = mq$ and $b(x - y) = mr$ for some integers q and r. But then $x - y = (as + bt)(x - y) = mqs + mrt = m(qs + rt)$, and so $x \equiv y \pmod{m}$.

Section 0.2. Quadratic Congruences Modulo Primes.

(1) Suppose that $b^2 \equiv a \pmod{p}$ where p is an odd prime.

(a) Since $(-b)^2 = b^2$, then $-b \equiv p - b \pmod{p}$ also satisfies $x^2 \equiv a \pmod{p}$.

(b) If $-b \equiv b \pmod{p}$, then p divides $2b$. Since p is odd, then p divides b. Conversely, if $b \equiv 0 \pmod{p}$, then $-b \equiv 0 \equiv b \pmod{p}$. In this case, $b^2 \equiv 0 \pmod{p}$ as well, so that $x^2 \equiv a \pmod{p}$ has exactly one solution if and only if p divides a.

(c) If b and c are solutions of $x^2 \equiv a \pmod{p}$, then $b^2 \equiv c^2 \pmod{p}$, which implies that p divides $c^2 - b^2 = (c - b)(c + b)$. Since p is prime, then either p divides $c - b$ or p divides $c + b = c - (-b)$. Thus either $c \equiv b \pmod{p}$ or $c \equiv -b \pmod{p}$, and $x^2 \equiv a \pmod{p}$ has no more than two solutions.

(2) The congruence $x^2 \equiv 1 \pmod{p}$ has two distinct solutions, 1 and $-1 \equiv p - 1 \pmod{p}$, modulo every odd prime p. So $\left(\frac{1}{p}\right) = 1$.

(3) If $a \equiv b \pmod{p}$, then $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ have the same solutions, and so the same number of solutions. Thus $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(4) Euler's criterion implies that $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. But each side of this congruence is 1 or -1, so this congruence is an equation since $p \geq 3$. For the final equation, note that if $p = 4q + 1$, then $\frac{p-1}{2} = 2q$ is even, while if $p = 4q + 3$, then $\frac{p-1}{2} = 2q + 1$ is odd.

(5) Here $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$, using Euler's criterion and properties of exponents. All symbols are 1, 0, or -1, as is the product of two symbols, and so this congruence is an equation.

(6) (a) $\left(\frac{-19}{43}\right) = \left(\frac{-1}{43}\right)\left(\frac{19}{43}\right) = -1 \cdot -\left(\frac{43}{19}\right) = \left(\frac{5}{19}\right)$, since 19 and 43 are both congruent to 3 modulo 4. Now with $5 \equiv 1 \pmod{4}$, we have $\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)^2 = 1$.

(b) $\left(\frac{35}{67}\right) = \left(\frac{5}{67}\right)\left(\frac{7}{67}\right) = \left(\frac{67}{5}\right) \cdot -\left(\frac{67}{7}\right) = -\left(\frac{2}{5}\right)\left(\frac{4}{7}\right) = -(-1) \cdot 1^2 = 1$.

(c) $\left(\frac{46}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{23}{97}\right) = \left(\frac{97}{23}\right) = \left(\frac{5}{23}\right)$, since $97 \equiv 1 \pmod 4$ and $97 \equiv 1 \pmod 8$. Now $\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$.

(7) Suppose that $q \equiv 3 \pmod 4$. If $p \equiv 1 \pmod 4$, then $\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = 1 \cdot \left(\frac{p}{q}\right)$. On the other hand, if $p \equiv 3 \pmod 4$, then $\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = -1 \cdot -\left(\frac{p}{q}\right)$. So $\left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right)$ in either case.

(8) (a) We can transform $x^2 + x - 3 \equiv 0 \pmod{17}$ into $(2x+1)^2 \equiv 13 \pmod{17}$. Since $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = 1$, this congruence has two solutions. Trial-and-error shows that $13 \equiv 64 \pmod{17}$, so we solve $2x + 1 \equiv 8 \pmod{17}$ and $2x + 1 \equiv -8 \pmod{17}$ for $x = 12$ and $x = 4$ respectively.

(b) $3x^2+5x+8 \equiv 0 \pmod{19}$ transforms into $(6x+5)^2 \equiv -71 \pmod{19}$, or $(6x+5)^2 \equiv 5 \pmod{19}$. Here $\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = 1$, so that two solutions exist, and we find that $6x + 5 \equiv \pm 9 \pmod{19}$. Solving these linear congruences, we find that $x = 4$ and $x = 7$ are the two solutions of $3x^2 + 5x + 8 \equiv 0 \pmod{19}$.

(c) $5x^2-x+1 \equiv 0 \pmod{23}$ transforms into $(10x-1)^2 \equiv -19 \pmod{23}$, or $(10x-1)^2 \equiv 4 \pmod{23}$, with solutions given by solving $10x - 1 \equiv \pm 2 \pmod{23}$ for $x = 16$ and $x = 21$.

Section 0.3. Quadratic Congruences Modulo Composite Integers.

(1) Let $f(x) = x^2 + x - 1$ so that $f'(x) = 2x + 1$. Note that $f(x) \equiv 0 \pmod p$ has the same solutions as $(2x + 1)^2 \equiv 5 \pmod p$ when p is an odd prime. Here $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$ if and only if p is congruent to 1 or 4 modulo 5. To simplify calculations, we can note that if $f(x) \equiv 0 \pmod m$ has a solution r, then $-r - 1$ is also a solution.

(a) $f(x) \equiv 0 \pmod 5$ has one solution, $x = 2$. Here $f'(2) = 5$ and $f(2) = 5$, and since $5t \equiv -1 \pmod 5$ has no solutions, it follows that $f(x) \equiv 0 \pmod{25}$ has no solutions. No solutions of $f(x) \equiv 0 \pmod{125}$ can exist either.

(b) $f(x) \equiv 0 \pmod{11}$ has solutions 3 and $-4 \equiv 7 \pmod{11}$ by direct calculation. When $r = 3$, then $f'(r) = 7$ and $f(r) = 11$. The congruence $7t \equiv -1 \pmod{11}$ has one solution, $t = 3$, and so $s = 3 + 11(3) = 36$ is a solution of $f(x) \equiv 0 \pmod{121}$. A second solution, using $r = -4$ or $r = 7$, is $s = -37 \equiv 84 \pmod{121}$. Now $f'(36) = 73 \equiv 7 \pmod{11}$ and $f(36) = 1331$. The congruence $7t \equiv -\frac{f(36)}{11^2} \equiv -11 \pmod{11}$ has solution $t = 0$, and thus $36 + 0(121) = 36$ is a solution of $f(x) \equiv 0 \pmod{1331}$. The second solution is $-37 \equiv 1294 \pmod{1331}$.

(c) $f(x) \equiv 0 \pmod{19}$ has solutions 4 and $-5 \equiv 14 \pmod{19}$. When $r = 4$, then $f'(r) = 9$ and $f(r) = 19$. The congruence $9t \equiv -1 \pmod{19}$ has solution $t = 2$ and so $s = 4 + 19(2) = 42$ is a solution of $f(x) \equiv 0 \pmod{361}$. The second solution is $-43 \equiv 318 \pmod{361}$. Now when $r = 42$, we have $f'(r) = 85 \equiv 9 \pmod{19}$ and $f(r) = 1805 = 5 \cdot 361$. The congruence $9t \equiv -5 \pmod{19}$ has solution $t = 10$, and thus $42 + 361(10) = 3652$ satisfies $f(x) \equiv 0 \pmod{6859}$. A second solution is given by $-3653 \equiv 3206 \pmod{6859}$.

(2) (a) Since $f(x) \equiv 0 \pmod 5$ has one solution, $q = 2$, and $f(x) \equiv 0 \pmod{11}$ has two solutions, $r = 3$ and $r = 7$, then $f(x) \equiv 0 \pmod{55}$ has two solutions, obtained by solving $x \equiv 2 \pmod 5$ and $x \equiv 3 \pmod{11}$ for $x = -8 \equiv 47 \pmod{55}$, and $x \equiv 2 \pmod 5$ and $x \equiv 7 \pmod{11}$ for $x \equiv 7 \pmod{55}$. (Again, we can also use the fact that if x is a solution, then $-x - 1$ is also a solution.)

(b) $f(x) \equiv 0 \pmod{209}$ has four solutions, obtained by solving $x \equiv q \pmod{11}$ and $x \equiv r \pmod{19}$ where $r = 3$ or 7 and $s = 4$ or 14. We find that these systems yield the solutions 14, 80, $-81 \equiv 128 \pmod{209}$ and $-15 \equiv 194 \pmod{209}$.

(c) $f(x) \equiv 0 \pmod{605}$ has two solutions, which we find by solving $x \equiv 2 \pmod 5$ and $x \equiv r \pmod{121}$ with $r = 36$ or $r = 84$. We find that $x = 157$ and $x = -158 \equiv 447 \pmod{605}$ are the solutions.

(d) $f(x) \equiv 0 \pmod{2299}$ has four solutions, which we find to be 641, 1125, $-1126 \equiv 1173 \pmod{2299}$, and $-642 \equiv 1657 \pmod{2299}$ by solving all systems of the form $x \equiv q \pmod{121}$ and $x \equiv r \pmod{19}$ with $q = 36$ or 84, and $r = 4$ or 14.

(3) $f(x) = x^2 + 18x + 1$ has discriminant $\Delta = 320 = 2^6 \cdot 5$. Here $\ell = 3$ since $5 \equiv 1 \pmod 4$. If $e > 2\ell = 6$, then $n_{2^e}(f) = 0$ since $\left(\frac{5}{2}\right) = -1$. On the other hand, if $e \leq 6$ is written as $e = 2k + r$ with $r = 0$ or 1, then $n_{2^e}(f) = 2^k$. The following table lists all possibilities.

e	0	1	2	3	4	5	6	7	8	$\cdots$
$n_{2^e}(f)$	1	1	2	2	4	4	8	0	0	$\cdots$

Since $f'(x) = 2x + 18$ is even for every x, the congruence $f'(x) \equiv -\frac{f(x)}{2^e} \pmod 2$ always has either two solutions or no solutions, depending on whether the right-hand side is even or odd. Direct calculation shows that $x = 1$ is the only solution of $f(x) \equiv 0 \pmod 2$. With $f(1) = 20$, we then find two solutions of $f(x) \equiv 0 \pmod 4$, that is, $x = 1 + 2(0) = 1$ and $x = 1 + 2(1) = 3$. Now $-f(1)/4 = -5$ is odd, but $-f(3)/4 = -16$ is even, and so there are two solutions of $f(x) \equiv 0 \pmod 8$, $x = 3 + 4(0) = 3$ and $x = 3 + 4(1) = 7$. Then we find that $-f(3)/8 = -8$ and $-f(7)/8 = -22$ are both even, and so 3, 7, 11, and 15 are all solutions of $f(x) \equiv 0 \pmod{16}$. Now $-f(3)/16 = -4$ and $-f(11)/16 = -20$ are even, while $-f(7)/16 = -11$ and $-f(15)/16 = -31$ are both odd, thus there are four solutions of $f(x) \equiv 0 \pmod{32}$, that is, 3, 11, 19, and 27. With $-f(3)/32 = -2$, $-f(11)/32 = -10$, $-f(19)/32 = -22$, and $-f(27)/32 = -38$ all even, we find that 3, 11, 19, 27, 35, 43, 51, and 59 are all solutions of $f(x) \equiv 0 \pmod{64}$. But finally, $-f(x)/64$ is not even for any of these eight values of x, and so $f(x) \equiv 0 \pmod{128}$ has no solutions. Therefore, $f(x) \equiv 0 \pmod{2^e}$ can have no solutions for $e \geq 7$.

(4) Let $f(x) = x^2 + x - 1$, which has discriminant $\Delta = 5$. Here $f(x) \equiv 0 \pmod m$ has no solutions if m is divisible by 25 or by any prime $p \equiv 2, 3 \pmod 5$. If this is not the case, and m has t distinct prime divisors satisfying $p \equiv 1, 4 \pmod 5$, then $f(x) \equiv 0 \pmod m$ has 2^t distinct solutions modulo m.

(5) If $q = q_1 \cdot q_2 \cdots q_k$ with each q_i prime, and $f(x) \equiv 0 \pmod q$ has a solution for some polynomial $f(x)$ with discriminant Δ, then each $f(x) \equiv 0 \pmod{q_i}$ has a solution and so $\left(\frac{\Delta}{q_i}\right) = 1$ for each i. (Here we are assuming that q and Δ have no common divisors.) But then the product of all of those symbols, which is $\left(\frac{\Delta}{q}\right)$, is also 1. On the other hand, this product can also be 1 if there are any even number of symbols equal to -1, in which case $f(x) \equiv 0 \pmod q$ has no solutions.

Section 1.1 Sums of Two Squares.

(1) For each a, we test $\sqrt{a/2} < x < \sqrt{a}$ to find $a = x^2 + y^2$.

(a) $a = 313 = 13^2 + 12^2$.

(b) $a = 377 = 16^2 + 11^2 = 19^2 + 4^2$.

(c) $a = 433 = 17^2 + 12^2$.

(2) (a) $481 = 13 \cdot 37 = (3^2+2^2)(6^2+1^2) = (3 \cdot 6+2 \cdot 1)^2+(3 \cdot 1-2 \cdot 6)^2 = (3 \cdot 6-2 \cdot 1)^2+(3 \cdot 1+2 \cdot 6)^2$. In standard form, $481 = 20^2 + 9^2 = 16^2 + 15^2$.

(b) $493 = 17 \cdot 29 = (4^2 + 1^2)(5^2 + 2^2) = 22^2 + 3^2 = 18^2 + 13^2$.

(c) $697 = 17 \cdot 41 = (4^2 + 1^2)(5^2 + 4^2) = 24^2 + 11^2 = 21^2 + 16^2$.

(d) $949 = 13 \cdot 73 = (3^2 + 2^2)(8^2 + 3^2) = 30^2 + 7^2 = 25^2 + 18^2$.

(e) $1537 = 29 \cdot 53 = (5^2 + 2^2)(7^2 + 2^2) = 39^2 + 4^2 = 31^2 + 24^2$.

(f) $8633 = 89 \cdot 97 = (8^2+5^2)(9^2+4^2) = 92^2+13^2 = 77^2+52^2$.

(3) (a) $107^2+1 = 229 \cdot 50$. Here $107 \equiv 7 \pmod{50}$ and $1 \equiv 1 \pmod{50}$, and we find that $7^2+1^2 = 50 = 50 \cdot 1$. So $229 \cdot 50 \cdot 50 \cdot 1 = (107^2+1^2)(7^2+1^2) = (107 \cdot 7 + 1 \cdot 1)^2 + (107 \cdot 1 - 7 \cdot 1)^2 = 750^2 + 100^2$. We can cancel 50^2 from both sides to conclude that $229 = 15^2 + 2^2$.

(b) $60^2+1 = 277 \cdot 13$. With $60 \equiv -5 \pmod{13}$ and $1 \equiv 1 \pmod{13}$, and $(-5)^2+1^2 = 26 = 13 \cdot 2$, we then see that $277 \cdot 13 \cdot 13 \cdot 2 = (60^2+1^2)((-5)^2+1^2) = (-299)^2+65^2$. We cancel 13^2 to write $277 \cdot 2 = (-23)^2 + 5^2$. Now with $-23 \equiv 1 \pmod{2}$ and $5 \equiv 1 \pmod{2}$, and $1^2+1^2 = 2 \cdot 1$, we then have $277 \cdot 2 \cdot 2 \cdot 1 = ((-23)^2+5^2)(1^2+1^2) = (-18)^2+(-28)^2$. Cancelling 2^2 yields $277 = (-9)^2 + (-14)^2$, or $277 = 14^2 + 9^2$ in standard form.

(c) $148^2+1 = 337 \cdot 65$. Here $148 \equiv 18 \pmod{65}$, and $18^2+1^2 = 65 \cdot 5$. Thus $337 \cdot 65 \cdot 65 \cdot 5 = (148^2+1^2)(18^2 1^2) = 2665^2+130^2$, and by cancelling 65^2 we find that $337 \cdot 5 = 41^2+2^2$. But now $41 \equiv 1 \pmod{5}$ and $2 \equiv 2 \pmod{5}$, with $1^2+2^2 = 5 \cdot 1$. Thus $337 \cdot 5 \cdot 5 \cdot 1 = (41^2+2^2)(1^2+2^2) = 45^2+80^2$, and we conclude that $337 = 9^2+16^2 = 16^2+9^2$.

(d) $52^2+1 = 541 \cdot 5$, with $52 \equiv 2 \pmod{5}$. We find that $541 \cdot 5 \cdot 5 \cdot 1 = (52^2+1^2)(2^2+1^2) = 105^2+50^2$, and so $541 = 21^2+10^2$.

(4) For each prime p, we first write p as a sum of two squares by testing $\sqrt{p/2} < x < \sqrt{p}$.

(a) $p = 509 = 22^2+5^2$. Here $1 = 22(-2)+5(9)$ by the Euclidean algorithm, and then we find that $x = 22(9)-5(-2) = 208$ is a solution of $x^2 \equiv -1 \pmod{509}$.

(b) $p = 757 = 26^2+9^2$. Now $1 = 26(-1)+9(3)$, and so $x = 26(3)-9(-1) = 87$ satisfies $x^2 \equiv -1 \pmod{757}$.

(c) $p = 953 = 28^2+13^2$, and $1 = 28(-6)+13(13)$, and we find that $x = 28(13)-13(-6) = 442$ satisfies $x^2 \equiv -1 \pmod{953}$.

(d) $p = 1009 = 28^2+15^2$, and $1 = 28(7)+15(-13)$, so that $x = 28(-13)-15(7) = -469$ satisfies $x^2 \equiv -1 \pmod{1009}$.

(5) (a) $125 = 11^2+2^2 = 10^2+5^2$.

(b) $180 = 12^2+6^2$.

(c) $325 = 18^2+1^2 = 17^2+6^2 = 15^2+10^2$.

(d) $985 = 29^2+12^2 = 27^2+16^2$.

(e) $1000 = 30^2+10^2 = 26^2+18^2$.

(f) $27625 = 164^2+27^2 = 144^2+83^2 = 141^2+88^2 = 132^2+101^2 = 165^2+20^2 = 160^2+45^2 = 155^2+60^2 = 120^2+115^2$.

Section 1.2 Gaussian Integers.

(1) If $w = a+bi$ and $z = c+di$, then $\overline{w+z} = (a+c)-(b+d)i = (a-bi)+(c-di) = \overline{w}+\overline{z}$. Likewise, $\overline{wz} = (ac-bd)-(ad+bc)i = (a-bi)(c-di) = \overline{w} \cdot \overline{z}$.

(2) By definition, m divides $q+ri$ in $\mathbb{Z}[i]$ if and only if $q+ri = m(s+ti)$ for some $s+ti \in \mathbb{Z}[i]$. But this occurs if and only if $q = ms$ and $r = mt$, that is, m divides q and m divides s in $\mathbb{Z}$.

(3) Let u, v, and w be Gaussian integers.

(a) Suppose that v divides w, say with $w = vz$ for some z in $\mathbb{Z}[i]$. Then $N(w) = N(vz) = N(v) \cdot N(z)$. Since $N(z)$ is a rational integers, it follows that $N(v)$ divides $N(w)$ in $\mathbb{Z}$.

(b) By definition, u is a unit in $\mathbb{Z}[i]$ if u divides 1. But then $N(u)$ divides $N(1) = N(1+0i) = 1^2+0^2 = 1$ in $\mathbb{Z}$, by part (a). The only divisors of 1 in $\mathbb{Z}$ are 1 and -1, and since the norm of a Gaussian integer cannot be negative, we conclude that $N(u) = 1$. Conversely, suppose that $N(u) = u \cdot \overline{u} = 1$ for some $u \in \mathbb{Z}[i]$. Here $\overline{u}$ is also a Gaussian integer, so it follows that u divides 1 in $\mathbb{Z}[i]$.

(c) By definition, v and w are associates in $\mathbb{Z}[i]$ if v divides w and w divides v. But then $N(v)$ divides $N(w)$ and $N(w)$ divides $N(v)$ in $\mathbb{Z}$. For rational integers, this occurs if

and only if $N(w) = \pm N(v)$, but the norm of a Gaussian integer cannot be negative, so it follows that $N(v) = N(w)$.

(4) By the preceding exercise, $u = a + bi$ is a unit in $\mathbb{Z}[i]$ if and only if $N(u) = a^2 + b^2 = 1$. We conclude that either $a^2 = 1$ and $b^2 = 0$, so $a = \pm 1$ and $b = 0$, or $a^2 = 0$ and $b^2 = 1$, so $a = 0$ and $b = \pm 1$. That is, $u = 1$, -1, i, or $-i$.

(5) If $w = uv$ for some unit u of $\mathbb{Z}[i]$, then $v = u^{-1}w$, where $u^{-1} = \overline{u}$ is also a Gaussian integer. It follows that v divides w and w divides v, and so v and w are associates. Conversely, if v divides w and w divides v, say with $w = vu$ and $v = wz$ for some $u, z \in \mathbb{Z}[i]$, then $w = vu = w(zu)$. If $w = 0$, then $v = wz = 0$ and we have $w = 1 \cdot v$. If $w \neq 0$, we can cancel w from the equation $w = w(zu)$ and conclude that $zu = 1$. But then u divides 1, so is a unit of $\mathbb{Z}[i]$, and we have that $w = uv$. Thus using Exercise 4, if $v = a + bi$, then its associates are $1 \cdot v = a + bi$, $-1 \cdot v = -a - bi$, $i \cdot v = -b + ai$, and $-i \cdot v = b - ai$.

(6) Define $\sim$ on $\mathbb{Z}[i]$ by $v \sim w$ if and only if v is an associate of w. By Exercise 5, we can say that $v \sim w$ if and only if $w = uv$ for some unit u of $\mathbb{Z}[i]$.

(a) Since $v = 1 \cdot v$, then $v \sim v$ and $\sim$ is reflexive. If $w = uv$, then $v = u^{-1}w = \overline{u}w$, with $\overline{u}$ also a unit in $\mathbb{Z}[i]$. Thus if $v \sim w$, then $w \sim v$ and $\sim$ is symmetric. If $w = u_1 v$ and $z = u_2 w$ for some units u_1 and u_2, then $z = u_2(u_1 v) = (u_2 u_1)v$. Here $u_2 u_1$ is a unit since its norm is 1. Thus we can say that if $v \sim w$ and $w \sim z$, then $v \sim z$, and so $\sim$ is transitive.

(b) Suppose that $v = u_1 u$ and $z = u_2 w$ for some units u_1 and u_2. Then $vz = (u_1 u_2)uw$, and $u_1 u_2$ is a unit, as noted above. Therefore if $u \sim v$ and $w \sim z$, then $uw \sim vz$.

(c) Again suppose that $v = u_1 u$ and $z = u_2 w$ for some units u_1 and u_2. If u divides w, then $w = uz_1$ for some z_1 in $\mathbb{Z}[i]$. But then $z = u_2 w = u_2 u z_1 = (u_2 u_1^{-1} z_1)v$, and it follows that v divides z. The converse is established similarly.

(7) If $N(w) = p$ is prime in $\mathbb{Z}$, but $w = uv$ in $\mathbb{Z}[i]$, then $p = N(u) \cdot N(v)$. Since each norm is a positive rational integer, one of them must equal 1. But if $N(u) = 1$, for instance, then u is a unit in $\mathbb{Z}[i]$. So it is impossible to write w as a product of two Gaussian integers neither of which is a unit, and w is irreducible by definition.

(8) If not every reducible Gaussian integer can be written as a product of irreducible elements of $\mathbb{Z}[i]$, we can assume that w is such an element with $N(w)$ as small as possible. Since w is reducible, it is possible to write $w = uv$ with neither u nor v a unit in $\mathbb{Z}[i]$. But then $N(w) = N(u) \cdot N(v)$, with neither $N(u)$ nor $N(v)$ equal to 1, so that $N(w) > N(u), N(v) > 1$. But now by our assumption both u and v can be expressed as a product of irreducible elements, and thus $w = uv$ can be written as such a product as well, contrary to assumption.

(9) (a) We find that $\frac{v}{w} = \frac{37-10i}{4+i} = \frac{(37-10i)(4-i)}{17} = \frac{138}{17} + \frac{-77}{17}i$. The closest integers to $\frac{138}{17}$ and $\frac{-77}{17}$ are 8 and -4 respectively. If $z = 8 - 4i$, we calculate that $u = v - wz = 1 - 2i$. So $37 - 10i = (4 + i)(8 - 4i) + (1 - 2i)$, with $5 = N(1 - 2i) < N(4 + i) = 17$.

(b) By the same approach, $13 + 19i = (3 + 4i)(5) + (-2 - i)$, with $5 = N(-2 - i) < N(3 + 4i) = 25$.

(c) $41 + 9i = (9 + 7i)(3 - 2i) + 6i$, with $36 = N(6i) < N(9 + 7i) = 130$.

(10) If not every reducible Gaussian integer can be written uniquely as a product of irreducible elements of $\mathbb{Z}[i]$, we can assume that w is such an element with $N(w)$ as small as possible. Let $w = u_1 \cdot u_2 \cdots u_k$ and $w = z_1 \cdot z_2 \cdots z_\ell$ with each u_i and z_i irreducible in $\mathbb{Z}[i]$. We can assume that no u_i is an associate of any z_j, since otherwise we could cancel that common factor from both sides, and would have an element of smaller norm with distinct irreducible factorizations. Now u_1 divides w, so must divide the product $z_1 \cdot z_2 \cdots z_\ell$. We can conclude, by properties established for irreducible elements in $\mathbb{Z}[i]$, that u_1 divides

a term in this product, say z_i. But now with z_i irreducible and u_1 not a unit, we must conclude that u_1 and z_i are associates, contrary to assumption. So it is impossible for w to have these distinct irreducible factorizations.

(11) (a) $850 = 2 \cdot 5^2 \cdot 17 = (1+i)(1-i)(2+i)^2(2-i)^2(4+i)(4-i)$.
(b) $4125 = 3 \cdot 5^3 \cdot 11 = 3 \cdot 11 \cdot (2+i)^3(2-i)^3$. (Here 3 and 11 are prime numbers congruent to 3 modulo 4, so are irreducible in $\mathbb{Z}[i]$.)
(c) Here $N(37-12i) = 1513 = 17 \cdot 89$, and so $v\overline{v} = (4+i)(4-i)(8+5i)(8-5i)$. These irreducible Gaussian integers are the only possible irreducible factors of $v = 37-12i$. By trial-and-error, we find that $37-12i = (4+i)(8-5i)$.
(d) Here $N(-11+27i) = 850$, so $v\overline{v}$ is made up of the same irreducible factors as in part (a). By trial-and-error, we find that $-11+27i = (1+i)(2+i)^2(4+i)$.

Section 1.3 Ideal Form for Gaussian Integers.

(1) Let $v = g(q+ri)$ have ideal form $g[a:k]$, so that $\gcd(q,r) = 1$ with $a = q^2+r^2$ and $rk \equiv q \pmod{a}$. In this case, $\overline{v} = g(q-ri)$, and since $a = q^2+(-r)^2$ and $(-r)(-k) \equiv q \pmod{a}$, it follows that an ideal form for $\overline{v}$ is $g[a:-k]$.

(2) (a) If $w = 11+3i$, then $N(w) = 11^2+3^2 = 130$ and $3x \equiv 11 \pmod{130}$ has solution $k = 47$. So $[130:47]$ is an ideal form for w.
(b) $w = 9-7i$ has ideal form $[130:-57]$. (To verify this, note that $9^2+(-7)^2 = 130$ and $-7(-57) \equiv 9 \pmod{130}$.)
(c) $w = 13+5i$ has ideal form $[194:-75]$.
(d) $w = -11+27i$ has ideal form $[850:157]$.
(e) $w = 14+16i = 2(7+8i)$ has ideal form $2[113:15]$
(f) $w = 141+3i = 3(47+i)$ has ideal form $3[2210:47]$.

(3) Let $v = g(q+ri)$ have ideal form $g[a:k]$, so that $\gcd(q,r) = 1$ with $a = q^2+r^2$ and $rk \equiv q \pmod{a}$. Then $i \cdot v = g(-r+qi)$. Here $(-r)^2+q^2 = a$, and we have that $qk \equiv -r \pmod{a}$ by Proposition 1.3.1. So $g[a:k]$ is also an ideal form for $i \cdot v$.

(4) An ideal form for $v = 1+i$ is $[2:1]$. So by Theorem 1.3.2, if w is a Gaussian integer with ideal form $h[b:\ell]$, then v divides w if and only if 2 divides bh and $h\ell \equiv h \pmod{2}$. Both requirements are met if h is even. If h is odd but b is even, then ℓ must be odd (so that b can divide ℓ^2+1 as in Proposition 1.3.1), and so both requirements are met in that case also. But if b and h are both odd, then 2 does not divide bh.

(5) Let $g[a:k]$ be an ideal form for a Gaussian integer v, so that $v = g(q+ri)$ with $a = q^2+r^2$ and $rk \equiv q \pmod{a}$. Likewise, let $h[b:\ell]$ be an ideal form for $w = h(s+ti)$, so that $b = s^2+t^2$ and $t\ell \equiv s \pmod{b}$. If v divides w, then g divides h by Lemma 1.3.3, and then $\frac{v}{g} = q+ri$ and $\frac{w}{g} = \frac{h}{g}(s+ti)$ are Gaussian integers having ideal form $[a:k]$ and $\frac{h}{g}[b:\ell]$ respectively. It is clear that $w = vu$ if and only if $\frac{w}{g} = \frac{v}{g}u$. If g divides h, then $bh = agq$ if and only if $b \cdot \frac{h}{g} = aq$. Similarly $h(\ell-k) = agr$ if and only if $\frac{h}{g}(\ell-k) = ar$. The claims of this exercise follow from these equations.

(6) In each part, we write v and w in ideal form and apply the criterion for divisibility in Theorem 1.3.2.
(a) $[13:-5]$ divides $[130:47]$ since 13 divides 130 and $47 \equiv -5 \pmod{13}$.
(b) $[13:5]$ does not divide $[130:47]$ since $47 \not\equiv 5 \pmod{13}$.
(c) $[13:-5]$ divides $[130:-57]$ since 13 divides 130 and $-57 \equiv -5 \pmod{13}$.
(d) $[13:5]$ does not divide $[130:-57]$ since $-57 \not\equiv 5 \pmod{13}$.
(e) $[13:-5]$ does not divide $[194:-75]$ since 13 does not divide 194.
(f) $[17:4]$ divides $[850:157]$ since 17 divides 850 and $157 \equiv 4 \pmod{17}$.
(g) $[17:-4]$ does not divide $[850:157]$ since $157 \not\equiv -4 \pmod{17}$.

(h) $[25:7]$ divides $[850:157]$ since 25 divides 850 and $157 \equiv 7 \pmod{25}$.
(i) $[25:-7]$ does not divide $[850:157]$ since $157 \not\equiv -7 \pmod{25}$.
(j) $[2:1]$ divides $2[113:15]$ since 2 divides $2 \cdot 113$ and $2 \cdot 15 \equiv 2 \cdot 1 \pmod{2}$.
(k) $2[2:1]$ does not divide $2[113:15]$ since $ag = 4$ does not divide $bh = 226$.
(l) $[5:-2]$ does not divide $3[2210:47]$ since $3 \cdot 47 \not\equiv 3(-2) \pmod{5}$.
(m) $[5:2]$ divides $3[2210:47]$ since 5 divides $3 \cdot 2210$ and $3 \cdot 47 \equiv 3 \cdot 2 \pmod{5}$.
(n) $[13:-5]$ divides $3[2210:47]$ since 13 divides $3 \cdot 2210$ and $3 \cdot 47 \equiv 3(-5) \pmod{13}$.
(o) $[13:5]$ does not divide $3[2210:47]$ since $3 \cdot 47 \not\equiv 3 \cdot 5 \pmod{13}$.
(p) $[17:4]$ does not divide $3[2210:47]$ since $3 \cdot 47 \not\equiv 3 \cdot 4 \pmod{17}$.
(q) $[17:-4]$ divides $3[2210:47]$ since 17 divides $3 \cdot 2210$ and $3 \cdot 47 \equiv 3(-4) \pmod{17}$.

Section 1.4. Factorization and Multiplication with Ideal Forms.

(1) (a) $[130:47] = [2:47][5:47][13:47] = [2:1][5:2][13:-5]$. These are ideal forms for $(1+i)(2+i)(3+2i) = -3+11i = i(11+3i)$, an associate of $11+3i$.
(b) $[130:-57] = [2:1][5:-2][13:-5] = (1+i)(2-i)(3+2i) = 7+9i$, an associate of $9-7i$.
(c) $[194:-75] = [2:1][97:22] = (1+i)(9-4i) = 13+5i$.
(d) $[850:157] = [2:1][5:2]^2[17:4] = (1+i)((2+i)^2(4+i) = -11+27i$.
(e) $2[170:47] = [2:1]^3[5:2][17:-4] = (1+i)^3(2+i)(4-i) = -22+14i$, an associate of $14+22i$.
(f) $v = 141+3i = 3[2210:47] = 3[2:1][5:2][13:-5][17:-4]$. These are ideal forms for $3(1+i)(2+i)(3+2i)(4-i) = (-3+141i)$, an associate of $141+3i$. (Here $3 = 3[1:0]$ is irreducible in $\mathbb{Z}[i]$.)
(2) (a) $[25:7][65:-8] = [5:2]^3[13:5] = [125:57][13:5] = [1625:57]$. (Here 57 is the unique solution of $x^2+1 \equiv 0 \pmod{125}$ congruent to 2 modulo 5, and 57 also satisfies $x \equiv 5 \pmod{13}$.) We calculate $(3+4i)(1+8i) = -29+28i$, and verify that $(-29)^2+28^2 = 1625$, with $28 \cdot 57 \equiv -29 \pmod{1625}$.
(b) $[25:7][65:8] = [5:2]^2[5:-2][13:-5] = 5[5:2][13:-5] = 5[65:-18]$. We verify that $(3+4i)(8+i) = 20+35i = 5(4+7i)$ with $4^2+7^2 = 65$ and $7 \cdot -18 \equiv 4 \pmod{65}$.
(c) $[13:-5][65:-8] = [13:-5][13:5][5:2] = 13[5:2]$. Here $(3+2i)(1+8i) = -13+26i = 13(-1+2i)$, with $[5:2]$ an ideal form for $-1+2i$.
(d) $[13:-5][65:8] = [13:-5]^2[5:-2] = [169:-70][5:-2] = [845:268]$. We verify that $(3+2i)(8+i) = 22+19i$, with $22^2+19^2 = 845$ and $19 \cdot 268 \equiv 22 \pmod{845}$.
(e) $[29:12][41:-9] = [1189:360]$, and $(2+5i)(5+4i) = -10+33i$ with $(-10)^2+33^2 = 1189$ and $33 \cdot 360 \equiv -10 \pmod{1189}$.
(f) $[29:12][58:-17] = [29:12]^2[2:1] = [1682:41]$, and $(2+5i)(7+3i) = -1+41i$ with $(-1)^2+41^2 = 1682$ and $41 \cdot 41 \equiv -1 \pmod{1682}$.
(g) $[29:12][58:17] = [29:12][29:-12][2:1] = 29[2:1]$, and $(2+5i)(3+7i) = -29+29i = 29(-1+i)$ with $[2:1]$ an ideal form for $-1+i$.
(h) $[65:18][65:-8] = [5:-2][5:2][13:5]^2 = 5[169:70]$, while $(7+4i)(1+8i) = -25+60i = 5(-5+12i)$ with $[169:70]$ an ideal form for $-5+12i$.
(i) $[65:18][65:8] = [5:-2]^2[13:5][13:-5] = 13[25:-7]$, while $(7+4i)(8+i) = 52+39i = 13(4+3i)$ with $[25:-7]$ an ideal form for $4+3i$.
(j) $[65:18][85:13] = [5:-2]^2[13:5][17:-4] = [25:-7][221:-21] = [5525:1968]$. We verify that $(7+4i)(6+7i) = 14+73i$ with $14^2+73^2 = 5525$ and $73 \cdot 1968 \equiv 14 \pmod{5525}$.

Section 1.5. Reduction of Ideal Forms for Gaussian Integers.

(1) Note that $43^2+1 = 1850 = 370\cdot 5$. Now $[5:-43] = [5:2]$ is an ideal form for $w = 2+i$. Thus $[370:43]$ is an ideal form for $\frac{1}{5}(43+i)(2+i) = \frac{1}{5}(85+45i) = 17+9i$.

(2) In each part, we write $[a:k] \to [c:-k]$, with $-k$ replaced by its minimal value modulo c, to summarize the data of the reduction algorithm.
   (a) $[97:22] \to [5:-2] \to [1:0]$ (that is, $22^2+1 = 97\cdot 5$ and $-22 \equiv -2 \pmod 5$, and then $(-2)^2+1 = 5\cdot 1$ with $2 \equiv 0 \pmod 1$). So $[97:22]$ is an ideal form for $v = \frac{1}{5}(22+i)\cdot\frac{1}{1}(-2+i) = -9+4i$.
   (b) $[145:17] \to [2:1] \to [1:0]$, so $v = \frac{1}{2}(17+i)\cdot\frac{1}{1}(1+i) = 8+9i$.
   (c) $[205:32] \to [5:-2] \to [1:0]$, so $v = \frac{1}{5}(32+i)\cdot\frac{1}{1}(-2+i) = -13+6i$.
   (d) $[205:73] \to [26:5] \to [1:0]$, and $v = \frac{1}{26}(73+i)\cdot\frac{1}{1}(5+i) = 14+3i$.
   (e) $[377:70] \to [13:-5] \to [2:1] \to [1:0]$; $v = \frac{1}{13}(70+i)\cdot\frac{1}{2}(-5+i)\cdot\frac{1}{1}(1+i) = -16-11i$.
   (f) $[377:99] \to [26:5] \to [1:0]$; $v = \frac{1}{26}(99+i)\cdot\frac{1}{1}(5+i) = 19+4i$.
   (g) $[425:132] \to [41:-9] \to [2:1] \to [1:0]$; $v = \frac{1}{41}(132+i)\cdot\frac{1}{2}(-9+i)\cdot\frac{1}{1}(1+i) = -16-13i$.
   (h) $[425:157] \to [58:17] \to [5:-2] \to [1:0]$; $v = \frac{1}{58}(157+i)\cdot\frac{1}{5}(17+i)\cdot\frac{1}{1}((-2+i) = -19+8i$.
   (i) $[493:157] \to [50:-7] \to [1:0]$; $v = \frac{1}{50}(157+i)\cdot\frac{1}{1}(-7+i) = -22+3i$.
   (j) $[493:191] \to [74:31] \to [13:-5] \to [2:1] \to [1:0]$; $v = \frac{1}{74}(191+i)\cdot\frac{1}{13}(31+i)\cdot\frac{1}{2}(-5+i)\cdot\frac{1}{1}(1+i) = -18-13i$.

(3) The congruence $x^2+1 \equiv 0 \pmod{290}$ has four solutions: $x = \pm 17$, $x = \pm 133$. Here $[290:17] \to [1:0]$, so that $v = 17+i$. On the other hand, $[290:133]$ leads to $v = -13-11i$. The other solutions produce conjugates of these.

(4) The ideal forms of Gaussian integers having norm 1625 are $[1625:\pm 57]$, $[1625:\pm 307]$, $5[65:\pm 8]$, and $5[65:18]$. These forms correspond to $28+29i$, $-37-16i$, $40+5i$, $35+20i$ respectively, and their conjugates.

Section 1.6. Sums of Two Squares Revisited.

(1) Since $353^2+1 = 733\cdot 170$ with $-353 \equiv -13 \pmod{170}$, and $(-13)^2+1 = 170$, we find that $[733:353]$ is an ideal form for $\frac{1}{170}(353+i)(-13+i) = -27+2i$, and conclude that $733 = 27^2+2^2$.

(2) From $133^2+1 = 1769\cdot 10$, we find that $\frac{1}{10}(133+i)(-3+i) = -40+13i$ is a Gaussian integer with ideal form $[1769:133]$. Similar calculations show that $[1769:621]$ is an ideal form for $\frac{1}{218}(621+i)\cdot\frac{1}{5}(33+i)(2+i) = 37+20i$. Thus $1769 = 40^2+13^2 = 37^2+20^2$.

(3) We find eight proper representations of $a = 10414625$ by x^2+y^2 from the following calculations.
   (a) $(2+i)^3\cdot(3+2i)^2\cdot(4+i)\cdot(5+2i) = -3223-164i$.
   (b) $(2+i)^3\cdot(3+2i)^2\cdot(4+i)\cdot(5-2i) = -2447+2104i$.
   (c) $(2+i)^3\cdot(3+2i)^2\cdot(4-i)\cdot(5+2i) = -2921+1372i$.
   (d) $(2+i)^3\cdot(3+2i)^2\cdot(4-i)\cdot(5-2i) = -1169+3008i$.
   (e) $(2+i)^3\cdot(3-2i)^2\cdot(4+i)\cdot(5+2i) = 2153+2404i$.
   (f) $(2+i)^3\cdot(3-2i)^2\cdot(4+i)\cdot(5-2i) = 3217+256i$.
   (g) $(2+i)^3\cdot(3-2i)^2\cdot(4-i)\cdot(5+2i) = 3031+1108i$.
   (h) $(2+i)^3\cdot(3-2i)^2\cdot(4-i)\cdot(5-2i) = 2959-1288i$.

(4) (a) $305 = 5\cdot 61 = 17^2+4^2 = 16^2+7^2$. (These arise from $v = (2+i)(6-5i)$ and $v = (2+i)(6+5i)$ respectively, for which $v\overline{v} = 5\cdot 61$.)
   (b) $493 = 17\cdot 29 = 22^2+3^2 = 18^2+13^2$.
   (c) $754 = 2\cdot 13\cdot 29 = 27^2+5^2 = 23^2+15^2$.
   (d) $1885 = 5\cdot 13\cdot 29 = 43^2+6^2 = 42^2+11^2 = 38^2+21^2 = 34^2+27^2$.

(e) $1898 = 2 \cdot 13 \cdot 73 = 43^2 + 7^2 = 37^2 + 23^2$.
(f) $7565 = 5 \cdot 17 \cdot 89 = 86^2 + 13^2 = 83^2 + 26^2 = 82^2 + 29^2 = 62^2 + 61^2$.
(g) $15170 = 2 \cdot 5 \cdot 37 \cdot 41 = 121^2 + 23^2 = 113^2 + 49^2 = 107^2 + 61^2 = 91^2 + 83^2$.

(5) (a) $a = 3250 = 2 \cdot 5^3 \cdot 13 = 57^2 + 1^2 = 55^2 + 15^2 = 53^2 + 21^2 = 45^2 + 35^2$. (Here we use the following products of Gaussian integers respectively: $(1+i)(2-i)^3(3+2i)$, $(1+i)(2+i)^2(2-i)(3+2i)$, $(1+i)(2+i)^3(3+2i)$, and $(1+i)(2+i)(2-i)^2(3+2i)$.) With $m = (3+1)(1+1) = 8$, we expect four representations of a by x^2+y^2 in total, with $2^{2-1} = 2$ of them proper, since a has two distinct prime divisors $p \equiv 1 \pmod 4$.
(b) $a = 3825 = 3^2 \cdot 5^2 \cdot 17 = 60^2 + 15^2 = 57^2 + 24^2 = 48^2 + 39^2$. Here $m = (2+1)(1+1) = 6$, so there are three representations of a by $x^2 + y^2$. None of them are proper, since a is divisible by a prime $p \equiv 3 \pmod 4$.
(c) $a = 12025 = 5^2 \cdot 13 \cdot 37 = 109^2 + 12^2 = 108^2 + 19^2 = 107^2 + 24^2 = 100^2 + 45^2 = 96^2 + 53^2 = 80^2 + 75^2$, with six total representations, four of them proper.
(d) $a = 357773 = 13^2 \cdot 29 \cdot 73 = 598^2 + 13^2 = 563^2 + 202^2 = 557^2 + 218^2 = 547^2 + 242^2 = 542^2 + 253^2 = 442^2 + 403^2$, with six total representations, four of them proper.
(e) $a = 359125 = 5^3 \cdot 13^2 \cdot 17$. There are $2^{3-1} = 4$ proper representations of a by $x^2 + y^2$: $a = 599^2 + 18^2 = 567^2 + 194^2 = 537^2 + 266^2 = 438^2 + 409^2$. There are twelve representations in total. The improper representations are $a = 598^2 + 39^2 = 590^2 + 105^2 = 585^2 + 130^2 = 570^2 + 185^2 = 546^2 + 247^2 = 535^2 + 270^2 = 490^2 + 345^2 = 455^2 + 390^2$.
(f) $a = 585000 = 2^3 \cdot 3^2 \cdot 5^4 \cdot 13$ has five representations by $x^2 + y^2$, none of them proper: $762^2 + 66^2 = 750^2 + 150^2 = 690^2 + 330^2 = 678^2 + 354^2 = 570^2 + 510^2$.
(g) $a = 903125 = 5^5 \cdot 17^2$ has nine representations by $x^2 + y^2$, with two of them proper: $950^2 + 25^2 = 935^2 + 170^2 = 919^2 + 242^2 = 905^2 + 290^2 = 898^2 + 311^2 = 850^2 + 425^2 = 775^2 + 550^2 = 745^2 + 590^2 = 697^2 + 646^2$.

(6) For $a = 10414625 = 5^3 \cdot 13^2 \cdot 17 \cdot 29$, we have $m = (3+1)(2+1)(1+1)(1+1) = 48$, and so 24 representations by $x^2 + y^2$ in total. In addition to the eight proper representations listed in Exercise 3, we have the following improper representations: $3224^2 + 143^2 = 3220^2 + 215^2 = 3215^2 + 280^2 = 3185^2 + 520^2 = 3160^2 + 655^2 = 3140^2 + 745^2 = 3068^2 + 1001^2 = 3055^2 + 1040^2 = 2912^2 + 1391^2 = 2860^2 + 1495^2 = 2740^2 + 1705^2 = 2705^2 + 1760^2 = 2665^2 + 1820^2 = 2480^2 + 2065^2 = 2420^2 + 2135^2 = 2327^2 + 2236^2$.

Section 2.1. Quadratic Numbers and Quadratic Integers.

(1) Let $v = q + r\sqrt{d}$ and $w = s + t\sqrt{d}$ be elements of a quadratic field $\mathbb{Q}(\sqrt{d})$.
(a) $\overline{v+w} = \overline{(q+s) + (r+t)\sqrt{d}} = (q+s) - (r+t)\sqrt{d} = (q - r\sqrt{d}) + (s - t\sqrt{d}) = \overline{v} + \overline{w}$.
(b) $\overline{vw} = \overline{(qs + rtd) + (qt + rs)\sqrt{d}} = (qs+rtd) - (qt+rs)\sqrt{d} = (q - r\sqrt{d})(s - t\sqrt{d}) = \overline{v} \cdot \overline{w}$.
(c) Using (b), $N(vw) = vw \cdot \overline{vw} = (v \cdot \overline{v})(w \cdot \overline{w}) = N(v) \cdot N(w)$.
(d) If d is negative, then $N(v) = (q + r\sqrt{d})(q - r\sqrt{d}) = q^2 - dr^2$ is a sum of two nonnegative real numbers, so can equal zero only when $q^2 = 0$ and $r^2 = 0$. In that case, $v = q + r\sqrt{d} = 0$. If $d > 1$, write $q = \frac{m}{k}$ and $r = \frac{n}{k}$ with m, n, and k integers. Then $N(v) = 0$ implies that $m^2 = dn^2$. Since $d > 1$, then d has some prime divisor d. If $n \neq 0$, then the exponent of p in dn^2 is $e_p(dn^2) = e_p(d) + e_p(n^2) = 2e_p(n) + 1$, since d is squarefree. This cannot equal $e_p(m^2) = 2e_p(m)$. So we must conclude that n and m equal 0.

(2) Let $\mathbb{Q}(\sqrt{d}) = \{q + r\sqrt{d} \mid q, r \in \mathbb{Q}\}$, where $d \neq 1$ is squarefree. Let $v = q + r\sqrt{d}$ and $w = s + t\sqrt{d}$ be elements of $\mathbb{Q}(\sqrt{d})$.

(a) $v+w=(q+s)+(r+t)\sqrt{d}$ and $v-w=(q-s)+(r-t)\sqrt{d}$ are elements of $\mathbb{Q}(\sqrt{d})$, since the sum and difference of rational numbers is rational. Also $0=0+0\sqrt{d}$ is an element of $\mathbb{Q}(\sqrt{d})$.

(b) $vw=(qs+rtd)+(qt+rs)\sqrt{d}$ is an element of $\mathbb{Q}(\sqrt{d})$ since $\mathbb{Q}$ is closed under multiplication and addition. Also $1=1+0\sqrt{d}$ is in $\mathbb{Q}(\sqrt{d})$.

(c) If $v\neq 0$, then $\frac{\overline{v}}{N(v)}=\frac{q}{q^2-dr^2}-\frac{r}{q^2-dr^2}\sqrt{d}$ is an element of $\mathbb{Q}(\sqrt{d})$ since q^2-dr^2 is a nonzero rational number by part (d) of Exercise 1. Here $v\cdot\frac{\overline{v}}{N(v)}=1$ since $v\cdot\overline{v}=N(v)$. Thus v has an inverse under multiplication when $v\neq 0$.

(3) (a) If $v=\frac{1}{3}-\frac{7}{5}\sqrt{3}=\frac{5-21\sqrt{3}}{15}$, then $\overline{v}=\frac{5+21\sqrt{3}}{15}$. We calculate that $v+\overline{v}=\frac{2}{5}$ and $v\cdot\overline{v}=\frac{25-3\cdot 441}{225}=-\frac{1298}{225}$. Thus v is a root of $x^2-\frac{2}{5}x-\frac{1298}{225}$, and has minimum polynomial $f(x)=225x^2-150x-1298$. The discriminant of v is $\Delta(v)=(-150)^2-4\cdot 225\cdot -1298=1190700=3\cdot 630^2$.

(b) $v=\frac{3+5\sqrt{-19}}{2}$ has minimum polynomial $f(x)=x^2-3x+121$ and discriminant $\Delta(v)=-475=-19\cdot 5^2$.

(c) $v=\frac{2}{7}+\frac{1}{3}\sqrt{-29}=\frac{6+7\sqrt{-29}}{21}$ has minimum polynomial $f(x)=441x^2-252x+1457$ and discriminant $\Delta(v)=-2506644=-29\cdot 294^2$.

(d) $v=\frac{1}{5}-\frac{2}{3}\sqrt{41}=\frac{3-10\sqrt{41}}{15}$ has minimum polynomial $f(x)=225x^2-90x-4091$ and discriminant $\Delta(v)=3690000=41\cdot 300^2$.

Section 2.2. Domains of Quadratic Integers.

(1) (a) $\Delta(-7,1)=-7$ since $-7\equiv 1 \pmod 4$; $z=\frac{1+\sqrt{-7}}{2}$; $N(q+rz)=q^2+qr+2r^2$; $\phi(x)=x^2+x+2$.

(b) $\Delta(-7,2)=-28$; $z=1+\sqrt{-7}$; $N(q+rz)=q^2+2qr+8r^2$; $\phi(x)=x^2+2x+8$.

(c) $\Delta(7,1)=28$ since $7\equiv 3 \pmod 4$; $z=\sqrt{7}$; $N(q+rz)=q^2-7r^2$; $\phi(x)=x^2-7$.

(d) $\Delta(17,1)=17$ since $17\equiv 1 \pmod 4$; $z=\frac{1+\sqrt{17}}{2}$; $N(q+rz)=q^2+qr-4r^2$; $\phi(x)=x^2+x-4$.

(2) (a) $\Delta=45=3^2\cdot 5=\Delta(5,3)$ since $5\equiv 1 \pmod 4$; $z=\frac{3+\sqrt{45}}{2}$; $N(q+rz)=q^2+3qr-9r^2$; $\phi(x)=x^2+3x-9$.

(b) $\Delta=-63=3^2\cdot -7=\Delta(-7,3)$; $z-\frac{3+\sqrt{-63}}{2}$; $N(q+rz)=q^2+3qr+18qr$; $\phi(x)=x^2+3x+18$.

(c) $\Delta=-84=2^2\cdot -21=\Delta(-21,1)$ since $-21\equiv 3 \pmod 4$; $z=\sqrt{-21}$; $N(q+rz)=q^2+21r^2$; $\phi(x)=x^2+21$.

(d) $\Delta=84=2^2\cdot 21=\Delta(21,2)$ since $21\equiv 1 \pmod 4$; $z=\frac{2+\sqrt{84}}{2}=1+\sqrt{21}$; $N(q+rz)=q^2+2qr-20r^2$; $\phi(x)=x^2+2x-20$.

(e) $\Delta=-88=2^2\cdot -22=\Delta(-22,1)$; $z=\sqrt{-22}$; $N(q+rz)=q^2+22r^2$; $\phi(x)=x^2+22$.

(f) $\Delta=88=2^2\cdot 22=\Delta(22,1)$; $z=\sqrt{22}$; $N(q+rz)=q^2-22r^2$; $\phi(x)=x^2-22$.

(g) $\Delta=-99=3^2\cdot -11=\Delta(-11,3)$; $z=\frac{3+\sqrt{-99}}{2}$; $N(q,r)=q^2+3qr+27r^2$; $\phi(x)=x^2+3x+27$.

(h) $\Delta=297=3^2\cdot 33=\Delta(33,3)$; $z=\frac{3+\sqrt{297}}{2}$; $N(q,r)=q^2+3qr-72r^2$; $\phi(x)=x^2+3x-72$.

(i) $\Delta=300=10^2\cdot 3=5^2\cdot 12=\Delta(3,5)$ since $3\equiv 3 \pmod 4$; $z=\frac{\sqrt{300}}{2}=\sqrt{75}$; $N(q,r)=q^2-75r^2$; $\phi(x)=x^2-75$.

(j) $\Delta=-300=10^2\cdot -3=\Delta(-3,10)$ since $-3\equiv 1 \pmod 4$; $z=\frac{10+\sqrt{-300}}{2}=5+\sqrt{-75}$; $N(q,r)=q^2+10qr+100r^2$; $\phi(x)=x^2+10x+100$.

(3) Let $v=q+rz$ and $w=s+tz$ be elements of a quadratic domain D_Δ.

(a) $\overline{v+w} = (q+s)+(r+t)\overline{z} = (q+r\overline{z})+(s+t\overline{z}) = \overline{v}+\overline{w}$.
(b) $\overline{v\cdot w} = \left(qs - \frac{\varepsilon^2-\Delta}{4}\cdot rt\right) + (qt+rs+\varepsilon rt)\overline{z} = (q+r\overline{z})\cdot(s+t\overline{z}) = \overline{v}\cdot\overline{w}$. (Here we use the fact that z and $\overline{z}$ are both roots of $x^2-\varepsilon x+\frac{\varepsilon^2-\Delta}{4}$.)
(c) $N(v\cdot w) = vw\cdot\overline{vw} = v\overline{v}\cdot w\overline{w} = N(v)\cdot N(w)$.

(4) $\phi(-k-\varepsilon) = (-k-\varepsilon)^2+\varepsilon(-k-\varepsilon)+\frac{\varepsilon^2-\Delta}{4} = k^2+2\varepsilon k+\varepsilon^2-\varepsilon k-\varepsilon^2+\frac{\varepsilon^2-\Delta}{4} = k^2+\varepsilon k+\frac{\varepsilon^2-\Delta}{4}$, which equals $\phi(k)$.

(5) We know that $\Delta(v) = (v-\overline{v})^2$ by Proposition 2.1.6, so then

$$(v+\overline{v})^2 - \Delta(v) = (v^2+2v\overline{v}+\overline{v}^2) - (v^2-2v\overline{v}+\overline{v}^2) = 4v\overline{v} = 4N(v).$$

(6) If $q+rz$ and $s+tz$ are elements of a quadratic domain $D = \{a+bz \mid a,b\in\mathbb{Z}\}$, then so is their sum, $(q+s)+(r+t)z$. Likewise $1 = 1+0z$ is in D, as is $-(q+rz) = (-q)+(-r)z$.

(7) If $\phi(x) = x^2+\varepsilon x+\frac{\varepsilon^2-\Delta}{4}$ is the principal polynomial of discriminant $\Delta = \Delta(d,1)$, then the principal polynomial of discriminant $\Delta_\gamma = \Delta(d,\gamma) = \gamma^2\Delta$ is $\phi_\gamma(x) = x^2+\varepsilon_\gamma x+\frac{\varepsilon_\gamma^2-\Delta_\gamma}{4} = x^2+\gamma\varepsilon x+\gamma^2\cdot\frac{\varepsilon^2-\Delta}{4}$, here using the fact that $\varepsilon_\gamma = \gamma\varepsilon$. So then

$$\phi_\gamma(\gamma x) = \gamma^2\left(x^2+\varepsilon x+\frac{\varepsilon^2-\Delta}{4}\right) = \gamma^2\phi(x).$$

With $\phi'(x) = 2x+\varepsilon$ and $\phi'_\gamma(x) = 2x+\varepsilon_\gamma = 2x+\gamma\varepsilon$, then $\phi'_\gamma(\gamma x) = \gamma(2x+\varepsilon) = \gamma\phi'(x)$ is also true.

(8) Let $v = q+rz_\gamma$ be an element of $D_\gamma = D_{\gamma^2\Delta}$. Since $z_{\gamma^\Delta} = \gamma z_\Delta$, we can also write $v = q+\gamma rz$ in $D = D_\Delta$. Now in D_γ, we have $N(v) = q^2+\varepsilon_\gamma qr+\frac{\varepsilon_\gamma^2-\gamma^2\Delta}{4}\cdot r^2$, while in D we find that $N(v) = q^2+\varepsilon(\gamma r)+\frac{\varepsilon^2-\Delta}{4}(\gamma r)^2$. But these are equal since $\varepsilon_\gamma = \gamma\varepsilon$.

(9) (a) If $w = vu$ for some u in D, then $N(w) = N(vu) = N(v)\cdot N(u)$. Since $N(u)$ is a rational integer, then $N(v)$ divides $N(w)$ in $\mathbb{Z}$.
(b) If u divides 1, so that $1 = uv$ for some v in D, then $N(1) = 1 = N(u)\cdot N(v)$. So $N(u)$ is a rational integer that divides 1 in $\mathbb{Z}$, and so $N(u) = \pm 1$. Conversely, if $N(u) = u\overline{u} = \pm 1$, then $\pm\overline{u}$ is an inverse of u in D, and so u is a unit in D.
(c) If u is a unit in D, then $N(\pm u^n) = N(\pm 1)\cdot N(u)^n = 1\cdot(\pm 1)^n = \pm 1$, and so $\pm u^n$ is also a unit in D by part (b).
(d) Let v and w be associates in D. First note that $v = 0$ if and only if $w = 0$, and in that case, $N(v) = N(w)$. So assume that $v\neq 0$. Now if v divides w and w divides v, then $w = vu_1$ and $v = wu_2$ for some u_1 and u_2 in D. Thus $v = vu_1u_2$, and so $u_1u_2 = 1$. But then u_1 and u_2 are units. Using part (b), then $N(w) = N(v)\cdot N(u_1) = \pm N(v)$.

(10) By direct calculation, if $z = \frac{1+\sqrt{-3}}{2}$, then $z^2 = \frac{-1+\sqrt{-3}}{2} = -1+z$, so that $z^3 = -1$, and then $z^4 = -z$, $z^5 = -(-1+z) = 1-z$, and $z^6 = -(-1) = 1$.

Section 2.3. Ideal Form for Quadratic Integers.

(1) Suppose that $v = g(q+rz)$ has ideal form $g[a:k]$, so that $N(g+rz) = a$ and $rk\equiv q \pmod a$. Since $N(w) = w\overline{w} = N(\overline{w})$ for each element w in a quadratic domain D, then $\overline{v} = g(q+r\overline{z})$ has ideal form $g[a:\ell]$ for some ℓ. Since $q+r\overline{z} = q+r(\varepsilon-z) = (q+r\varepsilon)-rz$, we find that $rk\equiv q \pmod a$ implies that $-r(-k-\varepsilon)\equiv q+r\varepsilon \pmod a$, and so we can take ℓ to equal $-k-\varepsilon$.

(2) (a) In D_{-8}, $N(q+rz) = q^2+2r^2$. If $v = 3+5z$, then $N(v) = 59$ and $5x\equiv 3 \pmod{59}$ has $k = -23$ as a solution. So $[59:-23]$ is an ideal form for v.
(b) $N(3+5z) = 3^2+3\cdot 5+5^2 = 49$ in D_{-3}, and $5(-19)\equiv 3 \pmod{49}$: $v = [49:-19]$.
(c) $N(3+5z) = 3^2-2\cdot 5^2 = -41$ in D_8, and $5(17)\equiv 3 \pmod{41}$: $v = [-41:17]$.
(d) $N(3+5z) = 3^2-3\cdot 5^2 = -66$ in D_{12}, and $5(27)\equiv 3 \pmod{66}$: $v = [-66:27]$.

(e) $N(5+2z) = 5^2 + 2 \cdot 2^2 = 33$ in D_{-8}, and $2(-14) \equiv 5 \pmod{33}$: $v = [33 : -14]$.
(f) $N(7+3z) = 7^2 - 3 \cdot 3^2 = 22$ in D_{12}, and $3(-5) \equiv 7 \pmod{22}$: $v = [22 : -5]$.
(g) $N(5-z) = 5^2 + 5(-1)^2 = 30$ in D_{-20}, and $-1(-5) \equiv 5 \pmod{30}$: $v = [30 : -5]$.
(h) $v = 15 + 6z = 3(5+2z)$, with $N(5+2z) = 5^2 + 5 \cdot 2 + 6 \cdot 2^2 = 59$ in D_{-23}. Since $2(-27) \equiv 5 \pmod{59}$, then $v = 3[59 : -27]$.
(i) $v = 14 - 6z = 2(7-3z)$, with $N(7-3z) = 7^2 + 6(-3)^2 = 103$ in D_{-24}. Here we have $-3(32) \equiv 7 \pmod{103}$, and so $v = 2[103 : 32]$.
(j) $v = 27 - 12z = 3(9-4z)$, with $N(9-4z) = 9^2 - 6(-4)^2 = -15$ in D_{24}. Here $-4(-6) \equiv 9 \pmod{15}$, so $v = 3[-15 : -6]$.

(3) Let $w = h(m+nz)$, with $\gcd(m,n) = 1$, so that $ms + nt = 1$ for some integers s and t. If $v = g(q+rz)$ divides w, then g divides both hm and hn, and so g divides $(hm)s+(hn)t = h$.

(4) (a) $v = 1 + z = [3 : 1]$ divides $w = 5 + 2z = [33 : -14]$ in D_{-8}, since 3 divides 33 and $-14 \equiv 1 \pmod{3}$.
(b) $v = [3 : 1]$ does not divide $w = 5 - 2z = [33 : 14]$ in D_{-8}, since $14 \not\equiv 1 \pmod{3}$.
(c) $v = 5 + 3z$ can be written as $[-2 : 1]$, since $N(5+3z) = 5^2 - 3 \cdot 3^2 = -2$ with $3 \equiv 1 \pmod{2}$, and $w = 7 + 3z$ as $[22 : -5]$ in D_{12}, from part (f) of Exercise 2. Here v divides w since -2 divides 22 and $-5 \equiv 1 \pmod{2}$.
(d) $v = 1 + z = [6 : 1]$ divides $w = 5 - z = [30 : -5]$ in D_{-20}.
(e) $v = 1 + z = [6 : 1]$ does not divide $w = 5 + z = [30 : 5]$ in D_{-20}.

(5) In D_{-8}, $N(q + rz) = q^2 + 2r^2$. We find that $N(1+2z) = 9$ with $2(-4) \equiv 1 \pmod{9}$, and that $N(1+3z) = 19$ with $3(-6) \equiv 1 \pmod{19}$. Since $\gcd(9, 19) = 1$, we then find that $[9 : -4] \cdot [19 : -6] = [171 : 32]$, since $x = 32$ satisfies $x \equiv -4 \pmod{9}$ and $x \equiv -6 \pmod{19}$. To verify this calculation directly, $(1+2z)(1+3z) = 1 + 5z + 6z^2 = -11 + 5z$ in D_{-8}, where $z^2 = -2$. We find that $N(-11+5z) = (-11)^2 + 2 \cdot 5^2 = 171$, and that $5(32) \equiv -11 \pmod{171}$.

(6) If $\Delta = -8$, then $\phi(x) = x^2 + 2$. We find that $v = 1 + z$ has ideal form $[3 : 1]$, and since $\phi(x) \equiv 0 \pmod{3}$ has two solutions, we can use Proposition 2.3.7 to calculate powers of v in ideal form. Here v^2 and v^3 have ideal form $[9 : 4]$ and $[27 : -5]$ respectively. (For instance, $\phi(-5) = 27$ so that $x = -5$ is the unique solution of $x^2 \equiv 0 \pmod{27}$ that is congruent to 1 modulo 3.) To verify these claims, note that $(1+z)^2 = 1 + 2z + z^2 = -1 + 2z$, and then $(1+z)^3 = (-1+2z)(1+z) = -1+z+2z^2 = -5+z$. Here $N(-1+2z) = (-1)^2+2\cdot 2^2 = 9$, with $2(-4) \equiv -1 \pmod{9}$, and $N(-5+z) = (-5)^2 + 2 \cdot 1^2 = 27$, with $1(-5) \equiv -5 \pmod{27}$.

Section 2.4. Ideal Numbers.

(1) We write $[a : k] \to [c : \ell]$ if $\phi(ak) = ac$ and $\ell \equiv -k - \varepsilon \pmod{c}$.
(a) With $\Delta = -8$, then $\phi(x) = x^2 + 2$. We find that $[121 : 19] \to [3 : -1] \to [1 : 0]$ since $\phi(19) = 121 \cdot 3$ and $\phi(-1) = 3 \cdot 1$. Thus $[121 : 19]$ is an ideal form for $v = \frac{1}{3}(19+z)(-1+z) = -7 + 6z$.
(b) For $\Delta = -11$, $\phi(x) = x^2+x+3$. Here $[111 : 23] \to [5 : 1] \to [1 : 0]$ since $\phi(23) = 111 \cdot 5$ with $-k - \varepsilon = -24 \equiv 1 \pmod{5}$, and $\phi(1) = 5 \cdot 1$. Thus $[111 : 23]$ is an ideal form for $v = \frac{1}{5}(23+z)(1+z) = 4 + 5z$. (Note that $z^2 = -3 + z$ in D_{-11}.)
(c) When $\Delta = -15$, then $\phi(x) = x^2+x+4$. Here since $\phi(-10) = 94$, we have immediately that $v = -10 + z$ is an element of D_{-15} having ideal form $[94 : -10]$.
(d) We find that $[94 : 37] \to [15 : 7] \to [4 : 0] \to [1 : 0]$, and thus

$$v = \frac{1}{15}(37+z) \cdot \frac{1}{4}(7+z) \cdot \frac{1}{1}(0+z) = \frac{1}{15}(37+z)(-1+2z) = -3 + 5z$$

is an element of D_{-15} with ideal form $[94 : 37]$. (Note that $z^2 = -4 + z$ in D_{-15}.)

(e) With $\phi_{-20}(x) = x^2 + 5$, we find that $[123 : 47] \to [18 : 7] \to [3 : -1] \to [2 : 1]$. Here $u_{-20} = 2$, so we know that none of these expressions is an ideal form for an element of D_{-20}.

(f) With $\Delta = -20$, we find that $[129 : 52] \to [21 : -10] \to [5 : 0][1 : 0]$. Thus $[129 : 52]$ is an ideal form for

$$v = \frac{1}{21}(52 + z) \cdot \frac{1}{5}(-10 + z) \cdot \frac{1}{1}(0 + z) = \frac{1}{21}(52 + z)(-1 + 2z) = -2 - 5z.$$

(Here $z^2 = -5$.)

(g) For $\Delta = -23$, we have $\phi(x) = x^2 + x + 6$. Since $\phi(15) = 246$, we immediately have that $[246 : 15]$ is an ideal form for $v = 15 + z$.

(h) Here $[246 : 56] \to [13 : -5] \to [2 : 0]$. With $u_{-23} = 2$, it follows that $[246 : 56]$ is not an ideal form for an element of D_{-23}.

(i) Here $[246 : 66] \to [18 : 5] \to [2 : 0]$, so that $[246 : 66]$ is not an ideal form for an element of D_{-23}.

(j) In this case, $[246 : 107] \to [47 : -14] \to [4 : 1] \to [2 : 0]$, and thus $[246 : 107]$ is not an ideal form for an element of D_{-23}.

Section 2.5. Quadratic Domains with Unique Factorization.

(1) Suppose that w is a prime element of a quadratic domain D, and that $w = uv$ for some elements u and v of D. Then w divides uv, and so either w divides u or w divides v by the definition of prime elements. We can assume that w divides v without loss of generality, say that $v = wx$ for some x in D. But now $w = uv = w(ux)$ and so $ux = 1$ since $w \neq 0$. Thus u is a unit of D, and it follows that w is irreducible in D by definition.

(2) Suppose that D is a quadratic domain in which every irreducible element is prime. If D is not a unique factorization domain, then there is an element w of D that can be written both as $w = u_1 \cdots u_k$ and as $w = v_1 \cdots v_\ell$ with each u_i and v_i irreducible. We can assume that no u_i is an associate of any v_j by assuming that $|N(w)|$ is as small as possible among all elements that can be written with distinct irreducible factorizations. But now u_1 divides w, so that u_1 divides the product $v_1 \cdots v_\ell$. Since u_1 is irreducible, and so prime by assumption, it follows that u_1 divides v_j for some $1 \leq j \leq \ell$. With v_j irreducible and u_1 not a unit, we must conclude that u_1 and v_j are associates, contrary to assumption. Thus these distinct irreducible factorizations cannot exist.

(3) Let D be a quadratic domain. Suppose that w is an irreducible element of D and that w divides uv for some u and v in D, say with $uv = wx$ for some x in D. Assume that w divides neither u nor v. It follows that neither u nor v can be a unit, and so each can be written as a product of irreducible elements of D, say $u = u_1 \cdots u_k$ and $v = v_1 \cdots v_\ell$. No u_i nor v_i can be an associate of w. But now if x is written as a product of irreducible elements, we have two irreducible factorizations of $y = wx = uv$, in which w appears as a factor in one expression (wx), but is not an associate of any irreducible factor in the other expression $(uv = u_1 \cdots u_k \cdot v_1 \cdots v_\ell)$. Thus D cannot be a unique factorization domain if it contains an irreducible element that is not prime.

(4) It is noted in this section that $D = D_{-8}$ is a principal ideal number domain, with $\left(\frac{-8}{p}\right) = -1$ if and only if $p \equiv 5$ or $7 \pmod 8$ and $\left(\frac{-8}{p}\right) = 0$ only for $p = 2$. Since $\phi(x, y) = x^2 + 2y^2$ is the principal form of discriminant $\Delta = -8$, the claim of this exercise is an immediate consequence of Theorem 2.5.3.

(5) In an example in §13, it is established that $D = D_{-3}$ is a principal ideal number domain. Here $\phi(x, y) = x^2 + xy + y^2$ is the principal form of discriminant $\Delta = -3$. In this case,

$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = -1$ if and only if $p \equiv 2 \pmod 3$, and $\left(\frac{-3}{p}\right) = 0$ only when $p = 3$. So the claim of this exercise follows from Theorem 2.5.3.

(6) If $\phi(q,r) = q^2+qr+r^2 = a$, then $\phi(-r, q+r) = (-r)^2 - r(q+r) + (q+r)^2 = q^2+qr+r^2 = a$, and $\phi(-q-r, q) = (-q-r)^2 - (q+r)q + q^2 = q^2 + qr + r^2 = a$.

(7) Let $\phi(x,y) = x^2 + xy + y^2$, and suppose that $\phi(q,r) = a$ with $\gcd(q,r) = 1$. If r is odd and q is even, replace (q,r) by $(-q-r, q)$. If r and q are both odd, replace (q,r) by $(-r, q+r)$. In this way, we can assume that r is even. Now note that $(q + \frac{r}{2})^2 + 3(\frac{r}{2})^2 = q^2 + qr + r^2 = a$. Any prime common divisor of $q + \frac{r}{2}$ and $\frac{r}{2}$ would also divide both q and r, and so $\gcd(q + \frac{r}{2}, \frac{r}{2}) = 1$. Thus every positive integer properly represented by $\phi(x,y)$ is also properly represented by $x^2 + 3y^2$.

Section 2.6. Quadratic Domains without Unique Factorization.

(1) (a) If $\Delta = -24$, then $N(q+rz) = q^2+6r^2$ and $\phi(x) = x^2+6$. We find that $x = 2$ satisfies the congruence $\phi(x) \equiv 0 \pmod 5$, and so $[5:2]$ is an ideal number of discriminant Δ. This ideal number cannot be principal since $q^2 + 6r^2 = 5$ has no integer solutions. Then notice that $\phi(2) = 10 = 2 \cdot 5$, and that $\phi(2) = N(2+z) = (2+z)(2-z)$. The equation $2 \cdot 5 = (2+z)(2-z)$ is an example of distinct irreducible factorizations of the same element. (No two of these elements are associates, and each is irreducible because there are no elements v of D_{-24} with $N(v) = 2$ or $N(v) = 5$.)

(b) If $\Delta = -40$, then $N(q+rz) = q^2 + 10r^2$ and $\phi(x) = x^2 + 10$. Here $[7:2]$ is an ideal number that cannot be principal, and since $\phi(2) = 14 = 2 \cdot 7$, but $\phi(2) = N(2+z) = (2+z)(2-z)$, we find that $14 = 2 \cdot 7 = (2+z)(2-z)$ is an example of distinct irreducible factorizations.

(c) If $\Delta = -52$, then $N(q+rz) = q^2 + 13r^2$ and $\phi(x) = x^2 + 13$. We have that $\phi(1) = 14 = 2 \cdot 7$, and so $[7:1]$ is an ideal number that is not principal. Since $\phi(1) = N(1+z) = (1+z)(1-z)$, we obtain the following distinct irreducible factorizations: $14 = 2 \cdot 7 = (1+z)(1-z)$.

(2) For $\phi(x) = x^2 + 5$, we write $[a:k] \to [c:\ell]$ if $\phi(k) = ac$ and $\ell \equiv -k \pmod c$.

(a) Since $[87:-16] \to [3:1] \to [2:1]$, then $[87:-16]$ is not a principal ideal number. With $87 = 3 \cdot 29$, we can write $[87:-16] = [3:-1] \cdot [29:13]$.

(b) Here $[161:31] \to [6:-1] \to [1:0]$, so that $[161:31]$ is an ideal form for the element $v = \frac{1}{6}(31+z)(-1+z) = -6 + 5z$. Since $161 = 7 \cdot 23$, then $[161:31] = [7:3] \cdot [23:8]$.

(c) $[161:-38] \to [9:2] \to [1:0]$, so that $[161:-38]$ is an ideal form for $v = \frac{1}{9}(-38+z)(2+z) = -9 - 4z$. We can write $[161:-38] = [7:-3] \cdot [23:8]$.

(d) $[203:-74] \to [27:-7] \to [2:1]$ is not an ideal form for an element of D_{-20}. Since $203 = 7 \cdot 29$, we can write $[203:-74] = [7:3] \cdot [29:13]$.

(e) $[270:115] \to [49:-17] \to [6:-1] \to [1:0]$, so that $[270:115]$ is an ideal form for $v = \frac{1}{49}(115+z) \cdot \frac{1}{6}(-17+z)(-1+z) = 5 - 7z$. Here $270 = 2 \cdot 3^3 \cdot 5$, and thus $[270:115] = [2:1] \cdot [3:1]^3 \cdot [5:0]$.

(3) (a) Since $z^2 = -6$, we find that $(3+2z)(2+z) = -6 + 7z = (4-z)(-3+z)$ in D_{-24}. Ideal form expressions for these factors are $3 + 2z = [33:-15]$, $2 + z = [10:2]$, $4 - z = [22:-4]$, and $-3 + z = [15:-3]$. Each factor is irreducible in D_{-24} since there are no elements $v = q + rz$ of that domain for which $N(v) = q^2 + 6r^2 = 2$ or 3. But we have the following ideal number factorizations:

$$[33:-15] \cdot [10:2] = [3:0] \cdot [11:-4] \cdot [2:0] \cdot [5:2],$$

and

$$[22:-4] \cdot [15:-3] = [2:0] \cdot [11:-4] \cdot [3:0] \cdot [5:2].$$

(b) Here with $z^2 = -13$, we have $(5+z)(8+z) = 27+13z = (-3+z)(4-3z)$ in D_{-52}. Ideal form expressions for the factors are $5+z = [38:5] = [2:1]\cdot[19:5]$, $8+z = [77:8] = [7:1]\cdot[11:-3]$, $-3+z = [22:-3] = [2:1]\cdot[11:-3]$, and $4-3z = [133:43] = [7:1]\cdot[19:5]$. Each factor is irreducible in D_{-52} since $q^2+13r^2 = 2$ or 7 has no integer solutions, and we find the same irreducible ideal number factors in both products.

(c) Here $(3+2z)(2-z) = 34+z = (4+z)(5-z)$ in D_{-56}, where $z^2 = -14$. We find that $3+2z = [65:-31] = [5:-1]\cdot[13:-5]$, $2-z = [18:-2] = [2:0]\cdot[3:1]^2$, $4+z = [30:4] = [2:0]\cdot[3:1]\cdot[5:-1]$, and $5-z = [29:-5] = [3:1]\cdot[13:-5]$. The factors are irreducible in D_{-56} since $q^2+14r^2 = 2$, 3, or 5 has no integer solutions.

(d) With $z^2 = -6+z$, we find that $(3+2z)(7+z) = 9+19z = (-5+z)(3-4z)$ in D_{-23}. Here $3+2z = [39:-18] = [3:0]\cdot[13:-5]$, $7+z = [62:7] = [2:1]\cdot[31:7]$, $-5+z = [26:-5] = [2:1]\cdot[13:-5]$, and $3-4z = [93:-24] = [3:0]\cdot[31:7]$. Here $N(q+rz) = q^2+qr+6r^2 = \frac{(2q+r)^2+23r^2}{4} = 2$ or 3 has no integer solutions, so it follows that the factors are irreducible in D_{-23}.

Section 3.1. Ideals and Ideal Numbers.

(1) Let v and w be elements of a quadratic domain D and let $\langle v,w\rangle = \{vx+wy \mid x,y \in D\}$. Using closure properties of D, we see that if $vx+wy$ and $vx'+wy'$ are in $\langle v,w\rangle$, then $(vx+wy)-(vx'+wy') = v(x-x')+w(y-y')$ is in $\langle v,w\rangle$, and if u is an element of D, then $(vx+wy)u = v(xu)+w(yu)$ is in $\langle v,w\rangle$. Thus $\langle v,w\rangle$ is an ideal of D.

(2) Let v be an element and A an ideal of D, and let $vA = \{vx \mid x \in A\}$. Using closure properties of A, we see that if vx and vx' are in vA and y is in D, then $vx-vx' = v(x-x')$ and $(vx)y = v(xy)$ are in vA. If x is in A, then x is also in D, and so vx is in the principal ideal $\langle v\rangle$, and $vA \subseteq \langle v\rangle$. Suppose that $v \neq 0$ and that $vA = vB$ for some ideals A and B of D. If a is an element of A, then va is in $vA = vB$, and so has the form vb for some b in B. But if $v \neq 0$, then $va = vb$ implies that $a = b$, and thus $A \subseteq B$. The reverse inclusion and the converse are similarly established.

(3) Let $A = \{x \in D \mid vx \in B\}$, where v is an element and B an ideal of a quadratic domain D. If x and y are in A, then vx and vy are in B, and so $vx-vy = v(x-y)$ is in B. But then $x-y$ is in A by definition. Likewise, if x is in A and u is in D, then vx is in B and so $(vx)u = v(xu)$ is in B. But then xu is in A by definition. Thus A is an ideal of D. Now suppose that B is a subset of the principal ideal $\langle v\rangle$. If y is in B, then $y = vx$ for some x in D. But then x is in A by definition, and so $y = vx$ is in vA. Thus $B \subseteq vA$. For the reverse inclusion, let x be an element of A. Then by definition vx is in B, and so $vA \subseteq B$.

(4) Let $S = \{v_1,\ldots,v_t\}$ be a finite subset of a quadratic domain D. Let $m_1v_1+\cdots+m_tv_t$ and $n_1v_1+\cdots+n_tv_t$ be $\mathbb{Z}$-combinations of S. Then $(m_1v_1+\cdots+m_tv_t)-(n_1v_1+\cdots+n_tv_t) = (m_1-n_1)v_1+\cdot+(m_t-n_t)v_t$ is also a $\mathbb{Z}$-combination of S. If $S = \{3,1+i\}$ in $\mathbb{Z}[i]$, let A be the set of all $\mathbb{Z}$-combinations of S. Note that $1+i$ is in A and $1-i$ is in $\mathbb{Z}[i]$, but that $(1+i)(1-i) = 2$ is not in A. (If $2 = 3m+(1+i)n = (3m+n)+ni$, then $n = 0$ and m is not a rational integer.)

(5) Let w be an element in the $\mathbb{Z}$-span of $\{a,k+z\}$, that is, let $w = m(a)+n(k+z)$ for some m and n in $\mathbb{Z}$. Then $w = (-m)(-a)+n(k+z)$ is also in the $\mathbb{Z}$-span of $\{-a,k+z\}$. The reverse inclusion is established in the same way. Suppose that $\ell \equiv k \pmod{a}$, say that $\ell-k = aq$ for some q in $\mathbb{Z}$, and that $w = m(a)+n(k+z)$ as above. Then $w = (m-nq)a+n(\ell+z)$, so that w is also in the $\mathbb{Z}$-span of $\{a,\ell+z\}$. Again the reverse inclusion is similar.

(6) Let g be the divisor of an ideal B of a quadratic domain, so that $B = gA$ for the ideal $A = \{x \in D \mid gx \in B\}$ of D. By definition, B contains an element $m+gz$, and the proof

of Proposition 3.1.2 shows that g divides m. But now $\frac{m}{g} + z$ is an element of A, and so the divisor of A must be 1, that is, A is primitive.

(7) Let B be a nontrivial ideal of a quadratic domain D, with divisor g, subnorm a, and character k. By definition, then B contains the elements ga and $g(k+z)$, and so contains every $\mathbb{Z}$-combination of the set $S = \{ga, g(k+z)\}$. The proof of Theorem 3.1.5 shows that every element of B can be written as a $\mathbb{Z}$-combination of S. Suppose that an element v of B can be written both as $v = m(ga) + n(gk+gz) = (mga + ngk) + ngz$ and as $s(ga) + t(gk+gz) = (sga + tgk) + tgz$ for some rational integers m, n, s, and t. Then $ng = tg$ since otherwise we could solve for z as a rational number. With g positive, it follows that $n = t$. Now since $mga + ngk = sga + tgk$ and $a \neq 0$, we see that $m = s$. So expressions for elements of B as $\mathbb{Z}$-combinations of S are unique, and S is a $\mathbb{Z}$-basis for B.

(8) Ideals of norm $75 = 3 \cdot 5^2$ can have divisor 1 or 5. Finding all solutions of $\phi(x) \equiv 0 \pmod 3$ and of $\phi(x) \equiv 0 \pmod{75}$, with $\phi(x) = x^2 - 31$ the principal polynomial of discriminant $\Delta = 124$, we obtain the following six ideal of norm 75: $[75 : 16]$, $[75 : -16]$, $[75 : 34]$, $[75 : -34]$, $5[3 : 1]$, and $5[3 : -1]$.

(9) (a) The principal polynomial of discriminant $\Delta = -7$ is $\phi(x) = x^2 + x + 2$. The congruence $\phi(x) \equiv 0 \pmod 2$ has two solutions, and so $[2 : 0]$ and $[2 : -1]$ are the distinct ideals of norm 2 in D_{-7}.

(b) Here $\phi(x) = x^2 + x + 8$, and with $70 = 2 \cdot 5 \cdot 7$, we find that there are eight distinct solutions of $\phi(x) \equiv 0 \pmod{70}$. The ideals of norm 70 in $D{-}31$ can be written as $[70 : 11]$, $[70 : -12]$, $[70 : 16]$, $[70 : -17]$, $[70 : 18]$, $[70 : -19]$, $[70 : 23]$, and $[70 : -24]$.

(c) The divisor of an ideal of norm $100 = 10^2$ can be any divisor of 10. The principal polynomial of discriminant $\Delta = 41$ is $\phi(x) = x^2 + x - 10$. Finding solutions of $\phi(x) \equiv 0 \pmod n$ for $n = 1$, 4, 25, and 100, we obtain the following list of ideals of norm 100 in D_{41}: $[100 : 10]$, $[100 : -11]$, $[100 : 14]$, $[100 : -15]$, $2[25 : 10]$, $2[25 : -11]$, $5[4 : 1]$, $5[4 : -2]$, and $10[1 : 0]$.

(10) If A is an ideal of a quadratic domain D, and v and w are elements of D, write $v \equiv w \pmod A$ to mean that $v - w$ is an element of A. We show as follows that *congruence modulo* A is an equivalence relation on D.

(a) If v is in D, then $v \equiv v \pmod A$ since $v - v = 0$ is an element of every ideal A. So congruence is reflexive.

(b) If $v \equiv w \pmod A$ so that $v - w$ is an element of A, then $w - v = -(v - w)$ is an element of A by properties of ideals. Thus $w \equiv v \pmod A$ and congruence is symmetric.

(c) If $u \equiv v \pmod A$ and $v \equiv w \pmod A$, so that $u - v$ and $v - w$ are elements of A, then $u - w = (u - v) + (v - w)$ is also in A by closure properties of ideals. Thus $u \equiv w \pmod A$ and congruence is transitive.

Now suppose that $A = g[a : k]$ with g and a positive, so that $S = \{ga, gk + gz\}$ is a $\mathbb{Z}$-basis for A. Let $v = s + tz$ be an element of D. Write $t = gn + r$ with $0 \leq r < g$, and then write $s - gnk = (ga)m + q$ with $0 \leq q < ga$. Then $(s + tz) - (q + rz) = (s - q) + (t - r)z = m(ga) + n(gk + gz)$ is an element of A, so that $s + tz \equiv q + rz \pmod A$. Thus every element of D is congruent modulo A to an element $q + rz$ with $0 \leq q < ga$ and $0 \leq r < g$. Finally, suppose that $q + rz \equiv s + tz \pmod A$ with $0 \leq q, s < ga$ and $0 \leq r, t < g$. We can assume without loss of generality that $r \geq t$. Then $(q - s) + (r - t)z$ is an element of A. With $0 \leq r - t < g$, we must conclude that $r = t$ to avoid contradicting the definition of the divisor of A. So $q - s$ is a rational integer in A, and with $-ga < q - s < ga$, we must likewise conclude that $q = s$. Thus every element of D is congruent modulo A to precisely one element $q + rz$ with $0 \leq q < ga$ and $0 \leq r < g$, and there are exactly $g \cdot ga = g^2 a$ distinct equivalence classes of elements of D under congruence modulo A.

Section 3.2. Writing Ideals as Ideal Numbers.

(1) (a) In D_{13}, $N(q+rz) = q^2+qr-3r^2$. Since $N(1+3z) = -23$ and $3x \equiv 1 \pmod{23}$ has solution $k = 8$, we can write $A = \langle 1+3z\rangle = [-23 : 8] = [23 : 8]$. [To confirm this claim directly, the typical element of A has the form $(1+3z)(q+rz) = (q+9r)+(3q+4r)z$, here using the fact that $z^2 = 3+z$. Such an element is in $\mathbb{Z}$ only when $3q+4r = 0$, so that $q = 4u$ and $r = -3u$ for some $u \in \mathbb{Z}$. Then $q+9r = -23u$, and so $a = 23$ is the smallest positive integer in A. When $q = -1$ and $r = 1$, we have $8+z$ in A, and so $A = [23 : 8]$. The following examples can be confirmed in the same way.]

(b) In D_{28}, $N(1+3z) = 1^2 - 7\cdot 3^2 = -62$ and $3x \equiv 1 \pmod{62}$ has solution $k = 21$. So $A = \langle 1+3z\rangle = [-62 : 21] = [62 : 21]$.

(c) $N(5-3z) = 5^2+5(-3)-9(-3)^2 = -71$ in $D = D_{37}$, and $-3x \equiv 5 \pmod{71}$ has solution $k = 22$. So $A = \langle 5-3z\rangle = [-71 : 22] = [71 : 22]$.

(d) Here note first that $A = \langle 12-9z\rangle = 3\langle 4-3z\rangle$. In $D = D_{-67}$, $N(q+rz) = q^2+qr+17r^2$, so that $N(4-3z) = 157$. We find that $-3x \equiv 4 \pmod{157}$ has solution $k = 51$. Thus $A = 3[157 : 51]$.

(e) $N(13+5z) = 13^2+17\cdot 5^2 = 594$ in $D = D_{-68}$, and $5x \equiv 13 \pmod{594}$ has solution $k = -235$. Thus $A = \langle 13+5z\rangle = [594 : -235]$.

(2) Let D be the quadratic domain and $\phi(x)$ the principal polynomial of discriminant Δ. Suppose that D is a principal ideal domain and that a and k are integers for which a divides $\phi(k)$. Then $A = [a : k]$ is an ideal of D, so can be written as $\langle v\rangle$ for some element v of D. But now either $[a : k]$ or $[-a : k]$ is an ideal form for v, using Theorem 3.2.2. Conversely, suppose that whenever a divides $\phi(k)$, then either $[a : k]$ or $[-a : k]$ is an ideal form of an element v of D. Then the ideal $A = [a : k]$ equals the principal ideal $\langle v\rangle$. Since every ideal of D has the form $g[a : k]$ where a divides $\phi(k)$, then every ideal of D is given by $g\langle v\rangle = \langle gv\rangle$ for some v in D. That is, D is a principal ideal domain.

(3) Let A and B be ideals of D, and let $A+B = \{a+b \mid a \in A \text{ and } b \in B\}$. If a_1+b_1 and a_2+b_2 are in $A+B$, then $(a_1+b_1)-(a_2+b_2) = (a_1-a_2)+(b_1-b_2)$ is an element of $A+B$ by the closure of both A and B under subtraction. Likewise, if $a+b$ is in $A+B$ and v is in D, then $(a+b)v = av+bv$ is an element of $A+B$ since av is in A and bv is in B. Thus $A+B$ is an ideal of D. If a is an element of A, then $a = a+0$ is in $A+B$, since 0 is an element of B. So $A \subseteq A+B$, and by the same argument, $B \subseteq A+B$. Finally, suppose that C is an ideal of D that contains both A and B as subsets. Then for any a in A and b in B, the sum $a+b$ is an element of C by closure properties of ideals. It follows that $A+B \subseteq C$.

(4) Let v and w be elements of a quadratic domain D. The typical element of $\langle v, w\rangle$ has the form $vx+wy$ where x and y are in D. Since $vx \in \langle v\rangle$ and $wy \in \langle w\rangle$, it follows that $\langle v, w\rangle \subseteq \langle v\rangle + \langle w\rangle$. The reverse inclusion is shown in the same way.

(5) (a) In D_{13}, we can write $\langle 12\rangle = 12[1 : 0]$ and $\langle 5+z\rangle = 275$ since $N(5+z) = 5^2+5\cdot 1-3(1)^2$. Since $\gcd(12, 27, 12\cdot 5) = 3$, with $x \equiv 5 \equiv -1 \pmod{3}$, we find that $A = \langle 12, 5+z\rangle = [3 : -1]$ in D_{13}.

(b) In D_{-40}, we have $\langle 7\rangle = 7[1 : 0]$ and $\langle 3-2z\rangle = [49 : 23]$. Here $\gcd(7, 49, 7\cdot 23) = 7$ and we find that $A = \langle 7, 3-2z\rangle = [7 : 2]$ in D_{-40}.

(c) Since $\langle 7\rangle = 7[1 : 0]$ and $\langle 3+z\rangle = [7 : 3]$, we find that $A = \langle 14, 6+2z\rangle = 2\langle 7, 3+z\rangle = 2[7 : 3]$ in D_8. (Note that in this example, 7 is an element of $\langle 3+z\rangle$, so that $\langle 7, 3+z\rangle = \langle 3+z\rangle$.)

(6) Suppose that A is an ideal of a quadratic domain D, and let $\overline{A} = \{\overline{v} \mid v \in A\}$. If $\overline{v}$ and $\overline{w}$ are elements of $\overline{A}$, so that v and w are in A, then $\overline{v}-\overline{w} = \overline{v-w}$ is also in $\overline{A}$, here using properties of conjugate elements and the fact that $v-w$ is an element of A. Likewise, if

$\overline{v}$ is in $\overline{A}$, so that v is in A, and w is an element of D, then $\overline{v}\cdot w = \overline{v\cdot\overline{w}}$ is an element of $\overline{A}$. (Here $\overline{w}$ is also an element of D, so we use the multiplicative property of the ideal A.) Thus $\overline{A}$ is an ideal of D.

(7) Let $A = \langle v\rangle$ be a principal ideal of a quadratic domain D. If w is an element of $\overline{A}$, then $w = \overline{vx} = \overline{v}\cdot\overline{x}$ for some element x of D, since every element of A has the form vx. It follows that $\overline{A}\subseteq\langle\overline{v}\rangle$. Conversely, the typical element of $\langle\overline{v}\rangle$ has the form $y = \overline{v}\cdot x$ for some x in D. But then $y = \overline{v\cdot\overline{x}}$ is in $\overline{A}$ by definition, since $\overline{x}$ is in D so that $v\cdot\overline{x}$ is in $A = \langle v\rangle$. Thus $\langle\overline{v}\rangle\subseteq\overline{A}$, and $\overline{A} = \langle\overline{v}\rangle$.

Section 3.3. Prime Ideals of Quadratic Domains.

(1) Let $A = [5:2]$, $\overline{A} = [5:-2]$, $B = 5[1:0]$, and $C = [65:8]$, ideals of the quadratic domain $\mathbb{Z}[i] = D_{-4}$.
   (a) B is a subset of A since $g = 1$ divides $h = 5$, $ag = 5$ divides $bh = 5$, and $h\ell\equiv hk \pmod{ag}$, that is, $0\equiv 10 \pmod 5$.
   (b) B is likewise a subset of $\overline{A}$. (Here we also have $0\equiv -10 \pmod 5$.)
   (c) C is not a subset of A, and A is not a subset of C. Here 5 is an element of A not in C, and $8+i$ is an element of C not in A.
   (d) C is a subset of $\overline{A}$. Here with $g = 1 = h$, we note that $a = 5$ divides $b = 65$, and that $\ell\equiv k \pmod a$, that is, $8\equiv -2 \pmod 5$.

(2) Let $A = g[a:k]$ and $B = h[b:\ell]$ be ideals of a quadratic domain D. By Proposition 3.3.1, $B\subseteq A$ if and only if g divides h, ag divides bh, and $h\ell\equiv hk \pmod{ag}$, and $A\subseteq B$ if and only if h divides g, bh divides ag, and $gk\equiv g\ell \pmod{bh}$. It follows that $A = B$ if and only if $g = h$ (since g and h are both positive), $ag = \pm bh$ so that $a = \pm b$, and $\ell\equiv k \pmod a$, using the congruence cancellation property.

(3) If $B = h[b:\ell]$ is a subset of $A = g[a:k]$, then g divides h and ag divides bh. It follows immediately that $N(A) = |g^2a|$ divides $N(B) = |h^2b|$.

(4) If $B = h[b:\ell]$ is a subset of $A = g[a:k]$, then g divides h, ag divides bh, and $h\ell\equiv hk \pmod{ag}$. But if $N(A) = |g^2a|$ equals $N(B) = |h^2b|$, then $g = h$ and $|ag| = |bh|$ so that $b = \pm a$. Then $h\ell\equiv hk \pmod{ag}$ implies that $\ell\equiv k \pmod a$, and by Exercise 2 we conclude that $A = B$.

(5) (a) Since $\left(\frac{-7}{23}\right) = \left(\frac{23}{7}\right) = 1$, there are two conjugate prime ideals of norm $p = 23$ in D_{-7}, which we find to be $[23:9]$ and $[23:-10]$.
   (b) With $-23\equiv 1 \pmod 8$, there are two prime ideals of norm $p = 2$ in D_{-23}, namely $[2:0]$ and $[2:-1]$.
   (c) $\left(\frac{29}{5}\right) = \left(\frac{4}{5}\right) = 1$, so there are two prime ideals of norm $p = 5$ in D_{29}: $[5:1]$ and $[5:-2]$.
   (d) $-47\equiv 1 \pmod 8$ so $[2:0]$ and $[2:1]$ are prime ideals of norm $p = 2$ in D_{-47}.
   (e) $\left(\frac{-47}{3}\right) = \left(\frac{1}{3}\right) = 1$, so there are two prime ideals of norm $p = 3$ in D_{-47}: $[3:0]$ and $[3:-1]$.
   (f) $\left(\frac{-47}{17}\right) = \left(\frac{4}{17}\right) = 1$, so there are two prime ideals of norm $p = 17$ in D_{-47}: $[17:7]$ and $[17:-8]$.
   (g) $\left(\frac{-47}{23}\right) = \left(\frac{-1}{23}\right) = -1$, so there are no ideals of norm $p = 23$ in D_{-47}. The only prime ideal containing 23 is the principal ideal $\langle 23\rangle$.
   (h) $\left(\frac{-60}{11}\right) = -1$, so there are no ideals of norm $p = 11$ in D_{-60}. The only prime ideal containing 11 is $\langle 11\rangle$.

Section 3.4. Multiplication of Ideals.

(1) Let A and B be ideals of a quadratic domain D. Let $v_1w_1 + v_2w_2 + \cdots v_nw_n$ and $x_1y_1 + x_2y_2 + \cdots + x_my_m$ be elements of AB, where each v_i and x_i is in A, and each w_i and y_i is in B. Then $(v_1w_1 + v_2w_2 + \cdots v_nw_n) - (x_1y_1 + x_2y_2 + \cdots + x_my_m) = v_1w_1 + \cdots + v_nw_n +$

$x_1(-y_1)+\cdots+x_m(-y_m)$ is a finite sum of products of element of A and elements of B, so is an element of AB. Likewise, if u is an element of D, then $u(v_1w_1+v_2w_2+\cdots v_nw_n) = (uv_1)w_1+(uv_2)w_2+\cdots+(uv_n)w_n$ is a finite sum of products of elements of A with elements of B, so is in AB. Thus AB is an ideal of D. Note that each product v_iw_i is an element of A, by closure properties of an ideal, and thus the sum of any finite number of such products is in A. Thus $AB \subseteq A$. The proof that $AB \subseteq B$ is similar.

(2) Let A, B, and C be ideals of a quadratic domain D.
   (a) The typical element of AB has the form $v_1w_1 + v_2w_2 + \cdots v_nw_n$ with each v_i in A and each w_i in B. This expression equals $w_1v_1 + w_2v_2 + \cdots w_nv_n$, so is an element of BA. Thus $AB \subseteq BA$. The proof of the reverse containment is similar.
   (b) The typical element of $A(BC)$ is a sum of products $u(v_1w_1+v_2w_2+\cdots v_nw_n)$ where u is in A, and each v_i is in A and each w_i is in B. If we distribute u through each sum, and write each product $u(v_iw_i)$ as $(uv_i)w_i$, we see that all such expressions are elements of $(AB)C$. Therefore $A(BC) \subseteq (AB)C$. The proof of the reverse containment is similar.
   (c) If a is in A, then $a = a \cdot 1$ is in AD, since 1 is in D. Thus $A \subseteq AD$. For the reverse containment, we can use the observation from Exercise 1 that a product AD of A with any ideal of D is a subset of A.
   (d) If $v_1w_1 + v_2w_2 + \cdots v_nw_n$ is in AB, then $\overline{v_1w_1 + v_2w_2 + \cdots v_nw_n} = \overline{v_1} \cdot \overline{w_1} + \cdots \overline{v_n} \cdot \overline{w_n}$ is an element of $\overline{A} \cdot \overline{B}$. Thus $\overline{AB} \subseteq \overline{A} \cdot \overline{B}$. The reverse containment uses the same equation.
   (e) The typical element of $\langle vw \rangle$ is vwx where x is in D. But $vwx = v(wx)$, with $wx \in \langle w \rangle$, and so $\langle vw \rangle \subseteq \langle v \rangle \langle w \rangle$. For the reverse containment, the typical element of $\langle v \rangle \langle w \rangle$ has the form $(vx_1)(wy_1) + (vx_2)(wy_2) + \cdots + (vx_n)(wy_n) = vw(x_1y_1 + x_2y_2 + \cdots x_ny_n)$, with each x_i and y_i in D. The final equation shows that each such expression is an element of $\langle vw \rangle$, and so $\langle v \rangle \langle w \rangle \subseteq \langle vw \rangle$.

(3) Let A be an ideal of a quadratic domain D_Δ, written as $A = g[a : k]$ and as $A = g[a : \ell]$, where $\ell \equiv k \pmod{a}$, say $\ell = k + aq$ for some rational integer q. If $\phi(x)$ is the principal polynomial of discriminant Δ, then direct calculation shows that $\phi(\ell) = \phi(k + aq) = \phi(k) + \phi'(k) \cdot aq + a^2q^2$ and $\phi'(ell) = \phi'(k) + 2aq$. So if $\phi(k) = ac$, $\phi(\ell) = ac_0$, $\phi'(k) = b$, and $\phi'(\ell) = b_0$, we find that $c_0 = c+bq+aq^2$ and $b_0 = b+2aq$. Any common divisor of a, b, and c also is a common divisor of a, b_0, and c_0. But likewise, any common divisor of a, b_0, and c_0 also divides a, $b = b_0 - 2aq$, and $c = c_0 - bq - aq^2$. Thus $\gcd(a, b, c) = \gcd(a, b_0, c_0)$, and the index of A is well-defined.

(4) The principal polynomial of discriminant $\Delta = 61$ is $\phi(x) = x^2 + x - 15$. Since $\phi(0) = -15$ is divisible by 3 and 5, then $A = [3 : 0]$ and $B = [5 : 0]$ are ideals of D_{61}.
   (a) $AB = [3 : 0] \cdot [5 : 0] = [15 : 0]$, since $x = 0$ is the unique solution modulo 15 of $x \equiv 0 \pmod 3$ and $x \equiv 0 \pmod 5$.
   (b) $A^2 = [3 : 0] \cdot [3 : 0] = [9 : -3]$. Here $A \neq \overline{A} = [3 : -1]$, and we find that -3 is the unique solution of $\phi(x) \equiv 0 \pmod 9$ that is congruent to 0 modulo 3.
   (c) $B^2 = [5 : 0] \cdot [5 : 0] = [25 : -10]$. Again $B \neq \overline{B} = [5 : -1]$, and here -10 satisfies $\phi(x) \equiv 0 \pmod{25}$ with $-10 \equiv 0 \pmod 5$.
   (d) $A\overline{B} = [3 : 0] \cdot [5 : -1] = [15 : -6]$, since $x = -6$ satisfies $x \equiv 0 \pmod 3$ and $x \equiv -1 \pmod 5$.
   (e) $A^2B = [9 : -3] \cdot [5 : 0] = [45 : 15]$, since $x = 15$ satisfies $x \equiv -3 \pmod 9$ and $x \equiv 0 \pmod 5$.
   (f) $A^3 = [27 : 6]$. Here $\phi(6) = 27$ is divisible by 27, with $6 \equiv 0 \pmod 3$.
   (g) $A^3B^2 = [27 : 6] \cdot [25 : -10] = [675 : -210]$, since $x = 210$ satisfies $x \equiv 6 \pmod{27}$ and $x \equiv -10 \pmod{25}$.

Section 3.5. Prime Ideal Factorization.

(1) (a) The principal polynomial of discriminant $\Delta = -20$ is $\phi(x) = x^2 + 5$. Since $\phi(35) = 1230 = 615 \cdot 2$, then $[615 : 35]$ is an ideal of D_{-20}. Since $-20 = 4 \cdot -5$ is a primitive discriminant, and $615 = 3 \cdot 5 \cdot 41$, we find that

$$[615 : 35] = [3 : 35] \cdot [5 : 35] \cdot [41 : 35] = [3 : -1] \cdot [5 : 0] \cdot [41 : -6].$$

(b) For $\Delta = 41$, $\phi(x) = x^2 + x - 10$. Here $\phi(39) = 1550 = 775 \cdot 2$, so $[775 : 39]$ is an ideal of D_{41}. With $775 = 5 \cdot 5 \cdot 31$, we have that

$$[775 : 39] = [5 : 39]^2 \cdot [31 : 39] = [5 : -1]^2 \cdot [31 : -8].$$

(c) For $\Delta = -39$, $\phi(x) = x^2 + x + 10$, and we find that $\phi(29) = 880 = 220 \cdot 4$. So $[220 : 29]$ is an ideal of D_{-39}, which we can factor as

$$[220 : 29] = [2 : 29]^2 \cdot [5 : 29] \cdot [11 : 29] = [2 : 1]^2 \cdot [5 : -1] \cdot [11 : -4].$$

(2) We found the following ideals of norm $75 = 3 \cdot 5^2$ in D_{124}, and can factor them as shown since D_{124} is a complete quadratic domain.
(a) $[75 : 16] = [3 : 1] \cdot [5 : 1] \cdot [5 : 1]$.
(b) $[75 : -16] = [3 : -1] \cdot [5 : -1] \cdot [5 : -1]$.
(c) $[75 : 34] = [3 : 1] \cdot [5 : -1] \cdot [5 : -1]$.
(d) $[75 : -34] = [3 : -1] \cdot [5 : 1] \cdot [5 : 1]$.
(e) $5 \cdot [3 : 1] = [3 : 1] \cdot [5 : 1] \cdot [5 : -1]$.
(f) $5 \cdot [3 : -1] = [3 : -1] \cdot [5 : 1] \cdot [5 : -1]$.

(3) (a) In D_{40}, we find that $\langle 4 - 6z \rangle = 2 \langle 2 - 3z \rangle = 2 \cdot [86 : 28]$, since $N((2 - 3z) = 2^2 - 10(-3)^2 = -86$, and $k = 28$ satisfies $-3k \equiv 2 \pmod{86}$. Since 2 divides 40, we find that $\langle 2 \rangle = [2 : 0]^2$, and so we calculate that $\langle 4 - 6z \rangle = [2 : 0]^3 \cdot [43 : -15]$.
(b) In D_{-11}, we can write $\langle 4 + 3z \rangle = [55 : -17]$, since $N(4+3z) = 4^2+4 \cdot 3+3 \cdot 3^2 = 55$ and $3 \cdot -17 \equiv 4 \pmod{55}$. This ideal factors into prime ideals as $[55 : 17] = [5 : 2] \cdot [11 : -5]$.
(c) In D_{-68}, we can write $\langle 6 + 12z \rangle = 6 \langle 1 + 2z \rangle = 6 \cdot [69 : -34]$, since $N(1 + 2z) = 1^2 + 17 \cdot 2^2 = 69$, and $2 \cdot -34 \equiv 1 \pmod{69}$. Since 2 divides -68, we find that $\langle 2 \rangle = [2 : 1]^2$, and since $\left(\frac{-68}{3}\right) = 1$, we find that $\langle 3 \rangle = [3 : 1] \cdot [3 : -1]$. Combining these results, we can write

$$\langle 6 + 12z \rangle = [2 : 1]^2 \cdot [3 : 1] \cdot [3 : -1]^2 \cdot [23 : -11].$$

(d) In D_{-23}, we can write $\langle -2 + 3z \rangle$ as $[52 : -18] = [2 : 0]^2 \cdot [13 : -5]$. (Here $N(-2+3z) = (-2)^2 + (-2)3 + 6(3)^2 = 52$, and $3 \cdot -18 \equiv -2 \pmod{52}$.)
(e) In D_{220}, we can write $\langle 23 + 3z \rangle$ as $[34 : -15] = [2 : 1] \cdot [17 : 2]$. (Here $N(23 + 3z) = 23^2 - 55 \cdot 3^2 = 34$, and $3 \cdot -15 \equiv 23 \pmod{34}$.)

(4) Let D be the quadratic domain of discriminant $\Delta(-11, 5) = -275$, for which $\phi(x) = x^2 + 5x + 75$.
(a) The ideal $A = [25 : 0]$ is not a complete ideal, and cannot be written as a product of prime ideals of D. Here $P = [5 : 0]$ is the only prime ideal that contains A, but we find that $P^2 = 5P$, so that $P^2 \subseteq A \subseteq P$ with both containments proper.
(b) $A = [27 : 1]$ is a complete ideal since $N(A) = 99$ is relatively prime to $\gamma_\Delta = 5$. We can factor A as $[3 : 1]^3$.
(c) $A = [99 : 3]$ is also a complete ideal, and can be factored as $[3 : 0]^2 \cdot [11 : 3]$.

(5) Applying Theorem 12.3, we find that an element v having ideal form $g[a : k]$ divides a rational integer $m = m[1 : 0]$ in a quadratic domain if and only if ag divides m. In each part below, we find divisors of m in D by testing for elements whose subnorm divides m.

(a) In D_{-40}, with $z = \sqrt{-10}$, the norm of an element $q + rz$ is $q^2 + 10r^2$. We find that $49 = 7 \cdot 7 = (3+2z)(3-2z)$, with each factor irreducible in D_{-40} since $q^2+10r^2 = 7$ has no integer solutions, so that no elements of norm 7 exist. In ideal number notation, we have that $\langle 49 \rangle = [7 : 2]^2 \cdot [7 : -2]^2$. Here

$$\langle 7 \rangle \cdot \langle 7 \rangle = ([7 : 2] \cdot [7 : -2])([7 : 2] \cdot [7 : -2]),$$

while

$$\langle 3 + 2z \rangle \cdot \langle 3 - 2z \rangle = ([7 : -2] \cdot [7 : -2])([7 : 2] \cdot [7 : 2]).$$

(Note that $[7 : -2]^2 = [49 : -23] = \langle 3 + 2z \rangle$ since $N(3 + 2z) = 49$ and $k = -23$ satisfies $2k \equiv 3 \pmod{49}$.)

(b) In D_{-15}, we can write $16 = 2 \cdot 2 \cdot 2 \cdot 2 = z \cdot z \cdot (1 - z) \cdot (1 - z)$ where $z = \frac{1+\sqrt{-15}}{2}$. (A third possibility, using the same factors, is $16 = 2 \cdot 2 \cdot z \cdot (1 - z)$.) The norm of an element $q + rz$ is $q^2 + qr + 4r^2 = \frac{1}{4}((2q + r)^2 + 15r^2)$, so it follows that there are no elements of norm 2 in D_{-15} (since there are no solutions of $x^2 + 15y^2 = 8$), and so each of these factors is irreducible. Here $\langle 16 \rangle = [2 : 0]^4 \cdot [2 : -1]^4$, with

$$\langle 2 \rangle \cdot \langle 2 \rangle \cdot \langle 2 \rangle \cdot \langle 2 \rangle = ([2 : 0] \cdot [2 : -1])^2 \cdot ([2 : 0] \cdot [2 : -1])^2$$

and

$$\langle z \rangle \cdot \langle z \rangle \cdot \langle 1 - z \rangle \cdot \langle 1 - z \rangle = ([2 : 0] \cdot [2 : 0])^2 \cdot ([2 : -1] \cdot [2 : -1])^2.$$

(For example, $[2 : 0]^2 = [4 : 0] = \langle z \rangle$ since $N(z) = 4$ and $1 \cdot 0 \equiv 0 \pmod{4}$.)

(c) In D_{-84}, we find that there are three ways of writing 85 as a product of irreducible elements in D_{-84}: $85 = 5 \cdot 17 = (1 + 2z)(1 - 2z) = (8 + z)(8 - z)$, where $z = \sqrt{-21}$. (These factors are irreducible since $N(q + rz) = q^2 + 21r^2$ cannot take on the value 5 or 17.) Here $\langle 85 \rangle = [5 : 2] \cdot [5 : -2] \cdot [17 : 8] \cdot [17 : -8]$, with

$$\langle 5 \rangle \cdot \langle 17 \rangle = ([5 : 2] \cdot [5 : -2]) \cdot ([17 : 8] \cdot [17 : -8]),$$
$$\langle 1 + 2z \rangle \cdot \langle 1 - 2z \rangle = ([5 : -2] \cdot [17 : -8]) \cdot ([5 : 2] \cdot [17 : 8]),$$
$$\langle 8 + z \rangle \cdot \langle 8 - z \rangle = ([5 : -2] \cdot [17 : 8]) \cdot ([5 : 2] \cdot [17 : -8]).$$

For example, $\langle 1 + 2z \rangle = [85 : -42] = [5 : -2] \cdot [17 : -8]$ since $2 \cdot -42 \equiv 1 \pmod{85}$, while $\langle 8 + z \rangle = [85 : 8] = [5 : -2] \cdot [17 : 8]$.

(d) In D_{-23}, we can write $12 = 2 \cdot 2 \cdot 3 = 2 \cdot z \cdot (1 - z) = (2 + z) \cdot (3 - z)$, where $z = \frac{1+\sqrt{-23}}{2}$. Each factor is irreducible in D_{-23}, since the norm of an element $q + rz$ is $q^2 + qr + 6r^2 = \frac{1}{4}((2q + r)^2 + 23r^2)$. There are no elements of norm 2 or 3 in D_{-23} because $x^2 + 23y^2 = 8$ and $x^2 + 23y^2 = 12$ have no integer solutions. Here $\langle 12 \rangle = [2 : 0]^2 \cdot [2 : -1]^2 \cdot [3 : 0] \cdot [3 : -1]$, with

$$\langle 2 \rangle \cdot \langle 2 \rangle \cdot \langle 3 \rangle = ([2 : 0] \cdot [2 : -1]) \cdot ([2 : 0] \cdot [2 : -1]) \cdot ([3 : 0] \cdot [3 : -1]),$$
$$\langle 2 \rangle \cdot \langle z \rangle \cdot \langle 1 - z \rangle = ([2 : 0] \cdot [2 : -1]) \cdot ([2 : 0] \cdot \langle 3 \rangle 0) \cdot ([2 : -1] \cdot [3 : -1]),$$
$$\langle 2 + z \rangle \cdot \langle 3 - z \rangle = ([2 : 0] \cdot [2 : 0] \cdot [3 : -1]) \cdot ([2 : -1] \cdot [2 : -1] \cdot [3 : 0]).$$

For example, $\langle z \rangle = [6 : 0] = [2 : 0] \cdot [3 : 0]$ and $\langle 2 + z \rangle = [12 : 2] = [2 : 0] \cdot [2 : 0] \cdot [3 : -1]$.

(e) In D_{-120}, $130 = 2 \cdot 5 \cdot 13 = (10 + z)(10 - z)$, where $z = \sqrt{-30}$. Since $x^2 - 30y^2 = n$ has no solutions for $n = 2$, $n = 5$, $n = 10$, and $n = 13$, we can see that each of these factors is irreducible. But $\langle 130 \rangle = [2 : 0]^2 \cdot [5 : 0]^2 \cdot [13 : 3] \cdot [13 : -3]$, and we find that

$$\langle 2 \rangle \cdot \langle 5 \rangle \cdot \langle 13 \rangle = ([2 : 0] \cdot [2 : 0]) \cdot ([5 : 0] \cdot [5 : 0]) \cdot ([13 : 3] \cdot [13 : -3]),$$

and

$$\langle 10 + z \rangle \cdot \langle 10 - z \rangle = ([2 : 0] \cdot [5 : 0] \cdot [13 : -3]) \cdot ([2 : 0] \cdot [5 : 0] \cdot [13 : 3]).$$

(f) In D_{-132}, $42 = 2 \cdot 3 \cdot 7 = (3+z)(3-z)$, where $z = \sqrt{-33}$. These factors are all irreducible in that domain. Here $\langle 42 \rangle = [2:1]^2 \cdot [3:0]^2 \cdot [7:3] \cdot [7:-3]$, with

$$\langle 2 \rangle \cdot \langle 3 \rangle \cdot \langle 7 \rangle = ([2:1] \cdot [2:1]) \cdot ([3:0] \cdot [3:0]) \cdot ([7:3] \cdot [7:-3]),$$

and

$$\langle 3+z \rangle \cdot \langle 3-z \rangle = ([2:1] \cdot [3:0] \cdot [7:3]) \cdot ([2:1] \cdot [3:0] \cdot [7:-3]).$$

(g) In D_{-35}, $150 = 2 \cdot 3 \cdot 5 \cdot 5 = 2 \cdot 5 \cdot (2+z) \cdot (3-z)$, where $z = \frac{1+\sqrt{-35}}{2}$. With $N(q+rz) = q^2 + qr + 9r^2 = \frac{1}{4}((2q+r)^2 + 35r^2)$, we find that each of these factors is irreducible. (For instance, to write $2+z$ as a nontrivial product vw, we must have $N(v) = 3$ and $N(w) = 5$, or vice versa. Both of these are impossible.) Here the ideal $\langle 150 \rangle$ factors as $2[3:0] \cdot [3:-1] \cdot [5:2]^4$. (Here 2 does not factor in D_{-35} since $-35 \equiv 5 \pmod 8$.) We find that

$$\langle 2 \rangle \cdot \langle 3 \rangle \cdot \langle 5 \rangle \cdot \langle 5 \rangle = 2([3:0] \cdot [3:-1]) \cdot ([5:2] \cdot [5:2]) \cdot ([5:2] \cdot [5:2]),$$

while

$$\langle 2 \rangle \cdot \langle 5 \rangle \cdot \langle 2+z \rangle \cdot \langle 3-z \rangle = 2([5:2] \cdot [5:2]) \cdot ([3:-1] \cdot [5:2]) \cdot ([3:0] \cdot [5:2]).$$

Section 3.6. A Formula for Ideal Multiplication.

(1) Let $\phi(x) = x^2 + \varepsilon x + \frac{\varepsilon^2 - \Delta}{4}$. If $t = k + \ell + \phi'(0) = k + \ell + \varepsilon$, then

$$kt - \phi(k) = k^2 + k\ell + \varepsilon k - k^2 - \varepsilon k - \frac{\varepsilon^2 - \Delta}{4} = k\ell - \phi(0).$$

Now if $g = \gcd(a, b, t)$, then g divides kt, and g divides $\phi(k)$ since a divides $\phi(k)$ when $[a:k]$ is an ideal. Thus g divides $kt - \phi(k) = k\ell - \phi(0)$.

(2) Let $P = [7:2]$, an ideal of $D = D_{-31}$, so that $P^2 = [49:9]$ as established in an example. Then $P^4 = P^2 \cdot P^2 = [49:9] \cdot [49:9]$. Here $\gamma = 1$ since $\Delta = -31$ is a primitive discriminant, and with $\phi(x) = x^2 + x + 8$, we find that $t = k + \ell + \phi'(0) = 9 + 9 + 1 = 19$. Now $g = \gcd(49, 49, 19) = 1$ and $c = \frac{49 \cdot 49}{1^2} = 2401$, so we know that $P^4 = [2401 : m]$ for some integer m. Here m satisfies (among other congruences) $tm \equiv k\ell - \phi(0) \pmod c$, that is, $19m \equiv 73 \pmod{2401}$. Applying the Euclidean algorithm to write $1 = 19(1011) + 2401(-8)$, we calculate the unique solution of $19m \equiv 73 \pmod{2401}$ as $73(1011) = 73803 \equiv -628 \pmod{2401}$. Thus $P^4 = [2401 : -628]$.

(3) Each discriminant in this exercise is primitive, so that $\gamma = 1$ in each application of Theorem 3.6.1.

(a) With $\Delta = -20$, so that $\phi(x) = x^2 + 5$, we find that $[6:1] \cdot [14:3] = 2[21:10]$. Here $t = 1 + 3 + 0 = 4$ and so $g = \gcd(6, 14, 4) = 2$. Then $c = \frac{6 \cdot 14}{2 \cdot 2} = 21$, and $AB = 2[21:m]$ for m satisfying $\frac{t}{g} \cdot m \equiv \frac{1}{g}(k\ell - \phi(0)) \pmod c$, that is, $2m \equiv \frac{1}{2}(3-5) \pmod{21}$, so that $m = 10$.

(b) For $\Delta = -20$, we find $[6:1][21:4] = [126:25]$. In this case, $t = 1 + 4 + 0 = 5$, $g = \gcd(6, 21, 5) = 1$, $c = 6 \cdot 21 = 126$, and m satisfies $5m \equiv -1 \pmod{126}$.

(c) If $\Delta = -20$, then $[6:1] \cdot [21:-4] = 3[14:3]$. Here $t = 1 - 4 + 0 = -3$, $g = \gcd(6, 21, -3) = 3$, $c = \frac{6 \cdot 21}{3 \cdot 3} = 14$, and m satisfies $-m \equiv \frac{1}{3}(-4-5) \pmod{14}$.

(d) If $\Delta = -23$, with $\phi(x) = x^2 + x + 6$, then $[36:14] \cdot [142:20] = [5112:446]$. In this case, $t = 14 + 20 + 1 = 35$ so that $g = \gcd(36, 142, 35) = 1$. Then $c = 36 \cdot 142 = 5112$ and m satisfies $35m \equiv 14 \cdot 20 - 6 \pmod{5112}$.

(e) If $\Delta = -23$, then $[36:14] \cdot [142:-21] = 2[1278:50]$. Now $t = 14 - 21 + 1 = -6$ and $g = \gcd(36, 142, -6) = 2$. Then $c = \frac{36 \cdot 142}{2 \cdot 2} = 1278$, and m satisfies $-3m \equiv \frac{1}{2}(14 \cdot -21 - 6) \pmod{1278}$.

(4) If $\Delta = \Delta(-5,3) = -180$, then $\phi(x) = x^2 + 45$. In the following table, we list $\gamma(A)$, $\gamma(B)$, $\gamma = \gcd(\gamma(A), \gamma(B))$, and $t = k + \ell + \phi'(0)$, for the calculation of AB as $g[c : m]$ where $g = \gcd(a, b, t)$, $c = ab\gamma/g^2$, and m satisfies the congruences of Theorem 3.6.1.

A	B	$\gamma(A)$	$\gamma(B)$	γ	t	AB
$[3:0]$	$[3:0]$	3	3	3	0	$3[3:0]$
$[9:0]$	$[3:0]$	1	3	1	0	$3[3:0]$
$[9:3]$	$[3:0]$	3	3	3	3	$3[9:3]$
$[9:0]$	$[9:3]$	1	3	1	3	$3[9:3]$
$[9:0]$	$[9:0]$	1	1	1	0	$9[1:0]$
$[9:3]$	$[9:3]$	3	3	3	6	$3[27:-6]$
$[9:-3]$	$[9:3]$	3	3	3	0	$9[3:0]$
$[27:3]$	$[9:3]$	1	3	1	6	$3[27:-6]$

(5) If $\Delta = \Delta(-11,5) = -275$, then $\phi(x) = x^2 + 5x + 75$. In the following table, we list $\gamma(A)$, $\gamma(B)$, $\gamma = \gcd(\gamma(A), \gamma(B))$, and $t = k + \ell + \phi'(0) = k + \ell + 5$, for the calculation of AB as $g[c : m]$ where $g = \gcd(a, b, t)$, $c = ab\gamma/g^2$, and m satisfies the congruences of Theorem 3.6.1.

A	B	$\gamma(A)$	$\gamma(B)$	γ	t	AB
$[5:0]$	$[25:0]$	5	1	1	5	$5[5:0]$
$[5:0]$	$[25:5]$	5	5	5	10	$5[25:5]$
$[25:0]$	$[25:0]$	1	1	1	5	$5[25:10]$
$[25:0]$	$[25:5]$	1	5	1	5	$5[25:5]$
$[25:0]$	$[25:10]$	1	1	1	15	$5[25:-5]$
$[25:5]$	$[25:5]$	5	5	5	15	$5[125:-45]$
$[25:5]$	$[25:10]$	5	1	1	20	$5[25:5]$
$[25:10]$	$[25:10]$	1	1	1	25	$25[1:0]$

(6) Let D_1 be a subdomain of some quadratic domain D, let A be an ideal of D, and consider the set $A_1 = A \cap D_1$. If x and y are elements of A_1, then $x, y \in A$ and $x, y \in D_1$. The subdomain D_1 is closed under subtraction, as is the ideal A, so it follows that $x - y$ is an element of both A and D_1, so is in A_1. Now let x be an element of A_1 and let y be an element of D_1, so also an element of D. Since x is in A and y is in D, then xy is an element of A by the definition of an ideal. But also x is in D_1 and y is in D_1, and so xy is in D_1 by the closure of a subdomain under multiplication. Thus xy is in A_1, and A_1 is an ideal of D_1.

Section 4.1. Classification of Quadratic Forms.

(1) Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, so that $\overline{A} = \begin{bmatrix} a & -b \\ -c & d \end{bmatrix}$ and $\overline{B} = \begin{bmatrix} e & -f \\ -g & h \end{bmatrix}$.

(a) The determinant of $\overline{A}$ is $ad - (-b)(-c) = ad - bc$, the same as the determinant of A.

(b) $\overline{A} + \overline{B} = \begin{bmatrix} a+e & -b-f \\ -c-g & d+h \end{bmatrix} = \begin{bmatrix} a+e & -(b+f) \\ -(c+g) & d+h \end{bmatrix} = \overline{A+B}$.

(c) $\overline{A} \cdot \overline{B} = \begin{bmatrix} ae+bg & -(af+bh) \\ -(ce+dg) & cf+dh \end{bmatrix} = \overline{A \cdot B}$.

(2) Let $\overline{f}(x,y) = ax^2 - bxy + cy^2$ and $-f(x,y) = -ax^2 - bxy - cy^2$ be the conjugate and negative of $f(x,y) = ax^2 + bxy + cy^2$ respectively.

(a) If $f(q,r) = aq^2 + bqr + cr^2 = m$, then $\overline{f}(q,-r) = aq^2 - bq(-r) + c(-r)^2 = m$ also.

(b) Part (a) shows that $(q,r) \leftrightarrow (q,-r)$ describes a one-to-one correspondence between solutions of $f(x,y) = m$ and solutions of $\overline{f}(x,y) = m$ for each integer m. So these two quadratic forms represent the same collection of integers.

(c) If $f(q,r) = aq^2 + bqr + cr^2 = m$, then $-f(q,r) = -aq^2 - bqr - cr^2 = -m$, and vice versa.

(3) (a) The discriminant of $f(x,y) = 5x^2 - 3xy + 7y^2$ is $\Delta = (-3)^2 - 4 \cdot 5 \cdot 7 = -131 = \Delta(-131, 1)$. With $\varepsilon_\Delta = 1$, we find that $k = \frac{-3-1}{2} = -2$ and $f = (5 : -2)$ in ideal notation.

(b) The discriminant of $f(x,y) = 3x^2 - 6xy + 2y^2$ is $\Delta = (-6)^2 - 4 \cdot 3 \cdot 2 = 12 = \Delta(3,1)$. Here $\varepsilon = 0$ and $f = (3 : -3)$.

(c) The discriminant of $f(x,y) = 6x^2 + 10xy + y^2$ is $\Delta = 10^2 - 4 \cdot 6 \cdot 1 = 76 = \Delta(19,1)$. Here $\varepsilon = 0$ and $f = (6 : 5)$.

(4) If $\Delta = -31$, then $\phi(x) = x^2 + x + 8$ is the principal polynomial of this discriminant.

(a) $\phi(x) \equiv 0 \pmod 5$ has two solutions, $x = 1$ and $x = -2$. So $(5 : 1 + 5q)$ and $(5 : -2 + 5q)$ are quadratic forms in $\mathcal{Q}_{-31}$ for every integer q.

(b) $(7 : 2 + 7q)$ and $(7 : -3 + 7q)$ are quadratic forms in $\mathcal{Q}_{-31}$ for all q.

(c) $(35 : 11 + 35q)$, $(35 : 16 + 35q)$, $(35 : -12 + 35q)$, and $(35 : -17 + 35q)$ are elements of $\mathcal{Q}_{-31}$ for all q.

(5) Let $f(x,y) = ax^2 + bxy + cy^2$ be a quadratic form of discriminant Δ, with $f = (a : k)$ in ideal form. (So $k = \frac{b-\varepsilon}{2}$.)

(a) For $\overline{f}(x,y) = ax^2 - bxy + cy^2$, we find that $\frac{-b-\varepsilon}{2} = -\frac{b-\varepsilon}{2} - \varepsilon = -k - \varepsilon$, so that $\overline{f} = (a : -k - \varepsilon)$ in ideal notation.

(b) For $-f(x,y) = -ax^2 - bxy - cy^2$, we have $\frac{-b-\varepsilon}{2} = -k - \varepsilon$ and $-f = (-a : -k - \varepsilon)$.

(c) For $-\overline{f}(x,y) = -ax^2 + bxy - cy^2$, we have $\frac{b-\varepsilon}{2} = k$ and $-\overline{f} = (-a : k)$.

Section 4.2. Equivalence of Quadratic Forms.

(1) Assuming the standard fact that $\det(AB) = \det(A) \cdot \det(B)$ for a pair of $n \times n$ matrices A and B, then Γ is closed under multiplication since $\det(UV) = \det(U) \cdot \det(V) = 1 \cdot 1 = 1$. Also, Γ contains the inverse of each of its elements, using the fact that $\det(A^{-1}) = 1/\det(A)$ when A is nonsingular.

(2) If $V = -U$, then $V^T = (-U)^T = -U^T$. So $V^T M_f V = -U^T M_f \cdot -U = U^T M_f U$, and $f \circ U = f \circ V$.

(3) Let f, g, and h be quadratic forms of some discriminant Δ.

(a) Since $I^T = I$, we find that $I^T M_f I = M_f$, and so $f \circ I = f$.

(b) If $U^T M_f U = M_g$, then $M_f = (U^T)^{-1} M_g U^{-1} = (U^{-1})^T M_g U^{-1}$, and so $f = g \circ U^{-1}$. (Note that $(U^T)^{-1} = (U^{-1})^T$ since $U^T \cdot (U^{-1})^T = (U^{-1} \cdot U)^T = I^T = I$, and likewise $(U^{-1})^T \cdot U^T = I$.)

(c) If $U^T M_f U = M_g$ and $V^T M_g V = M_h$, then $M_h = V^T (U^T M_f U) V = (UV)^T M_f (UV)$, and so $h = f \circ (UV)$. (Here we use the fact that $(AB)^T = B^T \cdot A^T$ for any two matrices A and B that can be multiplied.)

(4) Let H be a subgroup of Γ, with $f \sim_H g$ if $g = f \circ U$ for some U in H.

(a) We know that $f \circ I = f$, and I is an element of any subgroup H. Thus $f \sim_H f$ and $\sim_H$ is reflexive.

(b) If $g = f \circ U$, then $f = g \circ U^{-1}$, and if U is in H, then U^{-1} is in H. Thus if $f \sim_H g$, then $g \sim_H f$ and $\sim_H$ is symmetric.

(c) If $g = f \circ U$ and $h = g \circ V$, then $h = f \circ (UV)$, and if U and V are in H, then UV is also in H. Thus if $f \sim_H g$ and $g \sim_H h$, then $f \sim_H h$ and $\sim_H$ is transitive.

Therefore $\sim_H$ is an equivalence relation. If $f \sim_H g$ so that $g = f \circ U$ for some U in H, then U is also in Γ, and so $f \sim g$ is also true.

(5) The matrices of $-f$ and $-g$ are $-M_f$ and $-M_g$ respectively. If $g = f \circ U$, so that $M_g = U^T M_f U$, then $-M_g = -(U^T M_f U) = U^T(-M_f)U$, and thus $-g = -f \circ U$.

(6) The matrices of $\overline{f}$ and $\overline{g}$ are $\overline{M_f}$ and $\overline{M_g}$ respectively. If $M_g = U^T M_f U$, then

$$\overline{M_g} = \overline{U^T M_f U} = \overline{U}^T \cdot \overline{M_f} \cdot \overline{U}.$$

(Here we use Exercise 4.1.1, part (c).) Thus if $g = f \circ U$, then $\overline{g} = \overline{f} \circ \overline{U}$.

(7) Let $\Delta = -35$, so that $\phi(x) = x^2 + x + 9$. Since $\phi(7) = 65 = 13 \cdot 5$ and $\phi'(7) = 15$, then $f = (13 : 7)$ is an element of $\mathcal{Q}_{-35}$, specifically $f(x, y) = 13x^2 + 15xy + 5y^2$.

(a) If $U = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$, then $f(2, 3) = 187$ and $13(2)(3) + 15(3)(3) + 5(3)(5) + 7 = 295$, so that $f \circ U = (187 : 295)$.

(b) If $U = \begin{bmatrix} 7 & 3 \\ -5 & -2 \end{bmatrix}$, then $f(7, -5) = 237$ and $13(7)(3)+15(-5)(3)+5(-5)(-2)+7 = 105$, and $f \circ U = (237 : 105)$.

(c) If $U = \begin{bmatrix} 4 & 9 \\ 3 & 7 \end{bmatrix}$, then $f(4, 3) = 433$ and $13(4)(9) + 15(3)(9) + 5(3)(7) + 7 = 985$, and $f \circ U = (433 : 985)$.

(8) Since $\begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & v \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & u+v \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -u \\ 0 & 1 \end{bmatrix}$, then H is closed under multiplication and contains the inverse of each of its elements, and thus is a subgroup of Γ.

(9) Let $\Delta = -51$, so that $\phi(x) = x^2 + x + 13$. Since $\phi(16) = 285 = 57 \cdot 5$ and $\phi'(16) = 33$, we see that $f = [57 : 16]$ is a quadratic form in $\mathcal{Q}_{-51}$, specifically $f(x, y) = 57x^2 + 33xy + 5y^2$. Here we find that

$$(57 : 16) \leftrightarrow (5 : -17) \rightarrow_3 (5 : -2) \leftrightarrow (3 : 1),$$

so that f is equivalent to $(3 : 1)$, that is, $g(x, y) = 3x^2 + 3xy + 5y^2$. Specifically, $g = f \circ U$ where

$$U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 3 & -1 \end{bmatrix}.$$

Section 4.3. Representations of Integers by Quadratic Forms.

(1) If $f(x, y) = 3x^2 - 5xy + 4y^2$, then $f(2, 1) = 6$. With $\phi(x) = x^2 + x + 6$, we find that $f = (3 : -3)$ in ideal notation.

(a) If $U = \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix}$, then $g = f \circ U = (3 : -12)$, or $g(x, y) = 3x^2 - 23xy + 46y^2$ in standard notation. Here $U^{-1}\mathbf{x} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 1 \end{bmatrix}$, and we can verify that $g(5, 1) = 6$.

(b) $g = \begin{bmatrix} 2 & -3 \\ -3 & 5 \end{bmatrix} \circ (3 : -3) = (78 : -126)$, that is, $g(x, y) = 78x^2 - 251xy + 202y^2$. Here $U^{-1}\mathbf{x} = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 13 \\ 8 \end{bmatrix}$, and $g(13, 8) = 6$.

(c) $g = \begin{bmatrix} 7 & 9 \\ 3 & 4 \end{bmatrix} \circ (3 : -3) = (78 : 99)$, so $g(x,y) = 78x^2 + 199xy + 127y^2$. Here $U^{-1}\mathbf{x} = \begin{bmatrix} 4 & -9 \\ -3 & 7 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \end{bmatrix}$, and $g(-1,1) = 6$.

(2) If f is a quadratic form, then $\mathrm{Aut}(f)$ contains I, since $f \circ I = f$ is always true. If U and V are in $\mathrm{Aut}(f)$, so that $f \circ U = f$ and $f \circ V = f$, then we find that $f \circ U^{-1} = f$ and $f \circ (UV) = f$. (See Exercise 4.2.3.) Thus U^{-1} and UV are elements of $\mathrm{Aut}(f)$, and $\mathrm{Aut}(f)$ is a subgroup of the group Γ of unimodular matrices.

(3) Let $f(x,y) = x^2 + bxy + cy^2$, and suppose that $\Delta = b^2 - 4c < -4$. By equation (4.1.2), we know that if $f(q,r) = 1$, then $4 = (2q + br)^2 - \Delta r^2 > (2q + br)^2 + 4r^2$, and it follows that $r = 0$ and $q = \pm 1$. Then the characterization of automorphs in Proposition 4.3.4 shows that I and $-I$ are the only automorphs of f.

(4) For $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{Z} \times \mathbb{Z}$ (written as column matrices), we say that $\mathbf{x} \sim_f \mathbf{y}$ if there is an automorph U of f so that $\mathbf{y} = U\mathbf{x}$.
   (a) We know that I is an element of $\mathrm{Aut}(f)$ and $\mathbf{x} = I\mathbf{x}$. Thus $\sim_f$ is reflexive.
   (b) If $\mathbf{y} = U\mathbf{x}$, then $\mathbf{x} = U^{-1}\mathbf{y}$, and if U is in $\mathrm{Aut}(f)$, then U^{-1} is also in $\mathrm{Aut}(f)$. Thus $\sim_f$ is symmetric.
   (c) If $\mathbf{y} = U\mathbf{x}$ and $\mathbf{w} = V\mathbf{y}$, then $\mathbf{w} = (VU)\mathbf{x}$, and if U and V are in $\mathrm{Aut}(f)$, then VU is in $\mathrm{Aut}(f)$. Thus $\sim_f$ is transitive.

(5) Let $g = (87 : 39)$ in $\mathcal{Q}_{-23}$, with $\phi(x) = x^2 + x + 6$. Since $\phi(39) = 1566 = 87 \cdot 18$, and $\phi(-4) = 18$, we find that

$$g = (87 : 39) \leftrightarrow (18 : -40) \rightarrow_2 (18 : -4) \leftrightarrow (1 : 3) \rightarrow_{-3} (1 : 0) = h,$$

with

$$U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 3 \\ 2 & -7 \end{bmatrix}$$

a unimodular matrix for which $h = g \circ U$. Now since $g(1,0) = 87$, we calculate that

$$\begin{bmatrix} -1 & 3 \\ 2 & -7 \end{bmatrix}^{-1} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -7 & -3 \\ -2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -7 \\ -2 \end{bmatrix},$$

and verify that $h(-7,-2) = 87$.

Section 4.4. Genera of Quadratic Forms.

(1) In each part, we list all genus symbols defined for a primitive quadratic form of discriminant Δ, the combinations of genus symbols that can appear in practice, and an example of a quadratic form having that collection of genus symbols (found by trial-and-error).
   (a) For $\Delta = 21 = 3 \cdot 7$, the genus symbols that exist are $\left(\frac{f}{3}\right)$ and $\left(\frac{f}{7}\right)$. The product of these symbols must equal 1. We find that $f(x,y) = x^2 + xy - 5y^2$ is a quadratic form for which $\left(\frac{f}{3}\right) = 1 = \left(\frac{f}{7}\right)$, while for $f(x,y) = -x^2 - xy + 5y^2$ we have $\left(\frac{f}{3}\right) = -1 = \left(\frac{f}{7}\right)$.
   (b) For $\Delta = 28 = 2^2 \cdot 7$, the defined genus symbols are $\left(\frac{f}{7}\right)$ and $\left(\frac{-1}{f}\right)$, since $\frac{\Delta}{4} \equiv 3 \pmod 4$. The product of these symbols equals 1. Here $f(x,y) = x^2 - 7y^2$ has $\left(\frac{f}{7}\right) = 1 = \left(\frac{-1}{f}\right)$, while $f(x,y) = -x^2 + 7y^2$ has $\left(\frac{f}{7}\right) = -1 = \left(\frac{-1}{f}\right)$.
   (c) For $\Delta = 56 = 2^3 \cdot 7$, the defined genus symbols are $\left(\frac{f}{7}\right)$ and $\left(\frac{-2}{f}\right)$, since $\frac{\Delta}{4} \equiv 6 \pmod 8$, and the product of these symbols is 1. Here $f(x,y) = x^2 - 14y^2$ has $\left(\frac{f}{7}\right) = 1 = \left(\frac{-2}{f}\right)$, while $f(x,y) = -x^2 + 14y^2$ has $\left(\frac{f}{7}\right) = -1 = \left(\frac{-2}{f}\right)$.

(d) For $\Delta = 84 = 2^2 \cdot 3 \cdot 7$, the defined genus symbols are $\left(\frac{f}{3}\right)$ and $\left(\frac{f}{7}\right)$. (Since $\frac{\Delta}{4} \equiv 1 \pmod 4$, the symbol $\left(\frac{-1}{f}\right)$ is not well-defined for forms f of discriminant $\Delta = 84$.) Although $\Delta = \Delta(7,2)$, the product of these symbols equals 1, since both symbols are also defined for a quadratic form of discriminant $\Delta(21,1) = 21$. We find that $f(x,y) = x^2 - 21y^2$ has $\left(\frac{f}{3}\right) = 1 = \left(\frac{f}{7}\right)$ and $f(x,y) = -x^2 + 21y^2$ has $\left(\frac{f}{3}\right) = -1 = \left(\frac{f}{7}\right)$.

(e) For $\Delta = 112 = 2^4 \cdot 7$, the defined genus symbols are $\left(\frac{f}{7}\right)$ and $\left(\frac{-1}{f}\right)$, since $\frac{\Delta}{4} \equiv 0 \pmod 4$. Both symbols are defined for a quadratic form of discriminant $\Delta(7,1) = 28$, so their product equals 1. Here $f(x,y) = x^2 - 28y^2$ has $\left(\frac{f}{7}\right) = 1 = \left(\frac{-1}{f}\right)$, while $f(x,y) = -x^2 + 28y^2$ has $\left(\frac{f}{7}\right) = -1 = \left(\frac{-1}{f}\right)$.

(f) For $\Delta = 224 = 2^5 \cdot 7$, the symbols $\left(\frac{f}{7}\right)$, $\left(\frac{-1}{f}\right)$, $\left(\frac{2}{f}\right)$, and $\left(\frac{-2}{f}\right)$ are all defined, since $\frac{\Delta}{4} \equiv 0 \pmod 8$. With $\Delta = \Delta(14,2)$, we have that the product of $\left(\frac{f}{7}\right)$ and $\left(\frac{-2}{f}\right)$ must equal 1. (As noted in part (c), these are the defined genus symbols for a quadratic form of discriminant $\Delta(14,1) = 56$.) The product of $\left(\frac{-1}{f}\right)$, $\left(\frac{2}{f}\right)$, and $\left(\frac{-2}{f}\right)$ must also equal 1. Thus there are four possible genera. Here we find the following genus representatives, with symbols listed in order as $\left(\frac{f}{7}\right)$, $\left(\frac{-2}{f}\right)$, $\left(\frac{-1}{f}\right)$, and $\left(\frac{2}{f}\right)$.

$$\begin{array}{ll} ++++: & x^2 - 56y^2 \\ ---+: & -x^2 + 56y^2 \\ ++--: & -5x^2 + 2xy + 11y^2 \\ --+-: & 5x^2 - 2xy - 11y^2. \end{array}$$

Section 5.1. Equivalence of Ideals.

(1) Let B be an ideal of a quadratic domain D and let v be an element of D. Let x be an element of B, so that vx is an element of vB. Since v is an element of the principal ideal $\langle v \rangle$ and x is in B, then vx is an element of $\langle v \rangle B$, and thus $vB \subseteq \langle v \rangle B$. Conversely, let w be an arbitrary element of $\langle v \rangle B$, so that $w = (vy_1)x_1 + (vy_2)x_2 + \cdots + (vy_n)x_n$ where each y_i is an element of D and each x_i is an element of B. Notice that we can write $w = v(y_1x_1 + y_2x_2 + \cdots + y_nx_n)$, where $y_1x_1 + y_2x_2 + \cdots + y_nx_n$ is an element of B by the closure properties of an ideal. So w is in vB and it follows that $vB \subseteq \langle v \rangle B$. Therefore, vB is the same as the product of ideals $\langle v \rangle B$.

(2) Let A_1, A_2, B_1, and B_2 be nontrivial ideals of a quadratic domain D. Suppose that $A_1 \sim B_1$ and $A_2 \sim B_2$, say with $m_1A_1 = v_1B_1$ and $m_2A_2 = v_2B_2$ for some nonzero rational integers m_1 and m_2 and nonzero elements v_1 and v_2 of D. It follows that $(m_1m_2)A_1A_2 = (v_1v_2)B_1B_2$ and thus $A_1A_2 \sim B_1B_2$. (Here we use the fact that $m_1A_1 = \langle m_1 \rangle A_1$, and so forth, by Exercise 1, and properties of ideal multiplication from Exercise 3.4.2.)

(3) If A is a nontrivial ideal and v a nonzero element of a quadratic domain D, then the equation $1 \cdot (vA) = v \cdot A$ shows that $vA \sim A$ by definition.

(4) If $mA = vB$ for some nonzero rational integer m and nonzero element v of D, then $\langle m \rangle A = \langle v \rangle B$ by Exercise 1. It follows that $\overline{\langle m \rangle A} = \overline{\langle v \rangle B}$, so that $\overline{\langle m \rangle} \cdot \overline{A} = \overline{\langle v \rangle} \cdot \overline{B}$. Therefore $m\overline{A} = \overline{v}\overline{B}$, and thus $\overline{A} \sim \overline{B}$, using properties of conjugate ideals and of ideal multiplication.

(5) Let $f(x,y) = ax^2 + bxy + cy^2$, with index $\gamma = \gcd(a,b,c)$, and let $\phi(x)$ be the principal polynomial of discriminant $\Delta = b^2 - 4ac$. Let $k = \frac{b-\varepsilon}{2}$, where $\varepsilon = \phi'(0)$ is the basis index of Δ, so that $f = (a : k)$ in ideal notation, and let $A_f = [a : k]$ be its corresponding ideal. Since $\phi(k) = ac$ and $\phi'(k) = b$ (see Proposition 4.1.1), then $\gamma = \gcd(a,b,c)$ is also the index of A_f by definition.

(6) Let $D = D_{-79}$, with $z = \frac{1+\sqrt{-79}}{2}$ and $\phi(x) = x^2 + x + 20$.

(a) We find that $A = [80 : 19] \sim [5 : 0] \sim [4 : -1] = B$, using the fact that $\phi(19) = 400 = 80 \cdot 5$. It follows that $5 \cdot 4 \cdot A = (19 + z)(z)B$, that is, $A = (-1 + z)B$, since $z^2 = -20 + z$. (We can verify this equation by noting that $\langle -1 + z \rangle = [20 : -1]$, and calculating $[20 : -1] \cdot [4 : -1] = [80 : 19]$.)
(b) $A = [80 : -36] \sim [16 : 3] \sim [2 : 0] = B$, so that $16 \cdot 2 \cdot A = (-36 + z)(3 + z)B$. This simplifies to $A = (-4 - z)B$.
(c) $A = [178 : 59] \sim [20 : 0] \sim [1 : 0] = B$, with $20 \cdot A = (59 + z)(z)B$. This simplifies to $A = (-1 + 3z)B$.
(d) $A = [320 : -100] \sim [31 : 6] \sim [2 : -1] = B$, so that $31 \cdot 2 \cdot A = (-100 + z)(6 + z)B$, simplifying to $2A = (-20 - 3z)B$.
(e) $A = [325 : 80] \sim [20 : -1] \sim [1 : 0] = B$, with $20 \cdot A = (80 + z)(-1 + z)B$. This simplifies to $A = (-5 + 4z)B$.
(f) $A = [325 : -120] \sim [44 : -1] \sim [4 : 0] = B$, with $44 \cdot 4 \cdot A = (-120 + z)(-1 + z)B$, simplifying to $4A = (35 - 3z)B$.
(g) $A = [356 : 59] \sim [10 : 0] \sim [2 : -1] = B$, with $10 \cdot 2 \cdot A = (59 + z)(z)B$, simplifying to $A = (-1 + 3z)B$.
(h) $A = [712 : 59] \sim [5 : 0] \sim [4 : -1]$=B, with $5 \cdot 4 \cdot A = (59 + z)(z)B$, simplifying to $A = (-1 + 3z)B$.

Section 5.2. Quadratic Forms Associated to an Ideal.

(1) The principal polynomial of discriminant $\Delta = -111$ is $\phi(x) = x^2 + x + 28$. Since $\phi(3) = 40 = 8 \cdot 5$, then $A = [8 : 3]$ is an ideal of $D = D_{-111}$, that is, $S = \{8, 3 + z\}$ is an ordered basis for an ideal A of D. (Here $z = \frac{1+\sqrt{-111}}{2}$.) Let $u = 8$ and $v = 3 + z$.
   (a) For $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$, we have $qu + rv = 2(8) + 3(3 + z) = 25 + 3z$ and $su + tv = 3(8) + 5(3 + z) = 39 + 5z$. So $S \circ U = \{25 + 3z, 39 + 5z\}$.
   (b) If $U = \begin{bmatrix} 4 & -1 \\ 5 & -1 \end{bmatrix}$, then $S \circ U = \{47 + 5z, -11 - z\}$.
   (c) For $U = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$, we find $S \circ U = \{27 + z, 46 + 2z\}$.

(2) If $S = \{u, v\} = \{q + rz, s + tz\}$ is an ordered basis for the ideal $A = [8 : 3]$ of D_{-111}, then

$$u\overline{u} = q^2 + qr + 28r^2, \qquad u\overline{v} + \overline{u}v = 2qs + qt + rs + 56rt, \qquad v\overline{v} = s^2 + st + 28t^2.$$

In this case, $N(A) = 8$ divides each of these expressions, and $f_S(x, y)$ defined by

$$\left(\frac{q^2 + qr + 28r^2}{8}\right)x^2 + \left(\frac{2qs + qt + rs + 56rt}{8}\right)xy + \left(\frac{s^2 + st + 28t^2}{8}\right)y^2$$

is the quadratic form of this ordered basis. In particular, for $S = \{8, 3 + z\}$, with $q = 8$, $r = 0$, $s = 3$, and $t = 1$, we find that $f_S(x, y) = 8x^2 + 7xy + 5y^2$. In each part below, we calculate $f_S(x, y)$ for an ordered basis for A computed in Exercise 1.
   (a) If $S = \{25 + 3z, 39 + 5z\}$, we find that $f_S(x, y) = 119x^2 + 379xy + 302y^2$.
   (b) If $S = \{47 + 5z, -11 - z\}$, then $f_S(x, y) = 393x^2 - 177xy + 20y^2$.
   (c) If $S = \{27 + z, 46 + 2z\}$, then $f_S(x, y) = 98x^2 + 337xy + 290y^2$.

(3) Suppose that $S = \{u, v\}$ is a $\mathbb{Z}$-basis for an ideal A of a quadratic domain D so that every element of A can be written uniquely as $mu + nv$ for some rational integers m and n. Let w be an element of D, and consider the ideal $wA = \{wx \mid x \in A\}$. Every element of wA can be written as $w(mu + nv) = m(wu) + n(wv)$ for some rational integers m and n. If we write the same element of wA as $m(wu) + n(wv) = q(wu) + r(wv)$, then

$w(mu+nv) = w(qu+rv)$. If $w \neq 0$, then $mu+nv = qu+rv$ in A, from which we conclude that $m = q$ and $n = r$. Thus $\{wu, wv\}$ is a $\mathbb{Z}$-basis for wA by definition.

Section 5.3. Composition of Quadratic Forms.

(1) Let $f(x,y) = x^2 + 5y^2$ and $g(x,y) = 2x^2 + 2xy + 3y^2$.
   (a) If $f(q,r) = m$ and $f(s,t) = n$, then $f(u,v) = mn$ for $u = qs - 5rt$ and $v = qt + rs$. Here $f(2,1) = 9$ and $f(3,1) = 14$, so with $u = 2\cdot 3 - 5\cdot 1\cdot 1 = 1$ and $v = 2\cdot 1 + 1\cdot 3 = 5$, it follows that $f(1,5) = 9 \cdot 14 = 126$.
   (b) If $g(q,r) = m$ and $g(s,t) = n$, then $f(u,v) = mn$ for $u = 2qs + qt + rs - 2rt$ and $v = qt + rs + rt$. With $g(1,1) = 7$ and $g(2,1) = 15$, we find that $f(5,4) = 7 \cdot 15 = 105$.
   (c) If $f(q,r) = m$ and $g(s,t) = n$, then $g(u,v) = mn$ for $u = qs - rs - 3rt$ and $v = qt + 2rs + rt$. With $f(2,1) = 9$ and $g(1,1) = 7$, then $g(-2,5) = 9 \cdot 7 = 63$.
   (d) With $f(3,1) = 14$ and $g(1,1) = 7$, then $g(-1,6) = 14 \cdot 7 = 98$.
   (e) With $f(2,1) = 9$ and $g(2,1) = 15$, thn $g(-1,7) = 9 \cdot 15 = 135$.
   (f) With $f(3,1) = 14$ and $g(2,1) = 15$, then $g(1,8) = 14 \cdot 15 = 210$.

(2) (a) If $f_1(x,y) = x^2 + 2y^2 = f_2(x,y)$ in $\mathcal{Q}_{-8}$, then $f_1 = (1:0) = f_2$ in ideal notation, and $f_1 \cdot f_2 = f = (1:0)$ as well. If $f_1(q,r) = m$ and $f_2(s,t) = n$, then $f(u,v) = mn$ for $u = qs - 2rt$ and $v = qt + rs$.
   (b) If $f_1(x,y) = 2x^2 + 3y^2 = f_2(x,y)$ in $\mathcal{Q}_{-24}$, then $f_1 = (2:0) = f_2$ and $f_1 \cdot f_2 = f = (1:0)$, that is, $f(x,y) = x^2 + 6y^2$. If $f_1(q,r) = m$ and $f_2(s,t) = n$, then $f(u,v) = mn$ for $u = 2qs - 3rt$ and $v = qt + rs$.
   (c) For $f_1(x,y) = 2x^2 + xy + 3y^2 = f_2(x,y)$ in $\mathcal{Q}_{-23}$, we have $f = (2:0)\cdot(2:0) = (4:-2)$, that is, $f(x,y) = 4x^2 - 3xy + 2y^2$. If $f_1(q,r) = m$ and $f_2(s,t) = n$, then $f(u,v) = mn$ for $u = qs + qt + rs - rt$ and $v = 2qt + 2rs + rt$.
   (d) For $f_1(x,y) = 2x^2 + xy + 3y^2$ and $f_2(x,y) = 2x^2 - xy + 3y^2$ in $\mathcal{Q}_{-23}$, we have $f = (2:0)\cdot(2:-1) = (1:0)$, that is, $f(x,y) = x^2 + xy + 6y^2$. If $f_1(q,r) = m$ and $f_2(s,t) = n$, then $f(u,v) = mn$ for $u = 2qs - qt - 3rt$ and $v = qt + rs$.
   (e) For $f_1(x,y) = 2x^2 + xy + 6y^2 = f_2(x,y)$ in $\mathcal{Q}_{-47}$, we have $f = (2:0)\cdot(2:0) = (4:0)$, that is, $f(x,y) = 4x^2 + xy + 3y^2$. If $f_1(q,r) = m$ and $f_2(s,t) = n$, then $f(u,v) = mn$ for $u = qs - 3rt$ and $v = 2qt + 2rs + rt$.
   (f) For $f_1(x,y) = 2x^2 + xy + 6y^2$ and $f_2(x,y) = 3x^2 + xy + 4y^2$ in $\mathcal{Q}_{-47}$, we have $f = (2:0)\cdot(3:0) = (6:0)$, that is, $f(x,y) = 6x^2 + xy + 2y^2$. If $f_1(q,r) = m$ and $f_2(s,t) = n$, then $f(u,v) = mn$ for $u = qs - 2rt$ and $v = 2qt + 3rs + rt$.
   (g) For $f_1(x,y) = x^2 - 2y^2 = f_2(x,y)$ in $\mathcal{Q}_8$, we have $f = (1:0)\cdot(1:0) = (1:0)$, so that $f(x,y) = x^2 - 2y^2$ also. If $f_1(q,r) = m$ and $f_2(s,t) = n$, then $f(u,v) = mn$ for $u = qs + 2rt$ and $v = qt + rs$.
   (h) For $f_1(x,y) = x^2 - 10y^2 = f_2(x,y)$ in $\mathcal{Q}_{40}$, we find that $f(x,y) = x^2 - 10y^2$ also. If $f_1(q,r) = m$ and $f_2(s,t) = n$, then $f(u,v) = mn$ for $u = qs + 10rt$ and $v = qt + rs$.
   (i) For $f_1(x,y) = 2x^2 - 5y^2 = f_2(x,y)$ in $\mathcal{Q}_{40}$, we have $f = (2:0)\cdot(2:0) = (1:0)$, so that $f(x,y) = x^2 - 10y^2$. If $f_1(q,r) = m$ and $f_2(s,t) = n$, then $f(u,v) = mn$ for $u = 2qs + 5rt$ and $v = qt + rs$.
   (j) For $f_1(x,y) = x^2 - 10y^2$ and $f_2(x,y) = 2x^2 - 5y^2$ in $\mathcal{Q}_{40}$, $f = (1:0)\cdot(2:0) = (2:0)$, so that $f(x,y) = 2x^2 - 5y^2$. If $f_1(q,r) = m$ and $f_2(s,t) = n$, then $f(u,v) = mn$ for $u = qs + 5rt$ and $v = qt + 2rs$.

Section 5.4. Class Groups of Ideals and Quadratic Forms.

(1) Let u be an irreducible element of a quadratic domain D, and suppose that $\langle u\rangle \subseteq \langle v\rangle$ for some element v of D. In particular, since u is an element of $\langle u\rangle$, then u is in $\langle v\rangle$, and so $u = vw$ for some element w of D. But now by the definition of irreducible elements, then

either v or w is a unit in D. If w is a unit, then u and v are associates, and it follows that $\langle v\rangle = \langle u\rangle$. On the other hand, if v is a unit, then $1 = vv^{-1}$ is an element of $\langle v\rangle$, and thus $\langle v\rangle = D$. So $\langle u\rangle$ is maximal among principal ideals when u is irreducible in D.

(2) Suppose that D is a quadratic domain in which every ideal is a principal ideal, and let u be an irreducible element of D. If $\langle u\rangle \subseteq B$ for some ideal B of D, then $B = \langle v\rangle$ for some v in D, and Exercise 1 implies that either $B = \langle u\rangle$ or $B = D$. But then $\langle u\rangle$ is a prime ideal of D by definition.

(3) Let u be an element of a quadratic domain D, and suppose that $\langle u\rangle$ is a prime ideal of D. Suppose also that u divides some product vw of elements of D. It follows that vw is an element of $\langle u\rangle$. But then either v is in $\langle u\rangle$ or w is in $\langle u\rangle$. (This uses the property of prime ideals of D established in Proposition 3.3.2.) If v is in $\langle u\rangle$, then u divides v, while if w is $\langle u\rangle$, then u divides w. It follows that u is prime as an element of D.

(4) Suppose that D is a quadratic domain in which every ideal is a principal ideal. If u is an irreducible element of D, then Exercise 2 shows that $\langle u\rangle$ is a prime ideal of D. But then Exercise 3 implies that u is a prime element of D. Thus D is a unique factorization domain, since every irreducible element of D is also prime.

(5) Assuming that $D = [1 : 0]$ and $A = [2 : 1]$ represent all distinct classes of ideals of $D = D_{-20}$, we find the following operation table for $\mathcal{C}_{-20}$.

$\cdot$	$[1:0]$	$[2:1]$
$[1:0]$	$[1:0]$	$[2:1]$
$[2:1]$	$[2:1]$	$[1:0]$

Here the class of D is an identity element for multiplication. Since A is its own conjugate, we find that $[2:1]^2 = \langle 2\rangle$ is principal, and so is in the class of the ideal D. On the other hand, there are four distinct classes of quadratic forms in $\mathcal{F}_{-20}$, represented by $f = (1:0)$, $g = (2:1)$, $-f = (-1:0)$, and $-g = (-2:-1)$. An operation table for $\mathcal{F}_{-20}$ is

$\cdot$	$(1:0)$	$(2:1)$	$(-1:0)$	$(-2:-1)$
$(1:0)$	$(1:0)$	$(2:1)$	$(-1:0)$	$(-2:-1)$
$(2:1)$	$(2:1)$	$(1:0)$	$(-2:-1)$	$(-1:0)$
$(-1:0)$	$(-1:0)$	$(-2:-1)$	$(1:0)$	$(2:1)$
$(-2:-1)$	$(-2:-1)$	$(-1:0)$	$(2:1)$	$(1:0)$

(6) Assuming that each ideal of $D = D_{-56}$ is in the class of $D = [1:0]$, $A = [2:0]$, $B = [3:1]$, or $C = [3:-1]$, we find the following operation table for $\mathcal{C}_{-56}$.

$\cdot$	$[1:0]$	$[2:0]$	$[3:1]$	$[3:-1]$
$[1:0]$	$[1:0]$	$[2:0]$	$[3:1]$	$[3:-1]$
$[2:0]$	$[2:0]$	$[1:0]$	$[3:-1]$	$[3:1]$
$[3:1]$	$[3:1]$	$[3:-1]$	$[2:0]$	$[1:0]$
$[3:-1]$	$[3:-1]$	$[3:1]$	$[1:0]$	$[2:0]$

For example, $B^2 = [9:-2] \sim [2:0]$ using the fact that for the principal polynomial $\phi(x) = x^2 + 14$, we find that $\phi(-2) = 18 = 9 \cdot 2$. Other calculations are similar.

Section 6.1. Reduced Positive Definite Quadratic Forms.

(1) Let $f(x,y) = ax^2 + bxy + cy^2$ be a reduced quadratic form of some negative discriminant $\Delta = b^2 - 4ac$, so that $-a < b \leq a < c$ or $0 \leq b \leq a = c$. If g is a positive integer, then either $-ga < gb \leq ga < gc$ or $0 \leq gb \leq ga = gc$, and so the quadratic form $f_1(x,y) = gax^2 + gbxy + gcy^2$ is also reduced. The discriminant of f_1 is $(gb)^2 - 4(ga)(gc) = g^2(b^2 - 4ac) = g^2\Delta$.

(2) Let $f_1(x,y) = a_1x^2 + b_1xy + c_1y^2$ be a reduced quadratic form of negative discriminant $\Delta = b_1^2 - 4a_1c_1$. Let $g = \gcd(a_1, b_1, c_1)$ with $a_1 = ga$, $b_1 = gb$, and $c_1 = gc$. By definition, we have that $-ga < gb \le ga < gc$ or $0 \le gb \le ga = gc$, and since g is positive, we can cancel g throughout without changing the order of the inequalities. Thus $f(x,y) = ax^2 + bxy + cy^2$ is also reduced, and has discriminant $b^2 - 4ac = (b_1/g)^2 - 4(a_1/g)(c_1/g) = \Delta/g^2$.

(3) Let $f(x,y) = ax^2 + bxy + cy^2$ be a positive definite quadratic form of discriminant Δ. Let $\phi(x)$ be the principal polynomial of discriminant Δ, and suppose that $f = (a : k)$ in ideal notation, so that $\phi(k) = ac$ and $\phi'(k) = b$. Then we have that $-a < b \le a < c$ if and only if $-a < \phi'(k) \le a$ and $a^2 < ac = \phi(k)$. Likewise $0 \le b \le a = c$ if and only if $0 \le \phi'(k) \le a$ and $a^2 = ac = \phi(k)$.

(4) (a) If $\Delta = \Delta(-29, 1) = -116$, then $\phi(x) = x^2 + 29$ and $u_\Delta = \left\lfloor \sqrt{116/3} \right\rfloor = 6$. We can find all reduced forms of discriminant Δ by testing whether $1 \le a \le 6$ divides $\phi(k)$ for $-\frac{a}{2} < k \le \frac{a}{2}$. Using the following table

k	0	±1	±2	±3
$\phi(k)$	29	30	33	38

we obtain the following six reduced forms in $\mathcal{Q}_{-116}$:

$$(1:0), \quad (2:1), \quad (3:1), \quad (3:-1), \quad (5:1), \quad (5:-1).$$

Note that $(6:1)$ and $(6:-1)$ are not reduced since $6^2 > \phi(\pm1) = 30$.

(b) For $\Delta = \Delta(-29, 2) = -464$, we find $\phi(x) = x^2 + 116$ and $u_\Delta = 12$. From the table

k	0	±1	±2	±3	±4	±5	±6
$\phi(k)$	116	117	120	125	132	141	152

we obtain eighteen reduced forms in $\mathcal{Q}_{-464}$ (those in the third row are not primitive):

$$(1:0), \quad (3:1), \quad (3:-1), \quad (4:0), \quad (5:2), \quad (5:-2),$$
$$(8:2), \quad (8:-2), \quad (9:1), \quad (9:-1), \quad (11:4), \quad (11:-1),$$
$$(2:0), \quad (4:2), \quad (6:2), \quad (6:-2), \quad (10:2), \quad (10:-2).$$

(c) If $\Delta = \Delta(-119, 1) = -119$, then $\phi(x) = x^2 + x + 30$ and $u_\Delta = 6$. The table

k	$0, -1$	$1, -2$	$2, -3$
$\phi(k)$	30	32	36

produces ten reduced forms in $\mathcal{Q}_{-119}$:

$$(1:0), (2:0), (2:-1), (3:0), (3:-1), (4:1), (4:-2), (5:0), (5:-1), (6:2).$$

Note that $(6:-3)$ is not reduced since $6^2 = \phi(-3)$ but $-3 < 0$.

(d) If $\Delta = \Delta(-74, 1) = -296$, then $\phi(x) = x^2 + 74$ and $u_\Delta = 9$. From the table

k	0	±1	±2	±3	±4
$\phi(k)$	74	75	78	83	90

we obtain ten reduced forms in $\mathcal{Q}_{-296}$:

$$(1:0), (2:0), (3:1), (3:-1), (5:1), (5:-1), (6:2)(6:-2), (9:4), (9:-4).$$

(e) If $\Delta = \Delta(-85, 1) = -340$, then $\phi(x) = x^2 + 85$ and $m = 10$. The table

k	0	±1	±2	±3	±4	±5
$\phi(k)$	85	86	89	94	101	110

produces four reduced forms in $\mathcal{Q}_{-340}$:

$$(1:0), \qquad (2:1), \qquad (5:0), \qquad (10:5).$$

(f) If $\Delta = \Delta(-86, 1) = -344$, then $\phi(x) = x^2 + 86$ and $u_\Delta = 10$. From the table

k	0	±1	±2	±3	±4	±5
$\phi(k)$	86	87	90	95	102	111

we find ten reduced forms in $\mathcal{Q}_{-344}$:

$$(1:0), (2:0), (3:1), (3:-1), (5:2), (5:-2), (6:2), (6:-2), (9:2), (9:-2).$$

(g) If $\Delta = \Delta(-89, 1) = -356$, then $\phi(x) = x^2 + 89$ and $u_\Delta = 10$. From the table

k	0	±1	±2	±3	±4	±5
$\phi(k)$	89	90	93	98	105	114

we find twelve reduced forms in $\mathcal{Q}_{-356}$:

$$(1:0), \quad (2:1), \quad (3:1), \quad (3:-1), \quad (5:1), \quad (5:-1),$$

$$(6:1), \quad (6:-1), \quad (7:3), \quad (7:-3), \quad (9:1), \quad (9:-1).$$

(h) If $\Delta = \Delta(-105, 1) = -420$, then $\phi(x) = x^2 + 105$ and $u_\Delta = 11$. From

k	0	±1	±2	±3	±4	±5
$\phi(k)$	105	106	109	114	121	130

we find eight reduced forms in $\mathcal{Q}_{-420}$:

$$(1:0), \quad (2:1), \quad (3:0), \quad (5:0), \quad (6:3), \quad (7:0), \quad (10:5), \quad (11:4).$$

Note that $(11:-4)$ is not reduced since $11^2 = \phi(-4)$ but $-4 < 0$.

(5) (a) In $\mathcal{Q}_{-116}$, with $\phi(x) = x^2 + x + 30$, we find that $(60:14) \leftrightarrow (4:-15) \to_4 (4:1)$ since $\phi(14) = 240 = 60 \cdot 4$. The form $(4:1)$ is reduced, and the matrix

$$U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 4 \end{bmatrix}$$

has the property that $(60:14) \circ U = (4:1)$.

(b) In $\mathcal{Q}_{-340}$, with $\phi(x) = x^2 + 85$, we see that $(187:17) \leftrightarrow (2:-17) \to_9 (2:1)$, a reduced form. The matrix

$$U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 9 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 9 \end{bmatrix}$$

is such that $(187:17) \circ U = (2:1)$.

(c) In $\mathcal{Q}_{-420}$, we have $(179:49) \leftrightarrow (14:-49) \to_4 (14:7) \leftrightarrow (11:-7) \to_1 (11:4)$, a reduced form. The matrix

$$U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 4 & 3 \end{bmatrix}$$

has the property that $(179:49) \circ U = (11:4)$.

Section 6.2. Calculation of Ideal Class Groups.

(1) (a) The ideal class group of discriminant $\Delta = -20$ consists of the classes of $D = [1:0]$ and $A = [2:1]$. The invariant factor type of $\mathcal{C}_{-20}$ is (2), as we can verify by noting that $A^2 = 2[1:0] \sim [1:0]$.

(b) $\mathcal{C}_{-40} = \{[1:0], [2:0]\}$, with invariant factor type (2).

(c) There are five reduced ideals of discriminant $\Delta = -47$, so the class group $\mathcal{C}_{-47}$ must have invariant factor type (5). We can verify that if $A = [2:0]$, then $A^2 \sim [3:-1]$, $A^3 \sim [3:0]$, $A^4 \sim [2:-1]$, and $A^5 \sim [1:0]$.

(d) There are four reduced ideals of discriminant $\Delta = -56$. The invariant factor type of $\mathcal{C}_{-56}$ might be either (4) or (2, 2), but by trial-and-error, we find that if $A = [3 : 1]$, then $A^2 \sim [2 : 0]$, $A^3 \sim [3 : -1]$, and $A^4 \sim [1 : 0]$, so that $\mathcal{C}_{-56}$ has invariant factor type (4).

(e) There are four reduced ideals of discriminant $\Delta = -84$: $[1 : 0]$, $[2 : 1]$, $[3 : 1]$, and $[5 : 2]$. Each class is its own inverse in $\mathcal{C}_{-84}$, and so the ideal class group has invariant factor type $(2, 2)$. (For example, if $A = [5 : 2]$, then $A^2 = [25 : 2] \sim [1 : 0]$.)

(f) The class group of $\Delta = -116$ has six elements (listed in Exercise 6.1.4), and so must have invariant factor type (6). Direct calculation shows that if $A = [3 : 1]$, then the powers of $[A]$ in $\mathcal{C}_{-116}$ are, in order, $[3 : 1], [5 : 1], [2 : 1], [5 : -1], [3 : -1], [1 : 0]$.

(g) There are ten reduced ideals of discriminant $\Delta = -119$, found in Exercise 6.1.4, and so $\mathcal{C}_{-119}$ has invariant factor type (10). If $A = [3 : 0]$, then the powers of $[A]$ are:

$$[3 : 0], [4 : -2], [5 : 0], [2 : -1], [6 : 2], [2 : 0], [5 : -1], [4 : 1], [3 : -1], [1 : 0].$$

(h) The class group of $\Delta = -296$ has ten elements and invariant factor type (10). Direct calculation shows that if $A = [5 : 1]$, then the powers of $[A]$ are:

$$[5 : 1], [3 : -1], [6 : -2], [9 : -4], [2 : 0], [9 : 4], [6 : 2], [3 : 1], [5 : -1], [1 : 0].$$

(i) The class group of $\Delta = -340$ has four elements, $[1 : 0], [2 : 1], [5 : 0], [10 : 5]$. Each of these elements is its own inverse in $\mathcal{C}_{-340}$, so the class group has invariant factor type $(2, 2)$.

(j) The class group of $\Delta = -344$ has invariant factor type (10). If $A = [3 : 1]$, then the powers of $[A]$ are:

$$[3 : 1], [9 : -2], [5 : -2], [6 : 2], [2 : 0], [6 : -2], [5 : 2], [9 : 2], [3 : -1], [1 : 0].$$

(k) The class group of $\Delta = -356$ has twelve elements, so $\mathcal{C}_{-356}$ might have invariant factor type (12) or (6, 2). By trial-and-error, we find that every element of $\mathcal{C}_{-356}$ is a power of $[A]$, where $A = [3 : 1]$, and so has invariant factor type (12). The powers of $[A]$ are:

$$[3 : 1], [9 : 1], [7 : -3], [5 : 1], [6 : -1], [2 : 1], [6 : 1], [5 : -1], [7 : 3], [9 : -1], [3 : -1], [1 : 0].$$

(l) The class group of $\Delta = -420$ has eight elements,

$$[1 : 0], \quad [2 : 1], \quad [3 : 0], \quad [5 : 0], \quad [6 : 3], \quad [7 : 0], \quad [10 : 5], \quad [11 : 4],$$

so can have invariant factor type (8), (4, 2), or (2, 2, 2). In this case, each of these ideal classes is its own inverse, so $\mathcal{C}_{-420}$ has invariant factor type $(2, 2, 2)$.

(2) The upper bound u_Δ equals 1 for $\Delta = -3$, -4, -7, -8, and -11, so there can be only one distinct ideal class in $\mathcal{C}_\Delta$ in these cases, namely the class of $D = [1 : 0]$.

(a) If $\Delta = -19$, then $\phi(x) = x^2 + x + 5$ and $u_\Delta = 2$. Since 2 does not divide $\phi(0) = 5 = \phi(-1)$, we conclude that $\mathcal{C}_{-19}$ has only one element, the class of $[1 : 0]$.

(b) If $\Delta = -43$, then $\phi(x) = x^2 + x + 11$ and $u_\Delta = 3$. Since neither 2 nor 3 divides $\phi(0) = 11 = \phi(-1)$ or $\phi(1) = 13 = \phi(-2)$, we see that $\mathcal{C}_{-43} = \{[1 : 0]\}$.

(c) If $\Delta = -67$, then $\phi(x) = x^2 + x + 17$ and $u_\Delta = 4$. Since 2, 3, and 4 do not divide $\phi(0) = 17 = \phi(-1)$ or $\phi(1) = 19 = \phi(-2)$, it follows that $\mathcal{C}_{-67} = \{[1 : 0]\}$.

(d) If $\Delta = -163$, then $\phi(x) = x^2 + x + 41$ and $u_\Delta = 7$. Since $\phi(0) = 41 = \phi(-1)$, $\phi(1) = 43 = \phi(-2)$, $\phi(2) = 47 = \phi(-3)$, and $\phi(3) = 53 = \phi(-4)$ are not divisible by any integer 2 through 7, we conclude that $\mathcal{C}_{-163} = \{[1 : 0]\}$.

Section 6.3. Genera of Ideal Classes.

(1) In parts (a)–(l), we use the computations of $\mathcal{C}_\Delta$ compiled in Exercise 6.2.1.

(a) For ideals A of $\Delta = -20$, the defined genus symbols are $\left(\frac{-1}{A}\right)$ and $\left(\frac{A}{5}\right)$. We find that $\left(\frac{-1}{A}\right) = 1 = \left(\frac{A}{5}\right)$ for ideal classes in $\{[1:0]\}$ (the principal genus) and $\left(\frac{-1}{A}\right) = -1 = \left(\frac{A}{5}\right)$ for $\{[2:1]\}$. If $A = [2:1]$, then $G = \mathcal{C}_{-20} = \{[A]^0, [A]^1\}$, and $G^2 = \{[A]^0\} = \{[1:0]\}$, the principal genus as noted above.

(b) For $\Delta = -40$, the defined genus symbols are $\left(\frac{-2}{A}\right)$ and $\left(\frac{A}{5}\right)$. Here $\left(\frac{-2}{A}\right) = 1 = \left(\frac{A}{5}\right)$ for $[A]$ in $\{[1:0]\}$ and $\left(\frac{-2}{A}\right) = -1 = \left(\frac{A}{5}\right)$ for $[A]$ in $\{[2:0]\}$. If $A = [2:0]$, then $G = \mathcal{C}_{-20} = \{[A]^0, [A]^1\}$, and $G^2 = \{[A]^0\} = \{[1:0]\}$.

(c) For $\Delta = -47$, the only defined genus symbol is $\left(\frac{A}{47}\right)$, and $\left(\frac{A}{47}\right) = 1$ for all $[A]$ in $G = \mathcal{C}_{-47} = \{[1:0], [2:0], [2:-1], [3:0], [3:-1]\}$. If $A = [2:0]$, then $G = \{[A]^0, [A]^1, [A]^2, [A]^3, [A]^4\} = G^2$. (For example, $[A] = ([A]^3)^2$.)

(d) For $\Delta = -56$, the defined genus symbols are $\left(\frac{2}{A}\right)$ and $\left(\frac{A}{7}\right)$, with $\left(\frac{2}{A}\right) = 1 = \left(\frac{A}{7}\right)$ for $[A]$ in $\{[1:0], [2:0]\}$ and $\left(\frac{2}{A}\right) = -1 = \left(\frac{A}{7}\right)$ for $[A]$ in $\{[3:1], [3:-1]\}$. If $A = [3:1]$, then $G = \mathcal{C}_{-56} = \{[A]^0, [A]^1, [A]^2, [A]^3\}$ and $G^2 = \{[A]^0, [A]^2\}$.

(e) For $\Delta = -84$, the defined genus symbols are $\left(\frac{-1}{A}\right)$, $\left(\frac{A}{3}\right)$, and $\left(\frac{A}{7}\right)$ (presented in that order below). The distinct genera are:

$$+++ : \{[1:0]\}, \quad -+- : \{[2:0]\}, \quad --+ : \{[3:1]\}, \quad +-- : \{[5:2]\}.$$

If $A = [2:0]$ and $B = [3:1]$, then $G = \{[A]^0[B]^0, [A]^1[B]^0, [A]^0[B]^1, [A]^1[B]^1\}$, and $G^2 = \{[A]^0[B]^0\}$.

(f) For $\Delta = -116$, we find that $\left(\frac{-1}{A}\right) = 1 = \left(\frac{A}{29}\right)$ for $[A]$ in $\{[1:0], [5:1], [5:-1]\}$ and $\left(\frac{-1}{A}\right) = -1 = \left(\frac{A}{29}\right)$ for $[A]$ in $\{[2:1], [3:1], [3:-1]\}$. If $A = [3:1]$, then $G = \{[A]^0, [A]^1, [A]^2, [A]^3, [A]^4, [A]^5\}$ and $G^2 = \{[A]^0, [A]^2, [A]^4\}$.

(g) For $\Delta = -119$, we have $\left(\frac{A}{7}\right) = 1 = \left(\frac{A}{17}\right)$ in $\{[1:0], [2:0], [2:-1], [4:1], [4:-2]\}$ and $\left(\frac{A}{7}\right) = -1 = \left(\frac{A}{17}\right)$ in $\{[3:0], [3:-1], [5:0], [5:-1], [6:2]\}$. If $A = [3:0]$, then the principal genus consists of the even powers of $[A]$, and so equals G^2.

(h) For $\Delta = -296$, we have $\left(\frac{-2}{A}\right) = 1 = \left(\frac{A}{37}\right)$ in $\{[1:0], [3:1], [3:-1], [9:4], [9:-4]\}$ and $\left(\frac{-2}{A}\right) = -1 = \left(\frac{A}{37}\right)$ in $\{[2:0], [5:1], [5:-1], [6:2], [6:-2]\}$. If $A = [3:1]$, then the principal genus consists of the even powers of $[A]$.

(i) For $\Delta = -340$, the defined genus symbols are $\left(\frac{-1}{A}\right)$, $\left(\frac{A}{5}\right)$, $\left(\frac{A}{17}\right)$ (presented in that order below). The distinct genera are:

$$+++ : \{[1:0]\}, \quad --+ : \{[2:1]\}, \quad +-- : \{[5:0]\}, \quad -+- : \{[10:5]\}.$$

If $A = [2:1]$ and $B = [5:0]$, then $G = \{[A]^0[B]^0, [A]^1[B]^0, [A]^0[B]^1, [A]^1[B]^1\}$, and $G^2 = \{[A]^0[B]^0\}$.

(j) For $\Delta = -344$, we have $\left(\frac{2}{A}\right) = 1 = \left(\frac{A}{43}\right)$ in $\{[1:0], [6:2], [6:-2], [9:2], [9:-2]\}$ and $\left(\frac{2}{A}\right) = -1 = \left(\frac{A}{43}\right)$ in $\{[2:0], [3:1], [3:-1], [5:2], [5:-2]\}$. If $A = [3:1]$, then the principal genus consists of the even powers of $[A]$.

(k) If $\Delta = -356$, then $\left(\frac{-1}{A}\right) = 1 = \left(\frac{A}{89}\right)$ for $\{[1:0], [2:1], [5:1], [5:-1], [9:1], [9:-1]\}$ and $\left(\frac{-1}{A}\right) = -1 = \left(\frac{A}{89}\right)$ for $\{[3:1], [3:-1], [6:1], [6:-1], [7:3], [7:-3]\}$. The principal genus consists of the even powers of $[A]$, where $A = [3:1]$.

(l) For $\Delta = -420$, the defined genus symbols are $\left(\frac{-1}{A}\right)$, $\left(\frac{A}{3}\right)$, $\left(\frac{A}{5}\right)$, and $\left(\frac{A}{7}\right)$ (presented in that order below). The distinct genera are:

$$++++ : \{[1:0]\}, \quad +--+ : \{[2:1]\}, \quad ---- : \{[3:0]\}, \quad +-+- : \{[5:0]\},$$

$$-++- : \{[6:3]\}, \quad -+-+ : \{[7:0]\}, \quad ++-- : \{[10:5]\}, \quad --++ : \{[11:4]\}.$$

If $A = [2:1]$, $B = [3:0]$, and $C = [5:0]$, then every element of $G = \mathcal{C}_{-420}$ has the form $[A]^i[B]^j[C]^k$ with i, j, and k either 0 or 1 (independently). The square of each such element is $[A]^0[B]^0[C]^0$.

(m) If $\Delta = -191$, then $\phi(x) = x^2 + x + 48$ and u_Δ. From the table

k	$0, -1$	$1, -2$	$2, -3$	$3, -4$
$\phi(k)$	48	50	54	60

we find thirteen reduced ideals of discriminant -191 (listed below), so that $G = \mathcal{C}_{-191}$ has invariant factor type (13). Since 191 is prime, there is only one genus symbol, $\left(\frac{A}{191}\right)$, defined for these ideals, and each ideal class is in the principal genus. Each ideal class is also the square of an element of G. For instance, if $A = [2:0]$, then $[A] = ([A]^7)^2$. Direct calculation shows that the powers of $[A]$ are, in order,

$$[2:0], \quad [4:0], \quad [6:-1], \quad [3:-1], \quad [6:2], \quad [5:-2], \quad [5:1],$$
$$[6:-3], \quad [3:0], \quad [6:0], \quad [4:-1], \quad [2:-1], \quad [1:0].$$

(n) For $\Delta = -231 = -1 \cdot 3 \cdot 7 \cdot 11$, the defined genus symbols of ideals are $\left(\frac{A}{3}\right)$, $\left(\frac{A}{7}\right)$, and $\left(\frac{A}{11}\right)$ (listed in that order below). Here $\phi(x) = x^2 + x + 58$ and $u_\Delta = 8$, and from the table

k	$0, -1$	$1, -2$	$2, -3$	$3, -4$
$\phi(k)$	58	60	64	70

we find twelve reduced ideals of discriminant -231 (listed in the genera below). There are four distinct genera, and $G = \mathcal{C}_{-231}$ has invariant factor type $(6, 2)$. If $A = [2:0]$ and $B = [3:1]$, then every element of G can be written uniquely as $[A]^i[B]^j$ with $0 \le i < 6$ and $0 \le j < 2$. Specifically, the distinct genera are

$$+++ : \{[A]^0, [A]^2, [A]^4\} = \{[1:0], [4:-2], [4:1]\},$$
$$-+- : \{[A], [A]^3, [A]^5\} = \{[2:0], [8:2], [2:-1]\},$$
$$--+ : \{[B], [A]^2[B], [A]^4[B]\} = \{[3:1], [5:1], [5:-2]\},$$
$$+-- : \{[A][B], [A]^3[B], [A]^5[B]\} = \{[6:-2], [7:3], [6:1]\}.$$

Only the elements in the principal genus are squares of elements of G.

(o) For $\Delta = -440$, the defined genus symbols are $\left(\frac{2}{A}\right)$, $\left(\frac{A}{5}\right)$, and $\left(\frac{A}{11}\right)$. Calculating values of $\phi(x) = x^2 + 110$ for $-6 < x \le 6$, we find twelve reduced ideals of discriminant -440, in four genera. The class group $G = \mathcal{C}_{-440}$ has invariant factor type $(6, 2)$, and if $A = [3:1]$ and $B = [2:0]$, then every element of G can be written uniquely as $[A]^i[B]^j$ with $0 \le i < 6$ and $0 \le j < 2$. The distinct genera are

$$+++ : \{[A]^0, [A]^2, [A]^4\} = \{[1:0], [9:4], [9:-4]\},$$
$$--+ : \{[A], [A]^3, [A]^5\} = \{[3:1], [5:0], [3:-1]\},$$
$$+-- : \{[B], [A]^2[B], [A]^4[B]\} = \{[2:0], [7:3], [7:-3]\},$$
$$-+- : \{[A][B], [A]^3[B], [A]^5[B]\} = \{[6:-2], [10:0], [6:2]\}.$$

(p) For $\Delta = -724$, the defined genus symbols are $\left(\frac{-1}{A}\right)$ and $\left(\frac{A}{181}\right)$. From calculation of $\phi(x) = x^2 + 181$ for $-7 \le x \le 7$, we obtain ten reduced forms of discriminant -724, so that $G = \mathcal{C}_{-724}$ has invariant factor type (10). If $A = [7:1]$, the distinct genera are

$$++ : \{[A]^0, [A]^2, [A]^4, [A]^6, [A]^8\} = \{[1:0], [5:2], [13:1], [13:-1], [5:-2]\},$$
$$-- : \{[A], [A]^3, [A]^5, [A]^7, [A]^9\} = \{[7:1], [10:3], [2:1], [10:-3], [7:-1]\}.$$

Section 7.1. Negative Discriminants with Trivial Class Groups.

(1) The prime numbers $p < 150$ that satisfy $p \equiv 1$ or 3 (mod 8) are: 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97, 107, 113, 131, 137, and 139. In addition to 1 and 2, each of these primes appears exactly once in Table 4, as does each $2p < 150$ (that is, 6, 22, 34, 38, 82, 86, 118, 134, and 146), p^k with $k > 1$ (9, 27, 81, and 121), and $2p^k$ with $k > 1$ (18 and 54). The numbers that appear twice in this table are products of two these primes, or prime powers, perhaps multiplied by 2. These are $33 = 3 \cdot 11$, $51 = 3 \cdot 17$, $57 = 3 \cdot 19$, $123 = 3 \cdot 41$, $129 = 3 \cdot 43$, $99 = 3^2 \cdot 11$, $66 = 2 \cdot 3 \cdot 11$, $102 = 2 \cdot 3 \cdot 17$, and $114 = 2 \cdot 3 \cdot 19$.

(2) Let $f(x, y) = x^2 + 2y^2$. If $f(q, r) = m$ and $f(s, t) = n$, then $f(u, v) = mn$ where $u = |qs - 2rt|$ and $v = |qt + rs|$, or $u = |qs + 2rt|$ and $v = |qt - rs|$.
   (a) Since $f(3, 1) = 11$ and $f(1, 3) = 19$, we find that $f(3, 10) = 209 = f(9, 8)$.
   (b) From $f(1, 3) = 19$ and $f(3, 4) = 41$, we find $f(21, 13) = 779 = f(27, 5)$.
   (c) From $f(3, 4) = 41$ and $f(5, 3) = 43$, we find $f(9, 29) = 1763 = f(39, 11)$.
   (d) Using the preceding two solutions of $f(x, y) = 1763 = 41 \cdot 43$, we obtain four solutions of $f(x, y) = 5289 = 3 \cdot 41 \cdot 43$. From $f(1, 1) = 3$ and $f(9, 29) = 1763$, we find $f(49, 38) = 5289 = f(67, 20)$. From $f(1, 1) = 3$ and $f(39, 11) = 1763$, we obtain $f(17, 50) = 5289 = f(61, 28)$.

(3) The prime numbers $p < 150$ with $p \equiv 1$ (mod 3) are: 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, 103, 109, 127, and 139. In addition to 1, 3, 4, and 12, these primes appear once in Table 5, as do $3p < 150$ (that is, 21, 39, 57, 93, 111, and 129), and p^k or $3p^k$ with $k > 1$ (49 and 147). The numbers that appear twice in Table 5 are $4p$ (that is, 28, 52, 76, 124, and 148), or $3 \cdot 4p$ (that is, 84), or products of two distinct primes congruent to 1 modulo p ($91 = 7 \cdot 13$ and $133 = 7 \cdot 19$).

(4) Let $\phi(x) = x^2 + 2x + 4$, the principal polynomial of discriminant $\Delta = -12$. Since $\phi(x) \equiv 0$ (mod 4) has two solutions, 0 and -2, we find that if $a > 3$ has the form of equation (7.1.3), then $\phi(x) \equiv 0 \pmod{a}$ has 2^n solutions if $e = 0$ and 2^{n+1} solutions if $e = 2$. Conjugate pairs of these values correspond to solutions (q, r) and $(q, -r)$ of $x^2 + 3y^2 = a$, or their negatives. If we restrict our attention to primitive solutions in positive integers, then the number of resulting solutions is cut in half.

(5) Let $f(x, y) = x^2 + 3y^2$ and suppose that $f(q, r) = m$ and $f(s, t) = n$. If $u = qs - 3rt$ and $v = qt + rs$, then

$$\begin{aligned} f(u, v) = (qs - 3rt)^2 + 3(qt + rs)^2 &= q^2s^2 - 6qsrt + 9r^2t^2 + 3q^2t^2 + 6qtrs + 3r^2s^2 \\ &= q^2s^2 + 3q^2t^2 + 3r^2s^2 + 9r^2t^2 = (q^2 + 3r^2)(s^2 + 3t^2) = mn. \end{aligned}$$

   (a) Using $f(1, 2) = 13 = f(1, -2)$ and $f(4, 1) = 19$, we can then let $u = 1 \cdot 4 - 3 \cdot 2 \cdot 1 = -2$ and $v = 1 \cdot 1 + 2 \cdot 4 = 9$, or $u = 1 \cdot 4 - 3 \cdot -2 \cdot 1 = 10$ and $v = 1 \cdot 1 - 2 \cdot 4 = -7$, and conclude that $f(2, 9) = 247 = f(10, 7)$.
   (b) From $q = 4$ and $r = 1$, so that $f(q, r) = 19$, and $s = 2$ and $t = 3$, with $f(s, t) = 31$, we find that $(u, v) = (qs - 3rt, qt + rs) = (-1, 14)$ and $(u, v) = (qs + 3rt, qt - rs) = (17, 10)$ are solutions of $f(x, y) = 19 \cdot 31 = 589$.
   (c) From $q = 5$ and $r = 2$, with $f(q, r) = 37$, and $s = 4$ and $t = 3$, with $f(s, t) = 43$, we have that $(u, v) = (qs - 3rt, qt + rs) = (2, 23)$ and $(u, v) = (qs + 3rt, qt - rs) = (38, 7)$ are solutions of $f(x, y) = 37 \cdot 43 = 1591$.

(6) The prime numbers $p < 150$ with $p \equiv 1$, 2, or 4 (mod 7) are: 11, 13, 19, 37, 43, 53, 67, 71, 79, 107, 109, 113, 127, 137, and 149. Along with 1 and 7, these primes appear once each in Table 6, as do p^2 (121), $7p$ (77), 2^e for $e \geq 3$ (8, 16, 32, 64, and 128), and $2^e \cdot 7$ for $e \geq 3$ (56 and 112). The only number that appears twice in Table 6 is $88 = 2^3 \cdot 11$.

(7) Let $\phi(x) = x^2 + 2x + 8$, the principal polynomial of discriminant $\Delta = -28$. For $e \geq 3$, the congruence $\phi(x) \equiv 0 \pmod{2^e}$ has four solutions (by Theorem 3.4). But as noted in the proof of Proposition 7.1.5, one pair of these conjugate values corresponds to a solution of $g(x) \equiv 0 \pmod{2^e}$, where $g(x) = 2x^2 + 2x + 4$, and the other pair corresponds to a solution of $\phi(x) \equiv 0 \pmod{2^e}$. Thus if a is as given in Proposition 7.1.5, then there are 2^{n-1} solutions of $x^2 + 7y^2 = a$ if $e = 0$, and 2^n solutions if $e \geq 3$.

(8) Let $f(x, y) = x^2 + 7y^2$, with $f(q, r) = m$ and $f(s, t) = n$. If $u = qs - 7rt$ and $v = qt + rs$, then

$$f(u, v) = (qs - 7rt)^2 + 7(qt + rs)^2 = q^2s^2 - 14qsrt + 49r^2t^2 + 7q^2t^2 + 14qtrs + 7r^2s^2$$
$$= q^2s^2 + 7q^2t^2 + 7r^2s^2 + 49r^2t^2 = (q^2 + 7r^2)(s^2 + 7t^2) = mn.$$

(a) From $11 = f(q, r)$ with $q = 2$ and $r = 1$, and $23 = f(s, t)$ with $s = 4$ and $t = 1$, we find that $(qs - 7rt, qt + rs) = (1, 6)$ and $(qs + 7rt, qt - rs) = (15, -2)$ are solutions of $f(x, y) = 11 \cdot 23 = 253$.

(b) From $16 = f(q, r)$ with $q = 3$ and $r = 1$, and $23 = f(s, t)$ with $s = 4$ and $t = 1$, then $(qs - 7rt, qt + rs) = (5, 7)$ and $(qs + 7rt, qt - rs) = (19, -1)$ are solutions of $f(x, y) = 16 \cdot 23 = 368$.

(c) From $11 = f(q, r)$ with $q = 2$ and $r = 1$, and $37 = f(s, t)$ with $s = 3$ and $t = 2$, then $(qs - 7rt, qt + rs) = (-8, 7)$ and $(qs + 7rt, qt - rs) = (20, 1)$ are solutions of $f(x, y) = 11 \cdot 37 = 407$.

(d) From $11 = f(q, r)$ with $q = 2$ and $r = 1$, and $71 = f(s, t)$ with $s = 8$ and $t = 1$, then $(qs - 7rt, qt + rs) = (9, 10)$ and $(qs + 7rt, qt - rs) = (23, -6)$ are solutions of $f(x, y) = 11 \cdot 71 = 781$.

(e) We use the two solutions of $f(x, y) = 11 \cdot 23$ from part (a), together with $29 = f(s, t)$ for $s = 1$ and $t = 2$. If $q = 1$ and $r = 6$, then $(qs - 7rt, qt + rs) = (-83, 8)$ and $(qs + 7rt, qt - rs) = (85, -4)$ are solutions of $f(x, y) = 11 \cdot 23 \cdot 29 = 7337$. Likewise, if $q = 15$ and $r = 2$, we obtain $(qs - 7rt, qt + rs) = (-13, 32)$ and $(qs + 7rt, qt - rs) = (43, 28)$ as a second pair of solutions.

(9) Let $\Delta = -67$, so that $\phi(x) = x^2 + x + 17$ and $u_\Delta = \left\lfloor \sqrt{67/3} \right\rfloor = 4$. Since $\phi(0) = 17 = \phi(-1)$ and $\phi(1) = 19 = \phi(-2)$ are not divisible by 2, 3, or 4, then the principal form $\phi = (1 : 0)$, that is, $\phi(x, y) = x^2 + xy + 17y^2$, is the only reduced form of discriminant Δ. A prime p is represented by $\phi(x, y)$ if and only if $\phi(x) \equiv 0 \pmod{p}$ has a solution. But $\phi(q, r) = q^2 + qr + 17 \geq 17$ if $r \neq 0$, so $\phi(x) \equiv 0 \pmod{p}$ can have no solutions for primes $p < 17$. Now $\phi(x) = x^2 + x + 17 < 17^2$ if $0 \leq x \leq 15$. If any of these values were composite, it would have a prime divisor $p < 17$. Our observation above shows that this is impossible. So $\phi(x) = x^2 + x + 17$ must be prime for $0 \leq x \leq 15$.

Section 7.2. Principal Square Domains.

(1) The integers properly represented by $x^2 + 6y^2$ are 1, $6 = 2 \cdot 3$, 7, $10 = 2 \cdot 5$, $15 = 3 \cdot 5$, $22 = 2 \cdot 11$, $25 = 5^2$, 31, $33 = 3 \cdot 11$, $42 = 2 \cdot 3 \cdot 7$, $49 = 7^2$, $55 = 5 \cdot 11$, $58 = 2 \cdot 29$, $70 = 2 \cdot 5 \cdot 7$, 73, 79, $87 = 3 \cdot 29$, 97, 103, $105 = 3 \cdot 5 \cdot 7$, $106 = 2 \cdot 53$, $118 = 2 \cdot 59$, $121 = 11^2$, 127, and $145 = 5 \cdot 29$. In each case, the number of primes p dividing the squarefree part of the integer for which $p \equiv 5$ or $11 \pmod{24}$ (or $p = 2$ or $p = 3$) is even. On the other hand, the integers properly represented by $2x^2 + 3y^2$ are 2, 3, 5, 11, $14 = 2 \cdot 7$, $21 = 3 \cdot 7$, 29, $30 = 2 \cdot 3 \cdot 5$, $35 = 5 \cdot 7$, $50 = 2 \cdot 5^2$, 53, 59, $62 = 2 \cdot 31$, $66 = 2 \cdot 3 \cdot 11$, $75 = 3 \cdot 5^2$, $77 = 7 \cdot 11$, 83, $93 = 3 \cdot 31$, $98 = 2 \cdot 7^2$, 101, 107, $110 = 2 \cdot 5 \cdot 11$, $125 = 5^3$, 131, $146 = 2 \cdot 73$, $147 = 3 \cdot 7^2$, and 149. In each case, the number of such primes dividing the squarefree part of the integer is odd.

(2) Since $1 = 3(3) + 8(-1)$, we find that the solution of $x \equiv a \pmod 8$ and $x \equiv b \pmod 3$ is given by $x \equiv 9a - 8b \pmod{24}$.
   (a) $\left(\frac{2}{p}\right) = 1 = \left(\frac{p}{3}\right)$ if and only if $p \equiv 1$ or $7 \pmod 8$ and $p \equiv 1 \pmod 3$. Substituting 1 or 7 for a and 1 for b in $x \equiv 9a - 8b \pmod{24}$, we find $x \equiv 1$ or $7 \pmod{24}$.
   (b) $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{3}\right)$ if and only if $p \equiv 3$ or $5 \pmod 8$ and $p \equiv 2 \pmod 3$. With $a = 3$ or 5 and $b = 2$ in $x \equiv 9a - 8b \pmod{24}$, we find $x \equiv 5$ or $11 \pmod{24}$.
   (c) $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{p}{3}\right) = -1$ if and only if $p \equiv 1$ or $7 \pmod 8$ and $p \equiv 2 \pmod 3$. Likewise, $\left(\frac{2}{p}\right) = -1$ and $\left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 3$ or $5 \pmod 8$ and $p \equiv 1 \pmod 3$. Solving all possible pairs of congruence using the formula established above, we find that these cases occur if $p \equiv 13$, 17, 19, or $23 \pmod{24}$.

(3) (a) Since $223 \equiv 7 \pmod{24}$, we have that 223 is represented by $x^2 + 6y^2$. By trial-and-error, $223 = 13^2 + 6 \cdot 3^2$.
   (b) Here $227 \equiv 11 \pmod{24}$, so that 227 is represented by $2x^2 + 3y^2$. In fact, we find that $227 = 2 \cdot 10^2 + 3 \cdot 3^2$.
   (c) $341 = 11 \cdot 31$ has one prime divisor congruent to 7 modulo 24 and one prime divisor congruent to 11 modulo 24. So 341 is represented by $2x^2 + 3 \cdot y^2$. We find in fact that $2 \cdot 13^2 + 3 \cdot 1^2 = 341 = 2 \cdot 7^2 + 3 \cdot 9^2$.
   (d) Since $59 \equiv 11 \pmod{24}$, the number of primes p dividing $354 = 2 \cdot 3 \cdot 59$ for which $p = 2$, $p = 3$, or $p \equiv 5$ or $11 \pmod{24}$ is odd. Thus 354 is represented by $2x^2 + 3y^2$, and we find that $354 = 2 \cdot 9^2 + 3 \cdot 8^2$.
   (e) Since $409 \equiv 1 \pmod{24}$, we find that 409 is represented by $x^2 + 6y^2$, specifically $409 = 5^2 + 6 \cdot 8^2$.
   (f) $1015 = 5 \cdot 7 \cdot 11$ has an even number of prime divisors p with $p \equiv 5$ or $11 \pmod{24}$ (and no prime divisors with $p \equiv 13$, 17, 19, or $23 \pmod{24}$). So 1015 is represented by $x^2 + 6y^2$. We find four such representations: $1015 = 31^2 + 6 \cdot 3^2 = 23^2 + 6 \cdot 9^2 = 17^2 + 6 \cdot 11^2 = 1^2 + 6 \cdot 13^2$.

(4) Let $\Delta = -20$, so that $\phi(x) = x^2 + 5$ and $u_\Delta = 2$. With $\phi(0) = 5$ and $\phi(1) = 6$, we find that the reduced ideals of discriminant -20 are $D = [1 : 0]$ and $P = [2 : 1]$. Thus $\mathcal{C}_{-20}$ has invariant factor type (2) and D_{-20} is a principal square domain of type one. An integer m is properly represented by $f = (1 : 0)$ or $g = (2 : 1)$ (that is, $f(x, y) = x^2 + 5y^2$ or $g(x, y) = 2x^2 + 2xy + 3y^2$) if and only if $\phi(x) \equiv 0 \pmod m$ has a solution. For a prime $p \neq 2, 5$, this occurs if and only if $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right) = 1$. We can establish directly that $\left(\frac{-1}{p}\right) = 1 = \left(\frac{p}{5}\right)$ if $p \equiv 1$ or $9 \pmod{20}$ and $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{5}\right)$ if $p \equiv 3$ or $7 \pmod{20}$, while $\left(\frac{-1}{p}\right) \neq \left(\frac{p}{5}\right)$ if $p \equiv 11$, 13, 17, or $19 \pmod{20}$. For $p = 2$ and $p = 5$, we find that $\phi(x) \equiv 0 \pmod p$ has a solution but $\phi(x) \equiv 0 \pmod{p^2}$ does not. The unique ideal of norm 5, $Q = [5 : 0]$, is equivalent to D since $\phi(0) = 5 \cdot 1$, while P is the unique ideal of norm 2. We conclude that a positive integer m is properly represented by f or by g if and only if m is not divisible by 4, by 24, or by a prime $p \equiv 11$, 13, 17, or $19 \pmod{20}$. If this is the case, let a be the squarefree part of m, and let t be the number of prime divisors of a such that $p = 2$ or $p \equiv 3$ or $7 \pmod{20}$. Then m is properly represented by f if t is even, and is properly represented by g if t is odd.

(5) For $\Delta = -40$, we have $\phi(x) = x^2 + 10$ and $u_\Delta = 3$. With $\phi(0) = 10$ and $\phi(\pm 1) = 11$, we find that $D = [1 : 0]$ and $P = [2 : 0]$ are the only reduced ideals of discriminant Δ, and so D_{-40} is a principal square domain of type one. Here P is the unique ideal of norm 2, and $Q = [5 : 0]$, the unique ideal of norm 5, is equivalent to P. We find that a positive integer m is properly represented by $f(x, y) = x^2 + 10y^2$ or by $g(x, y) = 2x^2 + 5y^2$ if and only if m is not divisible by 4, by 25, or by any prime p for which $\left(\frac{-2}{p}\right) \neq \left(\frac{p}{5}\right)$. (These primes are

congruent to 3, 17, 21, 27, 29, 31, 33, or 39 modulo 40.) If m has that property, and a is the squarefree part of m, let t be the number of prime divisors p of a for which $p = 2$, $p = 5$, or $\left(\frac{-2}{p}\right) = -1 = \left(\frac{p}{5}\right)$ (that is, p congruent to 7, 13, 23, or 37 modulo 40). If t is even, then m is properly represented by f. If t is odd, then m is properly represented by g. (Primes p with $\left(\frac{-2}{p}\right) = 1 = \left(\frac{p}{5}\right)$, that is p congruent to 1, 9, 11, or 19 modulo 40, may appear any number of times in the factorization of m.) The integers $m < 100$ properly represented by f are 1, $10 = 2 \cdot 5$, 11, $14 = 2 \cdot 7$, 19, $26 = 2 \cdot 13$, $35 = 5 \cdot 7$, 41, $46 = 2 \cdot 23$, $49 = 7^2$, 59, $65 = 5 \cdot 13$, $74 = 2 \cdot 37$, 89, $91 = 7 \cdot 13$, and $94 = 2 \cdot 47$. Those properly represented by g are 2, 5, 7, 13, $22 = 2 \cdot 11$, 23, 37, $38 = 2 \cdot 19$, 47, 53, $55 = 5 \cdot 11$, $70 = 2 \cdot 5 \cdot 7$, $77 = 7 \cdot 11$, $82 = 2 \cdot 41$, $95 = 5 \cdot 19$, and $98 = 2 \cdot 7^2$.

(6) Using the formula established in the proof of the Chinese Remainder Theorem in Appendix B, we find that the unique solution of the congruences $x \equiv a \pmod 8$, $x \equiv b \pmod 3$, and $x \equiv c \pmod 5$ is given by $x \equiv -15a + 40b - 24c \pmod{120}$.
   (a) Substituting 1 or -1 for a, 1 for b, and 1 or -1 for c, we find that $\left(\frac{2}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{p}{5}\right) = 1$ if p is congruent to 1, 31, 49, or 79 modulo 120.
   (b) Substituting 1 or -1 for a, -1 for b, and 2 or -2 for c, we find that $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{p}{3}\right) = -1 = \left(\frac{p}{5}\right)$ if p is congruent to 17, 23, 47, or 113 modulo 120.
   (c) Substituting 3 or -3 for a, 1 for b, and 2 or -2 for c, we find that $\left(\frac{p}{3}\right) = 1$ and $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{5}\right)$ if p is congruent to 13, 37, 43, or 67 modulo 120.
   (d) Substituting 3 or -3 for a, -1 for b, and 1 or -1 for c, we find that $\left(\frac{p}{5}\right) = 1$ and $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{3}\right)$ if p is congruent to 11, 29, 59, or 101 modulo 120.

(7) Let r, s, and t be defined as in Proposition 7.2.4.
   (a) In the table for $x^2 + 30y^2$, we find that $r = s = t = 0$ for 1, 31, 79, and $121 = 11^2$; $r = s = t = 1$ for $30 = 2 \cdot 3 \cdot 5$, $66 = 2 \cdot 3 \cdot 11$, and $130 = 2 \cdot 5 \cdot 13$; $r = 2$ and $s = t = 0$ for $34 = 2 \cdot 17$, $46 = 2 \cdot 23$, and $94 = 2 \cdot 47$; $s = 2$ and $r = t = 0$ for $39 = 3 \cdot 13$, $111 = 3 \cdot 37$, and $129 = 3 \cdot 43$; and $t = 2$ and $r = s = 0$ for $55 = 5 \cdot 11$ and $145 = 5 \cdot 29$.
   (b) In the table for $2x^2 + 15y^2$, we have $r = 1$ and $s = t = 0$ for 2, 17, 23, 47, $62 = 2 \cdot 31$, 113, and 137; $r = 0$ and $s = t = 1$ for $15 = 3 \cdot 5$, $33 = 3 \cdot 11$, $65 = 5 \cdot 13$, $87 = 3 \cdot 29$, and $143 = 11 \cdot 13$; $r = 1$, $s = 2$, and $t = 0$ for $78 = 2 \cdot 3 \cdot 13$; and $r = 1$, $s = 0$, and $t = 2$ for $110 = 2 \cdot 5 \cdot 11$.
   (c) In the table for $3x^2 + 10y^2$, we have $s = 1$ and $r = t = 0$ for 3, 13, 37, 43, 67, and $93 = 3 \cdot 31$; $s = 0$ and $r = t = 1$ for $10 = 2 \cdot 5$, $22 = 2 \cdot 11$, $58 = 2 \cdot 29$, $85 = 5 \cdot 17$, $115 = 5 \cdot 23$, and $118 = 2 \cdot 59$; and $s = 1$, $r = 2$, and $t = 0$ for $102 = 2 \cdot 3 \cdot 17$ and $138 = 2 \cdot 3 \cdot 23$.
   (d) In the table for $5x^2 + 6y^2$, we have $t = 1$ and $r = s = 0$ for 5, 11, 29, 59, 101, 131, and 149; and $t = 0$ and $r = s = 1$ for $6 = 2 \cdot 3$, $26 = 2 \cdot 13$, $51 = 3 \cdot 17$, $69 = 3 \cdot 23$, $74 = 2 \cdot 37$, $86 = 2 \cdot 43$, $134 = 2 \cdot 67$, and $141 = 3 \cdot 47$.

(8) If $\Delta = -84$, then $\phi(x) = x^2 + 21$ and $u_\Delta = 5$. Since $\phi(0) = 21$, $\phi(\pm 1) = 22$, and $\phi(\pm 2) = 25$, we find that the only reduced ideals of discriminant -84 are $[1 : 0]$, $[2 : 1]$, $[3 : 0]$, and $[5 : 2]$. Each of these ideal classes is its own inverse in $\mathcal{C}_{-84}$ (for example, $[5 : 2]^2 = [25 : 2] \sim [1 : 0]$), and so $\mathcal{C}_{-84}$ has invariant factor type $(2, 2)$, and D_{-84} is a principal square domain of type two. A positive integer m is properly represented by a quadratic form of discriminant $\Delta = -84$ if and only if m is not divisible by 4, by 9, by 49, or by any prime for which $\left(\frac{-21}{p}\right) = -1$. (These primes are congruent to 13, 29, 43, 47, 53, 59, 61, 65, 67, 73, 79, or 83 modulo 84.) If m satisfies this condition, let a be the squarefree part of m, let r be the number of prime divisors p of a with $p = 2$ or $p \equiv 11$, 23, or 71 (mod 8)4, let s be the number of those divisors with $p = 3$, $p = 7$, or $p \equiv 19$, 31, or 55

(mod 8)4, and let t be the number of those divisors with $p \equiv 5$, 17, or 41 (mod 8)4. Then m is properly represented by $x^2 + 21y^2$ if r, s, and t are all even or all odd; m is properly represented by $2x^2 + 2xy + 11y^2$ if r has the opposite parity of both s and t; m is properly represented by $3x^2 + 7y^2$ if s has the opposite parity of both r and t; and m is properly represented by $5x^2 + 4xy + 5y^2$ if t has the opposite parity of both r and s.

(9) In Exercise 6.2.1 and 6.3.1, parts (l), we determined that $\mathcal{C}_{-420}$ has eight elements, each in a distinct genus, and so has invariant factor type $(2, 2, 2)$. Thus D_{-420} is a principal square domain of type three. The reduced quadratic forms of discriminant $\Delta = -420$ are:

$$(1:0) = x^2 + 105y^2, \quad (2:1) = 2x^2 + 2xy + 53y^2,$$

$$(3:0) = 3x^2 + 35y^2, \quad (5:0) = 5x^2 + 21y^2,$$

$$(6:3) = 6x^2 + 6xy + 19y^2, \quad (7:0) = 7x^2 + 15y^2,$$

$$(10:5) = 10x^2 + 10xy + 13y^2, \quad (11:4) = 11x^2 + 8xy + 11y^2.$$

If m is a positive integer not divisible by 4, by 9, by 25, by 49, or by a prime p with $\left(\frac{-105}{p}\right) = -1$, then m is properly represented by one of these forms. Let a be the squarefree part of m, and define integers q through w as follows. Let q be the number of prime divisors p of a so that $p = 2$ or $\left(\frac{-1}{p}\right) = 1 = \left(\frac{p}{7}\right)$ and $\left(\frac{p}{3}\right) = -1 = \left(\frac{p}{5}\right)$, let r be the number of these divisors with $p = 3$ or $\left(\frac{-1}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{p}{5}\right) = \left(\frac{p}{7}\right) = -1$, s the number with $p = 5$ or $\left(\frac{-1}{p}\right) = 1 = \left(\frac{p}{5}\right)$ and $\left(\frac{p}{3}\right) = -1 = \left(\frac{p}{7}\right)$, t the number with $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{7}\right)$ and $\left(\frac{p}{3}\right) = 1 = \left(\frac{p}{5}\right)$, u the number with $\left(\frac{-1}{p}\right) = 1 = \left(\frac{p}{3}\right)$ and $\left(\frac{p}{5}\right) = -1 = \left(\frac{p}{7}\right)$, v the number with $p = 7$ or $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{5}\right)$ and $\left(\frac{p}{3}\right) = 1 = \left(\frac{p}{7}\right)$, and w the number with $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{3}\right)$ and $\left(\frac{p}{5}\right) = 1 = \left(\frac{p}{7}\right)$. Then m is properly represented by $7x^2 + 15y^2$ if and only if $q + t + u + w$ is even, and $r + t + v + w$ and $s + u + v + w$ are both odd. [If $Q = [2:1]$, $R = [3:0]$, and $S = [5:0]$, and A is an ideal of norm a, then we find that in $\mathcal{C}_{-420}$

$$[A] = [Q]^{q+t+u+w} \cdot [R]^{r+t+v+w} \cdot [S]^{s+u+v+w}.$$

Here a and m are properly represented by $7x^2 + 15y^2$ if and only if $[A] = [R] \cdot [S]$, from which our claim follows.]

Section 7.3. Quadratic Domains that are not Principal Square Domains.

(1) The unique solution of $x \equiv a$ (mod 8) and $x \equiv b$ (mod 7) satisfies $x \equiv -7a + 8b$ (mod 56).
   (a) If $\left(\frac{2}{p}\right) = 1 = \left(\frac{p}{7}\right)$, then $p \equiv 1$ or 7 (mod 8) and $p \equiv 1$, 2, or 4 (mod 7). Substituting all possible pairs of these values into the formula above yields six possibilities for p: 1, 9, 15, 23, 25, or 39 modulo 56. (For instance, if $p \equiv 7$ (mod 8) and $p \equiv 2$ (mod 7), then $p \equiv -7(7) + 8(2) \equiv -33 \equiv 23$ (mod 56).)
   (b) If $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{7}\right)$, then $p \equiv 3$ or 5 (mod 8) and $p \equiv 3$, 5, or 6 (mod 7). Again by substitution of all possible pairs into our formula, we obtain six possibilities for p: 3, 5, 13, 19, 27, or 45 modulo 56.

(2) As noted above, $p = 3$, 5, 13, and 19 all satisfy $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{7}\right)$. The possible products of two of these primes are 15, 39, 57, 65, 95, and 247. Table 9 verifies that the first five of these are properly represented by both $x^2 + 14y^2$ and $2x^2 + 7y^2$. Direct calculation shows that $247 = 11^2 + 14 \cdot 3^2$ and $247 = 2 \cdot 6^2 + 7 \cdot 5^2$. Table 9 likewise confirms that $3^2 = 9$ and $5^2 = 25$ are properly represented by $2x^2 + 7y^2$ but not by $x^2 + 14y^2$. We find that $13^2 = 169 = 2 \cdot 9^2 + 7 \cdot 1^2$ and $19^2 = 361 = 2 \cdot 3^2 + 7 \cdot 7^2$, and can rule out proper representations of these squares by $x^2 + 14y^2$ using trial-and-error.

(3) (a) If $\Delta = -68$, then $\phi(x) = x^2 + 17$ and $u_\Delta = 4$. From $\phi(0) = 17$, $\phi(\pm 1) = 18$, and $\phi(\pm 2) = 21$, we determine that $[1:0]$, $[2:1]$, $[3:1]$, and $[3:-1]$ are the reduced ideals of discriminant -68. We find that if $A = [3:1]$, then $A^2 = [9:1] \sim [2:1]$, and then $A^3 \sim [6:1] \sim [3:-1]$, and $A^4 \sim [1:0]$. Thus $\mathcal{C}_{-68}$ has invariant factor type (4). The principal genus consists of $[1:0]$ and $[2:1]$.

(b) If p is an odd prime number for which $\left(\frac{-1}{p}\right) = 1 = \left(\frac{p}{17}\right)$, then $\phi(x) \equiv 0 \pmod{p}$ has two solutions, say k and $-k$, and the prime ideals $P = [p:k]$ and $\overline{P} = [p:-k]$ are in the principal genus of $\mathcal{C}_{-68}$, since $\left(\frac{-1}{P}\right) = 1 = \left(\frac{P}{17}\right)$. So we must have $P \sim [1:0]$ (and then $\overline{P} \sim [1:0]$), or $P \sim [2:1]$ (and $\overline{P} \sim [2:1]$), but not both. If $P \sim [1:0]$, then p is properly represented by $x^2 + 17y^2$. If $P \sim [2:1]$, then $P \cdot [2:1]$ is an ideal of norm $2p$ that is equivalent to $[1:0]$, then $2p$ is properly represented by $x^2 + 17y^2$.

(c) If $p > 3$ is a prime number for which $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{17}\right)$, then $\phi(x) \equiv 0 \pmod{p}$ again has two solutions, and so there are two conjugate ideals of norm p in D_{-68}, say P and $\overline{P}$. Here $\left(\frac{-1}{P}\right) = -1 = \left(\frac{P}{17}\right)$, and so P is not in the principal genus. We can assume that $P \sim [3:1]$ and $\overline{P} \sim [3:-1]$ by relabeling P if necessary. Now $P \cdot [3:-1]$ is an ideal of norm $3p$ that is equivalent to $[1:0]$, so that $3p$ is properly represented by $x^2 + 17y^2$.

(4) (a) If $\Delta = -152$, then $\phi(x) = x^2 + 38$ and $u_\Delta = 7$. There are six reduced ideals of discriminant -152: $[1:0]$, $[2:0]$, $[3:1]$, $[3:-1]$, $[6:2]$, $[6:-2]$, and so $\mathcal{C}_{-152}$ must have invariant factor type (6). If $A = [3:1]$, then $A^2 = [9:4] \sim [6:2]$, $A^3 \sim [2:0]$, $A^4 \sim [6:-2]$, $A^5 \sim [18:4] \sim [3:-1]$, and $A^6 \sim [1:0]$. The principal genus consists of $[1:0]$, $[6:2]$, and $[6:-2]$.

(b) If $p > 3$ is a prime number for which $\left(\frac{2}{p}\right) = 1 = \left(\frac{p}{19}\right)$, then $\phi(x) \equiv 0 \pmod{p}$ has two solutions, and so there are two conjugate ideals, P and $\overline{P}$, of norm p in D_{-152}. Here $\left(\frac{2}{P}\right) = 1 = \left(\frac{P}{19}\right)$, so that P is in the principal genus of $\mathcal{C}_{-152}$. If $P \sim [1:0]$ (so that $\overline{P} \sim [1:0]$), then p is properly represented by $x^2 + 38y^2$. Otherwise, we can assume, by relabeling P and $\overline{P}$ if necessary, that $P \sim [6:2]$ and $\overline{P} \sim [6:-2]$. In that case, $P \cdot [6:-2]$ is an ideal of norm $6p$ that is equivalent to $[1:0]$, so that $6p$ is properly represented by $x^2 + 38y^2$.

(c) If $p > 3$ is a prime number for which $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{19}\right)$, then $\phi(x) \equiv 0 \pmod{p}$ again has two solutions, and there are conjugate ideals P and $\overline{P}$ in D_{-152}. Now $\left(\frac{2}{P}\right) = -1 = \left(\frac{P}{19}\right)$, so that P is not in the principal genus of $\mathcal{C}_{-152}$. If $P \sim [2:0]$, then $P \cdot [2:0]$ is an ideal of norm $2p$ that is equivalent to $[1:0]$. In that case, $x^2 + 38y^2$ properly represents $2p$. If not, we can assume that $P \sim [3:1]$, and then $P \cdot [3:-1]$ is an ideal of norm $3p$ equivalent to $[1:0]$. In that case, $x^2 + 38y^2$ properly represents $3p$.

Section 7.4. Construction of Representations.

(1) (a) If $\Delta = -52$, with $\phi(x) = x^2 + 13$, then $g = (187:19) \leftrightarrow_{10} (2:1) = f$, with the latter form reduced. We conclude that if $f(x,y) = 2x^2 + 2xy + 7y^2$, then $f(10,-1) = 187$.

(b) Again with $\Delta = -52$, we see that $g = (187:36) \leftrightarrow_5 (7:-1) \leftrightarrow_0 [2:1] = f$, so $f(x,y) = 2x^2 + 2xy + 7y^2$ is the reduced form equivalent to g. Here with $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 5 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ -5 & -1 \end{bmatrix}$, it follows that $f(-1,-5) = 187$.

(c) Let $\Delta = -56$, so that $\phi(x) = x^2 + 14$. Here $g = (171:29) \leftrightarrow_6 (5:1) \leftrightarrow_0 (3:-1) = f$, with $f(x,y) = 3x^2 - 2xy + 5y^2$ reduced. Since $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 6 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ -6 & -1 \end{bmatrix}$, it follows that $f(-1,-6) = 171$.

(d) Again with $\Delta = -56$, we find that $g = (171 : 47) \leftrightarrow_4 (13 : 5) \leftrightarrow_2 (3 : 1)$, with $f(x, y) = 3x^2 + 2xy + 5y^2$ reduced. Here $\begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 4 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 7 & 2 \\ -4 & -1 \end{bmatrix}$, so that $f(7, -4) = 171$.

(e) Let $\Delta = -84$, so that $\phi(x) = x^2 + 21$. Then $g = (185 : 33) \leftrightarrow_6 (6 : 3) \leftrightarrow_2 (5 : 2) = f$, with $f(x, y) = 5x^2 + 4xy + 5y^2$ reduced. Since $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 6 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ -6 & -1 \end{bmatrix}$, it follows that $f(5, -6) = 185$.

(f) Again with $\Delta = -84$, we have $g = (185 : 78) \leftrightarrow_2 (33 : -12) \leftrightarrow_{-2} (5 : 2) = f$, with $f(x, y) = 5x^2 + 4xy + 5y^2$ reduced. Here $\begin{bmatrix} -2 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -5 & -2 \\ -2 & -1 \end{bmatrix}$, so that $f(-5, -2) = 185$.

(2) (a) When $\Delta = -52$, then $M = [187 : 19] \leftrightarrow [2 : 1] = A$, a reduced ideal. Let $f = (2 : 1) = 2x^2 + 2xy + 7y^2$. Here $2M = (19 + z)A$, where $z = \sqrt{-13}$, and with $w = s + tz = 19 + z$, $a = 2$, and $k = 1$, we find that $q = \frac{s+tk}{a} = \frac{19+1(1)}{2} = 10$ and $r = -t = -1$ is a pair of integers for which $f(q, r) = 187$.

(b) When $\Delta = -52$, then $M = [187 : 36] \leftrightarrow [7 : -1] \leftrightarrow [2 : 1] = A$, again with $f = (2 : 1) = 2x^2 + 2xy + 7y^2$. In this case,

$$7 \cdot 2M = (36 + z)(-1 + z) = (-36 + 35z + z^2)A = (-49 + 35z)A,$$

so that $2M = (-7 + 5z)A$. With $s + tz = -7 + 5z$, $a = 2$, and $k = 1$, we find that $q = \frac{s+tk}{a} = \frac{-7+5(1)}{2} = -1$ and $r = -t = -5$ are integers for which $f(q, r) = 187$.

(c) Let $\Delta = -56$, so that $z = \sqrt{-14}$. Here we find that $M = [171 : 29] \leftrightarrow [5 : 1] \leftrightarrow [3 : -1] = A$, so that $f = (3 : -1) = 3x^2 - 2xy + 5y^2$. Now $5 \cdot 3M = (29 + z)(1 + z)A = (29 + 30z + z^2)A = (15 + 30z)A$, and so $3M = (3 + 6z)A$. With $s + tz = 3 + 6z$, $a = 3$, and $k = -1$, we have that $q = \frac{s+tk}{a} = \frac{3+6(-1)}{3} = -1$ and $r = -t = -6$ are integers for which $f(q, r) = 171$.

(d) Again with $\Delta = -56$, we have $M = [171 : 47] \leftrightarrow [13 : 5] \leftrightarrow [3 : 1] = A$, so that $f = (3 : 1) = 3x^2 + 2xy + 5y^2$. Now $13 \cdot 3M = (47 + z)(5 + z)A$, which simplifies to $3M = (17 + 4z)A$. With $s + tz = 17 + 4z$, $a = 3$, and $k = 1$, we find that $q = \frac{s+tk}{a} = \frac{17+4(1)}{3} = 7$ and $r = -t = -4$ are integers for which $f(q, r) = 171$.

(e) Let $\Delta = -84$, so that $z = \sqrt{-21}$. Here $M = [185 : 33] \leftrightarrow [6 : 3] \leftrightarrow [5 : 2] = A$, and so $f = [5 : 2] = 5x^2 + 4xy + 5y^2$. Now $6 \cdot 5M = (33 + z)(3 + z)A$, which simplifies to $5M = (13 + 6z)A$. With $s + tz = 13 + 6z$, $a = 5$, and $k = 2$, then $q = \frac{s+tk}{a} = \frac{13+6(2)}{5} = 5$ and $r = -t = -6$ are integers for which $f(q, r) = 185$.

(f) Again with $\Delta = -84$, we have $M = [185 : 78] \leftrightarrow [6 : 3] \leftrightarrow [5 : 2] = A$, and $f = [5 : 2] = 5x^2 + 4xy + 5y^2$. Here $33 \cdot 5M = (78 + z)(-12 + z)A$, which simplifies to $5M = (-29 + 2z)A$. With $s + tz = -29 + 2z$, $a = 5$, and $k = 2$, we find that $q + \frac{s+tk}{a} = \frac{-29+2(2)}{5} = -5$ and $r = -t = -2$ are integers for which $f(q, r) = 185$.

Section 8.1. Constructing Class Groups of Subdomains.

(1) (a) For $\Delta = -20$, we find that $G = \mathcal{F}_\Delta$ consists of $(1 : 0)$ and $(2 : 1)$, which is equivalent to $(3 : -1)$. For $p = 2$, we can use $(1 : 0)$ and $(3 : -2)$ as representatives for G in $G_2 = \mathcal{F}_{p^2\Delta}$; for $p = 3$, we can use $(1 : 0)$ and $(2 : 3)$ as these representatives; for $p = 5$, we can use $(1 : 0)$ and $(2 : 5)$.

(b) When $\Delta = -40$, then $(1 : 0)$ and $(2 : 0) \sim (5 : 0)$ are the elements of $G = \mathcal{F}_\Delta$. We can use $(1 : 0)$ and $(5 : 0)$ as representatives for G in $\mathcal{F}_{p^2\Delta}$ when $p = 2$; we can use

$(1:0)$ and $(2:0)$ as these representatives when $p=3$; we can use $(1:0)$ and $(2:0)$ when $p=5$.

(c) For $\Delta=-56$, we find that $G=\mathcal{F}_\Delta$ consists of $(1:0)$, $(2:0)$, $(3:1)$, and $(3:-1)$. When $p=2$, then $(1:0)$, $(7:0)$, $(3:1)$, and $(3:-1)$ are representatives for G in $\mathcal{F}_{p^2\Delta}$ (since $(2:0)\sim(7:0)$); when $p=3$, we can use $(1:0)$, $(2:0)$, $(5:-3)$, and $(5:3)$ as these representatives (here using the fact that $(3:1)\sim(5:-1)$ and $(3:-1)\sim(5:1)$); when $p=5$, then $(1:0)$, $(2:0)$, $(3:5)$, and $(3:-5)$ are these representatives.

(d) For $\Delta=-84$, we have that $G=\mathcal{F}_\Delta$ consists of $(1:0)$, $(2:1)$, $(3:0)$, and $(5:2)$. Since $(2:1)\sim(11:-1)$, we then find that $(1:0)$, $(11:-2)$, $(3:0)$, and $(5:4)$ are representatives for G in $\mathcal{F}_{p^2\Delta}$ when $p=2$. With $(3:0)\sim(7:0)$, we likewise find that $(1:0)$, $(2:3)$, $(7:0)$, and $(5:6)$ are representatives for G in $\mathcal{F}_{p^2\Delta}$ when $p=3$. Finally, since $(5:2)\sim(5:-3)\sim(6:3)$, we have that $(1:0)$, $(2:5)$, $(3:0)$, and $(6:15)$ are representatives for G in $\mathcal{F}_{p^2\Delta}$ when $p=5$.

(e) For $\Delta=-116$, class representatives for $G=\mathcal{F}_\Delta$ are $(1:0)$, $(2:1)$, $(3:1)$, $(3:-1)$, $(5:1)$, and $(5:-1)$. For $p=2$, with $(2:1)\sim(15:1)$, we have that $(1:0)$, $(15:2)$, $(3:2)$, $(3:-2)$, $(5:2)$, and $(5:-2)$ are representatives for G in $\mathcal{F}_{p^2\Delta}$. For $p=3$, with $(3:\pm1)\sim(10:\mp1)$, we can use $(1:0)$, $(2:3)$, $(10:-3)$, $(10:3)$, $(5:3)$, and $(5:-3)$ as these representatives. For $p=5$, with $(5:\pm1)\sim(6:\mp1)$, we find these representatives as $(1:0)$, $(2:5)$, $(3:5)$, $(3:-5)$, $(6:-5)$, and $(6:5)$.

(f) For $\Delta=-119$, we find that $G=\mathcal{F}_\Delta$ has ten elements, with class representatives

$$(1:0),(2:0),(2:-1),(3:0),(3:-1),(4:1),(4:-2),(5:0),(5:-1),(6:2).$$

Using various equivalences, we find the following representatives for G in $\mathcal{F}_{p^2\Delta}$. When $p=2$,

$$(1:0),(15:-2),(15:0),(3:0),(3:-2),(9:4),(9:-6),(5:0),(5:-2),(7:6);$$

when $p=3$,

$$(1:0),(2:0),(2:-3),(10:-3),(10:0),(4:3),(4:-6),(5:0),(5:-3),(7:9);$$

and when $p=5$,

$$(1:0),(2:0),(2:-5),(3:0),(3:-5),(4:5),(4:-10),(6:-5),(6:0),(6:10).$$

(2) Let $\Delta=-3$. Then $p-\left(\frac{\Delta}{p}\right)=2-(-1)=3$ when $p=2$; $p-\left(\frac{\Delta}{p}\right)=3-0=3$ when $p=3$; $p-\left(\frac{\Delta}{p}\right)=p-1$ when $p>3$ is congruent to 1 modulo 3; and $p-\left(\frac{\Delta}{p}\right)=p-(-1)=p+1$ when $p>3$ is congruent to 2 modulo 3. In each case, $p-\left(\frac{\Delta}{p}\right)$ is divisible by 3, and so $|K_p|=\frac{1}{3}\left(p-\left(\frac{\Delta}{p}\right)\right)$ is an integer when $\Delta=-3$. Now let $\Delta=-4$. Then $p-\left(\frac{\Delta}{p}\right)=2-0=2$ when $p=2$; $p-\left(\frac{\Delta}{p}\right)=p-1$ if $p\equiv1\pmod 4$; and $p-\left(\frac{\Delta}{p}\right)=p-(-1)=p+1$ if $p\equiv3\pmod 4$. In each case, $p-\left(\frac{\Delta}{p}\right)$ is even, and so $|K_p|=\frac{1}{2}\left(p-\left(\frac{\Delta}{p}\right)\right)$ is an integer when $\Delta=-4$.

(3) For each discriminant Δ, we list the elements of K_p for $p=2$, $p=3$, and $p=5$, and the reduced form of discriminant $p^2\Delta$ to which each is equivalent, showing that the classes of these forms are distinct in $\mathcal{C}_{p^2\Delta}$.

(a) For $\Delta=-20$, then K_2 contains $(1:0)$ and $(4:0)$, both reduced; K_3 contains $(1:0)$ and $(9:0)\sim(5:0)$; and K_5 contains $(1:0)$, $(25:5)\sim(6:1)$, $(25:-5)\sim(6:-1)$, $(25:10)\sim(9:-1)$, and $(25:-10)\sim(9:1)$.

(b) For $\Delta = -40$, K_2 contains $(1:0)$ and $(4:2)$; K_3 contains $(1:0)$, $(9:0)$, $(9:3)$, and $(9:-3)$; and K_5 contains $(1:0)$, $(25:5) \sim (11:-5)$, $(25:-5) \sim (11:5)$, $(25:10) \sim (14:4)$, and $(25:-10) \sim (14:-4)$.

(c) For $\Delta = -56$, K_2 contains $(1:0)$ and $(4:2)$; K_3 contains $(1:0)$ and $(9:0)$; and K_5 contains $(1:0)$, $(25:0) \sim (14:0)$, $(25:10) \sim (18:8)$, and $(25:-10) \sim (18:-8)$.

(d) For $\Delta = -84$, K_2 contains $(1:0)$ and $(4:0)$; K_3 contains $(1:0)$, $(9:3)$, and $(9:-3)$; and K_5 contains $(1:0)$, $(25:0) \sim (21:0)$, $(25:5) \sim (22:-5)$, and $(25:-5) \sim (22:5)$.

(e) For $\Delta = -116$, K_2 contains $(1:0)$ and $(4:0)$; K_3 contains $(1:0)$ and $(9:0)$; and K_5 contains $(1:0)$, $(25:0)$, $(25:10)$, and $(25:-10)$. All of these forms are reduced.

(f) For $\Delta = -119$, K_2 contains only $(1:0) \sim (1:-1)$; K_3 contains $(1:0) \sim (1:-1)$ and $(9:3)$; and K_5 contains $(1:0) \sim (1:-2)$, $(25:5)$, $(25:10)$, and $(25:-10)$.

(4) If $\Delta = -3$, so that $\phi(x) = x^2 + x + 1$, then $\phi(x) \equiv 0 \pmod{11}$ has no solutions, and thus K_{11} could have as many as twelve distinct elements, of the form $(1:0)$ or $(121:11k)$ with $-5 \le k \le 5$. But with $\phi_{11}(x) = x^2 + 11x + 121$, we find that

$$(121:0) \sim (121:-11) \sim (1:0) \sim (1:-5),$$

a reduced form of discriminant $\Delta_{11} = -363$. Likewise

$$(121:11) \sim (121:-22) \sim (121:-55) \sim (3:-4),$$

$$(121:22) \sim (121:-44) \sim (121:44) \sim (7:-5),$$

and

$$(121:-33) \sim (121:33) \sim (121:-55) \sim (7:-6).$$

So in fact there are only four distinct elements in K_{11}.

(5) The principal polynomial of discriminant $\Delta_p = -47 \cdot 5^2 = -1175$ is $\phi(x)x^2 + 5x + 300$. We use this polynomial below to find the reduced form equivalent to each representative of $\mathcal{F}_{-1175}$ listed. For example, we have that $(75:30) \sim (18:-35) = (18:1)$ since $\phi(30) = 1350 = 75 \cdot 18$. But then with $\phi(1) = 306 = 18 \cdot 17$, then $(18:1) \sim (17:-6)$, a reduced form. We list the reduced form representatives $(a:k)$ of $\mathcal{F}_{-1175}$ in increasing order of a, to help verify that all such forms are distinct.

$$\begin{array}{lll}
(1:0) \sim (1:-2), & (2:0) \sim (2:-2), & (2:-5) \sim (2:-3), \\
(3:0) \sim (3:-3), & (3:-5) \sim (3:-2), & (75:0) \sim (4:-1), \\
(75:-5) \sim (4:-4), & (50:0) \sim (6:-5), & (50:-5) \sim (6:0), \\
(75:-15) \sim (6:-2), & (75:10) \sim (6:-3), & (50:5) \sim (7:-3), \\
(50:-10) \sim (7:-2), & (75:-20) \sim (8:-1), & (75:15) \sim (8:-4), \\
(50:10) \sim (9:-6), & (50:-15) \sim (9:1), & (25:-5) \sim (12:0), \\
(25:0) \sim (12:-5), & (50:-20) \sim (12:3), & (50:15) \sim (12:-8), \\
(75:25) \sim (14:-2), & (75:-30) \sim (14:-3), & (25:5) \sim (14:4), \\
(25:-10) \sim (14:-9), & (50:-25) \sim (16:4), & (50:20) \sim (16:-9), \\
(75:30) \sim (17:-6), & (75:-35) \sim (17:1), & (25:10) \sim (18:3).
\end{array}$$

(6) In parts (a)–(i), we use calculations of S_p and K_p from Exercises 1 and 3 in this section. In each array, the first row lists the elements of S_p and the first column lists the elements of K_p, with products of those elements as the remaining entries of the table. We then note the reduced form of discriminant $p^2\Delta$ to which each one is equivalent. In parts (j)–(o), the group $\mathcal{C}_\Delta$ is trivial, so that S_p contains only $(1:0)$ and the class group of discriminant $p^2\Delta$ is identical to K_p.

(a) $\Delta = -20$ and $p = 2$.

$$\begin{array}{cc} (1:0) & (3:-2) \\ (4:0) & (12:4) \end{array}$$

Here $(1:0)$ and $(4:0)$ are reduced, while $(3:-2) \sim (3:1)$ and $(12:4) \sim (3:-1)$. One can verify that these are the only (primitive) reduced forms of discriminant -80.

(b) $\Delta = -20$ and $p = 3$.

$$\begin{array}{cc} (1:0) & (2:3) \\ (9:0) & (18:9) \end{array}$$

with $(2:3) \sim (2:1)$, $(9:0) \sim (5:0)$, and $(18:9) \sim (7:2)$.

(c) $\Delta = -20$ and $p = 5$.

$$\begin{array}{cc} (1:0) & (2:5) \\ (25:5) & (50:5) \\ (25:-5) & (50:-5) \\ (25:10) & (50:-15) \\ (25:-10) & (50:15) \end{array}$$

with $(2:5) \sim (2:1)$, $(25:5) \sim (6:1)$, $(25:-5) \sim (6:-1)$, $(25:10) \sim (9:-1)$, $(25:-10) \sim (9:1)$, $(50:5) \sim (3:1)$, $(50:-5) \sim (3:-1)$, $(50:-15) \sim (7:1)$, and $(50:15) \sim (7:-1)$ as reduced form representatives.

(d) $\Delta = -40$ and $p = 2$.

$$\begin{array}{cc} (1:0) & (5:0) \\ (4:2) & (20:10) \end{array}$$

with $(20:10) \sim (7:3)$ and all other forms reduced.

(e) $\Delta = -40$ and $p = 3$.

$$\begin{array}{cc} (1:0) & (2:0) \\ (9:0) & (18:0) \\ (9:3) & (18:-6) \\ (9:-3) & (18:6) \end{array}$$

with $(18:0) \sim (5:0)$, $(18:-6) \sim (7:-1)$, $(18:6) \sim (7:1)$, and all other forms reduced.

(f) $\Delta = -56$ and $p = 2$.

$$\begin{array}{cccc} (1:0) & (7:0) & (3:2) & (3:-2) \\ (4:2) & (28:14) & (12:2) & (12:-2) \end{array}$$

with $(3:2) \sim (3:-1)$, $(3:-2) \sim (3:1)$, $(28:14) \sim (8:4)$, $(12:2) \sim (5:-2)$, and $(12:-2) \sim (5:2)$.

(g) $\Delta = -56$ and $p = 3$.

$$\begin{array}{cccc} (1:0) & (2:0) & (5:-3) & (5:3) \\ (9:0) & (18:0) & (45:-18) & (45:18) \end{array}$$

with $(5:-3) \sim (5:2)$, $(5:3) \sim (5:-2)$, $(18:0) \sim (7:0)$, $(45:-18) \sim (10:-2)$, and $(45:18) \sim (10:2)$.

(h) $\Delta = -84$ and $p = 2$.

$$\begin{array}{cccc} (1:0) & (11:-2) & (3:0) & (5:4) \\ (4:0) & (44:20) & (12:0) & (20:4) \end{array}$$

with $(11:-2) \sim (8:2)$, $(5:4) \sim (5:-1)$, $(44:20) \sim (8:-2)$, $(12:0) \sim (7:0)$, and $(20:4) \sim (5:1)$.

(i) $\Delta = -116$ and $p = 2$.

$(1:0)$	$(15:2)$	$(3:2)$	$(3:-2)$	$(5:2)$	$(5:-2)$
$(4:0)$	$(60:-28)$	$(12:-4)$	$(12:4)$	$(20:-8)$	$(20:8)$

with $(15:2) \sim (8:-2)$, $(3:2) \sim (3:-1)$, $(3:-2) \sim (3:1)$, $(60:-28) \sim (8:2)$, $(12:-4) \sim (11:4)$, $(12:4) \sim (11:-4)$, $(20:-8) \sim (9:-1)$, and $(20:8) \sim (9:1)$.

(j) For $\Delta = -3$ and $p = 7$, we find that $(49:0) \sim (49:-7) \sim (1:0) \sim (1:-3)$ and $(49:7) \sim (49:-14) \sim (49:21) \sim (3:-2)$, and so $\mathcal{F}_{-147} = \{(1:-3), (3:-2)\}$.

(k) $\mathcal{F}_{-363} = \{(1:-5), (3:-4), (7:-5), (7:-6)\}$.

(l) $\mathcal{F}_{-507} = \{(1:-6), (3:-5), (7:-4), (7:-9)\}$.

(m) $\mathcal{F}_{-196} = \{(1:0), (2:1), (5:1), (5:-1)\}$.

(n) $\mathcal{F}_{-484} = \{(1:0), (2:1), (5:2), (5:-2), (10:3), (10:-3)\}$.

(o) $\mathcal{F}_{-676} = \{(1:0), (2:1), (5:1), (5:-1), (10:1), (10:-1)\}$.

(7) Let $\Delta = \Delta(-1, 12) = -576$, so that $\phi(x) = x^2 + 144$ and $u_\Delta = 13$. From the table

k	0	±1	±2	±3	±4	±5	±6
$\phi(k)$	144	145	148	153	160	169	180

we compile the following list of reduced forms of discriminant Δ. (We group these forms by index, which is a divisor of 12.)

1	$(1:0)$	$(4:2)$	$(5:1)$	$(5:-1)$	$(9:0)$	$(9:3)$	$(9:-3)$	$(13:5)$
2	$(2:0)$	$(8:0)$	$(10:4)$	$(10:-4)$				
3	$(3:0)$	$(12:6)$						
4	$(4:0)$							
6	$(6:0)$							
12	$(12:0)$							

The form class group $\mathcal{F}_{-576}$ has eight elements.

Section 8.2. Projection Homomorphisms.

(1) For each Δ and p, we list the reduced quadratic forms of discriminant Δ and the (primitive) reduced forms of discriminant $p^2\Delta$, and describe the projection homomorphism ψ from $\mathcal{F}_{p^2\Delta}$ to $\mathcal{F}_\Delta$.

(a) The only reduced form of discriminant $\Delta = -4$ is $(1:0)$; if $p = 7$, the primitive reduced forms of discriminant $p^2\Delta = -196$ are $(1:0)$, $(2:1)$, $(5:1)$, and $(5:-1)$. To apply the projection homomorphism, we note that $(2:1) \sim (2:7)$, $(5:1) \sim (5:-14)$, and $(5:-1) \sim (5:14)$. Then $\psi((1:0)) = (1:0)$, $\psi((2:7)) = (2:1)$, $\psi((5:-14)) = (5:-2)$, and $\psi((5:14)) = (5:2)$. Each of the resulting forms is equivalent to $(1:0)$ in $\mathcal{F}_\Delta$.

(b) The primitive reduced forms of discriminant $13^2 \cdot -4 = -676$ are $(1:0)$, $(2:1) \sim (2:13)$, $(5:1) \sim (5:26)$, $(5:-1) \sim (5:-26)$, $(10:1) \sim (10:-39)$, and $(10:-1) \sim (10:39)$. These are sent by the projection homomorphism to $(1:0)$, $(2:1)$, $(5:2)$, $(5:-2)$, $(10:-3)$, and $(10:3)$ respectively. Each of those forms is equivalent to $(1:0)$ in $\mathcal{F}_{-4}$.

(c) The only reduced form of discriminant $\Delta = -7$ is $(1:0)$; when $p = 3$, the primitive reduced forms of discriminant $p^2\Delta = -63$ are $(1:-1) \sim (1:0)$, $(2:-1) \sim (2:-3)$, $(2:-2) \sim (2:0)$, and $(4:-1) \sim (4:3)$, sent by ψ to $(1:0)$, $(2:-1)$, $(2:0)$, and $(4:1)$ respectively. Each of these forms is equivalent to $(1:0)$ in $\mathcal{F}_{-7}$.

(d) The primitive reduced forms of discriminant $5^2 \cdot -7 = -175$ are $(1:-2) \sim (1:0)$, $(2:-2) \sim (2:0)$, $(2:-3) \sim (2:-5)$, $(4:-2) \sim (4:-10)$, $(4:-3) \sim (4:5)$, and

$(7:1) \sim (7:15)$, sent by ψ to $(1:0)$, $(2:0)$, $(2:-1)$, $(4:-2)$, $(4:1)$, and $(7:3)$ respectively, each equivalent to $(1:0)$ in $\mathcal{F}_{-7}$.

(e) The primitive reduced forms of discriminant $11^2 \cdot -7 = -847$ are $(1:-5) \sim (1:0)$, $(2:-5) \sim (2:-11)$, $(2:-6) \sim (2:0)$, $(4:-5) \sim (4:11)$, $(4:-6) \sim (4:-22)$, $(7:-2) \sim (7:33)$, $(8:-2) \sim (8:22)$, $(8:-9) \sim (8:-33)$, $(14:-2) \sim (14:-44)$, and $(14:-9) \sim (14:33)$. These elements are sent by ψ to $(1:0)$, $(2:-1)$, $(2:0)$, $(4:1)$, $(4:-2)$, $(7:3)$, $(8:2)$, $(8:-3)$, $(14:-4)$, and $(14:3)$ respectively, each equivalent to $(1:0)$ in $\mathcal{F}_{-7}$.

(f) There are two reduced forms of discriminant $\Delta = -15$, $(1:0)$ and $(2:0)$. When $p = 3$, we find the following reduced forms of discriminant $p^2\Delta = -135$: $(1:-1) \sim (1:0)$, $(2:-1) \sim (2:-3)$, $(2:-2) \sim (2:0)$, $(4:0)$, $(4:-3)$, and $(5:1) \sim (5:6)$. These are sent by ψ to $(1:0)$, $(2:-1)$, $(2:0)$, $(4:0)$, $(4:-1)$, and $(5:6)$. We then find that $(4:0) \sim (4:-1) \sim (1:0)$, while $(5:2) \sim (2:-1) \sim (2:0)$ in $\mathcal{F}_{-15}$.

(g) There are ten primitive reduced forms of discriminant $5^2 \cdot -15 = -375$. We list these forms below, along with equivalent forms to which ψ can be applied, and then the resulting forms in $\mathcal{F}_{-15}$. Those in the first column are equivalent to $(1:0)$, and those in the second column are equivalent to $(2:0)$.

$(1:-2) \sim (1:0) \to (1:0)$	$(2:-2) \sim (2:0) \to (2:0)$
$(4:-1) \sim (4:-5) \to (4:-1)$	$(2:-3) \sim (2:-5) \to (2:-1)$
$(4:-4) \sim (4:0) \to (4:0)$	$(3:-1) \sim (3:5) \to (3:1)$
$(6:-1) \sim (6:5) \to (6:1)$	$(8:-1) \sim (8:15) \to (8:3)$
$(6:-4) \sim (6:-10) \to (6:-2)$	$(8:-4) \sim (8:-20) \to (8:-4)$

(h) There are sixteen primitive reduced forms of discriminant $7^2 \cdot -15 = -735$. We note the effect of the projection homomorphism below, with those forms sent to $(1:0)$ in the first column and those sent to $(2:0)$ in the second column.

$(1:-3) \sim (1:0) \to (1:0)$	$(2:-3) \sim (2:-7) \to (2:-1)$
$(4:-3) \sim (4:-7) \to (4:-1)$	$(2:-4) \sim (2:0) \to (2:0)$
$(4:-4) \sim (4:0) \to (4:0)$	$(3:-2) \sim (3:7) \to (3:1)$
$(6:-2) \sim (6:-14) \to (6:-2)$	$(5:-1) \sim (5:14) \to (5:2)$
$(6:-5) \sim (6:7) \to (6:1)$	$(8:-3) \sim (8:21) \to (8:3)$
$(10:-1) \sim (10:-21) \to (10:-3)$	$(8:-4) \sim (8:-28) \to (8:-4)$
$(10:-6) \sim (10:14) \to (10:4)$	$(12:1) \sim (12:-35) \to (12:-5)$
$(15:4) \sim (15:49) \to (15:7)$	$(12:-8) \sim (12:28) \to (12:4)$

(i) There are two reduced forms of discriminant $\Delta = -20$, $(1:0)$ and $(2:1)$. When $p = 3$, we find the following primitive reduced forms of discriminant $p^2\Delta = -180$: $(1:0)$, $(2:1) \sim (2:3)$, $(5:0)$, and $(7:2) \sim (7:9)$. The projection homomorphism sends these forms to $(1:0)$, $(2:1)$, $(5:0)$, and $(7:3)$ respectively. Here $(5:0) \sim (1:0)$ and $(7:3) \sim (2:1)$ in $\mathcal{F}_{-20}$.

(j) There are twelve primitive reduced forms of discriminant $7^2 \cdot -20 = -980$. These forms are listed below, along with an equivalent form to which ψ can be applied. Those in the first column are sent to a form equivalent to $(1:0)$ in $\mathcal{F}_{-20}$; those in

the second column are sent to $(2:1)$.

$(1:0)$	$(2:1) \sim (2:7)$
$(5:0)$	$(3:1) \sim (3:7)$
$(6:1) \sim (6:7)$	$(3:-1) \sim (3:-7)$
$(6:-1) \sim (6:-7)$	$(10:5) \sim (10:35)$
$(9:4) \sim (9:-14)$	$(15:5) \sim (15:35)$
$(9:-4) \sim (9:14)$	$(15:-5) \sim (15:-35)$

(k) There are three reduced forms of discriminant $\Delta = -23$: $(1:0)$, $(2:0)$, and $(2:-1)$. When $p = 3$, we find six primitive reduced forms of discriminant $p^2\Delta = -207$: $(1:-1) \sim (1:0)$, $(2:-1) \sim (2:-3)$, $(2:-2) \sim (2:0)$, $(4:-1) \sim (4:3)$, $(4:-2) \sim (4:-6)$, and $(8:2) \sim (8:-6)$. The projection homomorphism sends these forms to $(1:0)$, $(2:-1)$, $(2:0)$, $(4:1) \sim (2:0)$, $(4:-2) \sim (2:-1)$, and $(8:-2) \sim (1:0)$ respectively.

(l) There are eighteen primitive reduced forms of discriminant $5^2 \cdot -23 = -575$. We list these forms below, along with an equivalent form to which ψ can be applied. Those in the first column are sent to a form equivalent to $(1:0)$ in $\mathcal{F}_{-23}$; those in the second column are sent to $(2:0)$; those in the third column are sent to $(2:-1)$.

$(1:-2) \sim (1:0)$	$(2:-2) \sim (2:0)$	$(2:-3) \sim (2:-5)$
$(6:0)$	$(3:-2) \sim (3:-5)$	$(3:-3) \sim (3:0)$
$(6:-5)$	$(4:-3) \sim (4:5)$	$(4:-2) \sim (4:-10)$
$(8:-2) \sim (8:-10)$	$(6:-3) \sim (6:-15)$	$(6:-2) \sim (6:10)$
$(8:-3) \sim (8:5)$	$(9:-3) \sim (9:15)$	$(9:-2) \sim (9:-20)$
$(12:-2) \sim (12:10)$	$(12:-6) \sim (12:-30)$	$(12:1) \sim (12:25)$

(m) There are two reduced forms of discriminant $\Delta = -24$, $(1:0)$ and $(2:0)$. When $p = 3$, we find six primitive reduced forms of discriminant $p^2\Delta = -216$: $(1:0)$, $(2:0)$, $(5:1) \sim (5:6)$, $(5:-1) \sim (5:-6)$, $(7:3)$, and $(7:-3)$. The projection homomorphism sends these forms to $(1:0)$, $(2:0)$, $(5:2) \sim (2:0)$, $(5:-2) \sim (2:0)$, $(7:1) \sim (1:0)$, and $(7:-1) \sim (1:0)$ respectively.

(n) There are eight primitive reduced forms of discriminant $5^2 \cdot -24 = -600$. These forms are listed below, along with an equivalent form to which ψ can be applied. Those in the first column are sent to a form equivalent to $(1:0)$ in $\mathcal{F}_{-24}$; those in the second column are sent to $(2:0)$.

$(1:0)$	$(2:0)$
$(6:0)$	$(3:0)$
$(7:2) \sim (7:-5)$	$(11:2) \sim (11:-20)$
$(7:-2) \sim (7:5)$	$(11:-2) \sim (11:20)$

(2) Let Γ_p be the set of all unimodular 2×2 matrices having the lower left-hand entry divisible by p. The identity matrix is an element of Γ_p; the inverse of a matrix $\begin{bmatrix} q & s \\ r & t \end{bmatrix}$ in Γ_p is $\begin{bmatrix} t & -s \\ -r & q \end{bmatrix}$, which is also in Γ_p; the product of two elements of Γ_p is also in Γ_p, since the lower left-hand entry of $\begin{bmatrix} q & s \\ r & t \end{bmatrix} \cdot \begin{bmatrix} u & w \\ v & x \end{bmatrix}$ is $ru+tv$, which is divisible by p if both r and v are divisible by p. The remaining claims of this exercise were established in Exercise 4 of §4.2.

Section 8.3. The Kernel of a Projection Homomorphism.

(1) Let $\phi = (1:0) = x^2 + bxy + cy^2$, where $b = \varepsilon$ and $c = \frac{\varepsilon^2 - \Delta}{4}$ for some discriminant Δ, and let $V_k = \begin{bmatrix} -k-b & -1 \\ 1 & 0 \end{bmatrix}$. Applying Proposition 4.2.1, we have that $\phi \circ V_k = (m : \ell)$, where

$$m = \phi(-k-b, 1) = (-k-b)^2 + b(-k-b) + c = k^2 + bk + c = \phi(k)$$

and

$$\ell = (-k-b)(-1) + b(-1)(1) + c(1)(0) + 0 = k.$$

So $\phi \circ V_k = (\phi(k) : k)$, which is denoted as ϕ_k.

(2) Let $\phi_k = (\phi(k) : k) = \phi(k)x^2 + \phi'(k)xy + y^2$ and $V_{\ell,k} = \begin{bmatrix} 1 & 0 \\ \ell - k & 1 \end{bmatrix}$ for some k and ℓ. Again applying Proposition 4.2.1, we find that $\phi_k \circ V_{\ell,k} = (\phi(\ell) : \ell)$ since

$$\begin{aligned} \phi_k(1, \ell - k) &= \phi(k) + \phi'(k)(\ell - k) + (\ell - k)^2 \\ &= (k^2 + bk + c) + (2k + b)(\ell - k) + (\ell^2 - 2k\ell + k^2) = \ell^2 + b\ell + c \end{aligned}$$

and

$$\phi(k)(1)(0) + \phi'(k)(0)(1) + 1(\ell - k)(1) + k = \ell.$$

That is, $\phi_\ell = \phi(k) \circ V_{\ell,k}$.

Section 9.1. Introduction to Continued Fractions.

(1) Let $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. Let $r_0 = 1$ and $r_{i+1} = \frac{r_i + 1}{r_i}$ for $i \geq 0$. Note that $r_0 = F_2/F_1$ since $F_2 = F_1 + F_0 = 1 + 0 = 1$. Suppose that $r_k = F_{k+2}/F_{k+1}$ for some $k \geq 0$. Then notice that

$$r_k + 1 = \frac{F_{k+2}}{F_{k+1}} + 1 = \frac{F_{k+2} + F_{k+1}}{F_{k+1}} = \frac{F_{k+3}}{F_{k+1}}.$$

So now

$$r_{k+1} = \frac{r_k + 1}{r_k} = \frac{F_{k+3}}{F_{k+1}} \cdot \frac{F_{k+1}}{F_{k+2}} = \frac{F_{(k+1)+2}}{F_{(k+1)+1}}.$$

It follows that $r_n = F_{n+2}/F_{n+1}$ for all $n \geq 0$ by induction.

(2) (a) If $v = v_0 = \frac{249}{89} = 2 + \frac{71}{89}$, then $v_1 = \frac{89}{71} = 1 + \frac{18}{71}$, $v_2 = \frac{71}{18} = 3 + \frac{17}{18}$, $v_3 = \frac{18}{17} = 1 + \frac{1}{17}$, and $v_4 = \frac{17}{1} = 17 + \frac{0}{1}$, with v_5 undefined. The continued fraction for v is

$$2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{17}}}},$$

with the sequence of convergents

$$r_0 = 2, \quad r_1 = 3, \quad r_2 = \tfrac{11}{4}, \quad r_3 = \tfrac{14}{5}, \quad r_4 = \tfrac{249}{89}.$$

(b) For $v = v_0 = \sqrt{2} = 1 + (-1 + \sqrt{2})$, we find that $v_1 = \frac{1}{-1+\sqrt{2}} = 1 + \sqrt{2} = 2 + (-1 + \sqrt{2})$, and then $v_i = 1 + \sqrt{2}$ for all $i \geq 1$. Now $r_0 = 1$, then $r_1 = 1 + \frac{1}{2} = \frac{3}{2}$, so that $r_2 = 1 + \frac{1}{2 + \frac{1}{2}} = \frac{7}{5}$, and so forth. The sequence of convergents r_i with $i \leq 5$ is

$$r_0 = 1, \quad r_1 = \tfrac{3}{2}, \quad r_2 = \tfrac{7}{5}, \quad r_3 = \tfrac{17}{12}, \quad r_4 = \tfrac{41}{29}, \quad r_5 = \tfrac{99}{70}.$$

(c) For $v = \sqrt{3}$, the sequence of convergents begins

$$r_0 = 1, \quad r_1 = 2, \quad r_2 = \tfrac{5}{3}, \quad r_3 = \tfrac{7}{4}, \quad r_4 = \tfrac{19}{11}, \quad r_5 = \tfrac{26}{15}.$$

(d) The sequence of convergents for $v = \sqrt{7}$ begins

$$r_0 = 2, \quad r_1 = 3, \quad r_2 = \tfrac{5}{2}, \quad r_3 = \tfrac{8}{3}, \quad r_4 = \tfrac{37}{14}, \quad r_5 = \tfrac{45}{17}.$$

(e) The sequence of convergents for $v = \frac{4+\sqrt{3}}{7}$ begins

$$r_0 = 0, \quad r_1 = 1, \quad r_2 = \tfrac{4}{5}, \quad r_3 = \tfrac{5}{6}, \quad r_4 = \tfrac{9}{11}, \quad r_5 = \tfrac{104}{127}.$$

(3) (a) If $w = \langle\overline{1,2}\rangle$, we can assume that $w = 1+\frac{1}{2+\frac{1}{w}} = 1+\frac{w}{2w+1} = \frac{3w+1}{2w+1}$, so that w satisfies $(2w^2+w)-(3w+1) = 2w^2-2w-1 = 0$. Since w is larger than 1, we conclude that $w = \frac{2+\sqrt{12}}{4} = \frac{1+\sqrt{3}}{2}$.

(b) If $w = \langle\overline{1,2,3}\rangle$, then $w = 1+\frac{1}{2+\frac{1}{3+\frac{1}{w}}} = 1+\frac{1}{2+\frac{w}{3w+1}} = 1+\frac{3w+1}{7w+2} = \frac{10w+3}{7w+2}$. We find that w is the larger solution of $(7w^2+2w)-(10w+3) = 7w^2-8w-3 = 0$, that is, $w = \frac{4+\sqrt{37}}{7}$.

(c) If $w = \langle\overline{1,2}\rangle = \frac{1+\sqrt{3}}{2}$ as in part (a), then $v = \langle 3,\overline{1,2}\rangle = 3+\frac{1}{w} = \frac{5+3\sqrt{3}}{1+\sqrt{3}} = 2+\sqrt{3}$.

(d) If $w = \langle\overline{1}\rangle = 1+\frac{1}{w}$, we find that $w^2-w-1 = 0$ and that $w = \frac{1+\sqrt{5}}{2}$. So then $v = \langle 3,2,\overline{1}\rangle = 3+\frac{1}{2+\frac{1}{w}} = 3+\frac{w}{2w+1} = \frac{7w+3}{2w+1}$, which simplifies to $v = \frac{9-\sqrt{5}}{2}$.

(e) If $w = \langle\overline{2,5}\rangle = 2+\frac{1}{5+\frac{1}{w}}$, then w is the larger solution of $(5w^2+w)-(11w+2) = 5w^2-10w-2 = 0$, that is, $w = \frac{10+\sqrt{140}}{10}$. Then $v = \langle 1,\overline{2,5}\rangle = 1+\frac{1}{w}$, which simplifies to $v = \frac{-3+\sqrt{35}}{2}$.

(f) If $w = \langle\overline{1,1,1,4}\rangle$, we find that $w = \frac{14w+3}{9w+2}$. Then w satisfies $3w^2-4w-1 = 0$, and so $w = \frac{2+\sqrt{7}}{3}$. Now $v = \langle 1,4,\overline{1,1,1,4}\rangle = 1+\frac{1}{4+\frac{1}{w}}$, which simplifies to $v = \frac{1+\sqrt{7}}{3}$.

Section 9.2. Pell's Equation.

(1) For each d, we present the data from the algorithm of Theorem 9.2.2 as a table.

(a) For $d = 11$:

i	0	1	2
a	1	2	1
k	0	-3	-3
q	3	3	
m	3	10	
n	1	3	

Here beginning with $a_0 = 1$ and $k_0 = 0$, we select k_1 to be the smallest integer greater than $-\sqrt{11} \approx -3.3$ congruent to $-k_0 = 0$ modulo $a_0 = 1$, that is, $k_1 = -3$. So then $a_1 = \frac{11-k_1^2}{a_0} = 2$. Now we select $k_2 > -\sqrt{11}$ congruent to $-k_1 = 3$ modulo $a_1 = 2$, that is, $k_2 = -3$. Thus $a_2 = \frac{11-k_2^2}{a_1} = 1$. We terminate the algorithm when we obtain an $\ell > 0$ so that $a_\ell = 1$. For $0 \le i < \ell$, we calculate $q_i = -\frac{k_i+k_{i+1}}{a_i}$, and then $m_i = q_i m_{i-1} + m_{i-2}$ and $n_i = q_i n_{i-1} + n_{i-2}$ where $m_{-2} = 0$, $m_{-1} = 1$, $n_{-2} = 1$, and $n_{-1} = 0$. If ℓ is even, then $(x,y) = (m_{\ell-1}, n_{\ell-1})$ is the fundamental solution of $x^2 - dy^2 = 1$. In this example, $(x,y) = (10,3)$ and we verify that $10^2 - 11\cdot 3^2 = 1$.

(b) For $d = 13$:

i	0	1	2	3	4	5
a	1	4	3	3	4	1
k	0	-3	-1	-2	-1	-3
q	3	1	1	1	1	
m	3	4	7	11	18	
n	1	1	2	3	5	

Here $\ell = 5$ is odd. If we let $v = m_{\ell-1} + n_{\ell-1}\sqrt{d}$, then $v^2 = m_{2\ell-1} + n_{2\ell-1}\sqrt{d}$ and $(x, y) = (m_{2\ell-1}, n_{2\ell-1})$ is the fundamental solution of $x^2 - dy^2 = 1$. In this example, $v = 18 + 5\sqrt{13}$ and $v^2 = 649 + 180\sqrt{13}$, so that $(x, y) = (649, 180)$.

(c) For $d = 14$:

i	0	1	2	3	4
a	1	5	2	5	1
k	0	-3	-2	-2	-3
q	3	1	2	1	
m	3	4	11	15	
n	1	1	3	4	

So $(x, y) = (15, 4)$ is the fundamental solution of $x^2 - 14y^2 = 1$.

(d) For $d = 20$:

i	0	1	2
a	1	4	1
k	0	-4	-4
q	4	2	
m	4	9	
n	1	2	

Thus $(x, y) = (9, 2)$ is the fundamental solution of $x^2 - 20y^2 = 1$.

(e) For $d = 23$:

i	0	1	2	3	4
a	1	7	2	7	1
k	0	-4	-3	-3	-4
q	4	1	3	1	
m	4	5	19	24	
n	1	1	4	5	

The fundamental solution of $x^2 - 23y^2 = 1$ is $(x, y) = (24, 5)$.

(f) For $d = 31$:

i	0	1	2	3	4	5	6	7	8
a	1	6	5	3	2	3	5	6	1
k	0	-5	-1	-4	-5	-5	-4	-1	-5
q	5	1	1	3	5	3	1	1	
m	5	6	11	39	206	657	863	1520	
n	1	1	2	7	37	118	155	273	

The fundamental solution of $x^2 - 31y^2 = 1$ is $(x, y) = (1520, 273)$.

(g) For $d = 33$:

i	0	1	2	3	4
a	1	8	3	8	1
k	0	-5	-3	-3	-5
q	5	1	2	1	
m	5	6	17	23	
n	1	1	3	4	

The fundamental solution of $x^2 - 33y^2 = 1$ is $(x, y) = (23, 4)$.

(h) For $d = 41$:

i	0	1	2	3
a	1	5	5	1
k	0	-6	-4	-6
q	6	2	2	
m	6	13	32	
n	1	2	5	

Here ℓ is odd. Since $(32+5\sqrt{41})^2 = 2049+320\sqrt{41}$, we have that $(x, y) = (2049, 320)$ is the fundamental solution of $x^2 - 41y^2 = 1$.

(i) For $d = 46$:

i	0	1	2	3	4	5	6	7	8	9	10	11	12
a	1	10	3	7	6	5	2	5	6	7	3	10	1
k	0	-6	-4	-5	-2	-4	-6	-6	-4	-2	-5	-4	-6
q	6	1	3	1	1	2	6	2	1	1	3	1	
m	6	7	27	34	61	156	997	2150	3147	5297	19038	24335	
n	1	1	4	5	9	23	147	317	464	781	2807	3588	

The fundamental solution of $x^2 - 46y^2 = 1$ is $(x, y) = (24335, 3588)$.

(j) For $d = 53$:

i	0	1	2	3	4	5
a	1	4	7	7	4	1
k	0	-7	-5	-2	-5	-7
q	7	3	1	1	3	
m	7	22	29	51	182	
n	1	3	4	7	25	

Since $(182 + 25\sqrt{53})^2 = 66249 + 9100\sqrt{53}$, the fundamental solution of $x^2 - 53y^2 = 1$ is $(x, y) = (66249, 9100)$.

(2) (a) Let $d = t^2 + 1$ for some positive integer t. The smallest integer greater than $-\sqrt{d}$ is $-t$, and we find in applying Theorem 9.2.2 that $k_1 = -t$ and $a_1 = 1$, so that $\ell = 1$ in the notation of that algorithm. Then $q_0 = t = m_0$ and $n_0 = 1$, and the fundamental solution of $x^2 - dy^2 = 1$ is given by $(t+\sqrt{d})^2 = (t^2+d)+2t\sqrt{d} = (2t^2+1)+2t\sqrt{d}$. That is, $(x, y) = (2t^2 + 1, 2t)$ is the fundamental solution of $x^2 - dy^2 = 1$ when $d = t^2 + 1$.

(b) Let $d = t^2 - 1$ for some $t > 1$. Here the smallest integer greater than $-\sqrt{d}$ is $-t + 1$. Since $d - (-t + 1)^2 = 2t - 2$, we can compile the following data from Pell's equation

algorithm.

i	0	1	2
a	1	$2t-2$	1
k	0	$-t+1$	$-t+1$
q	$t-1$	1	
m	$t-1$	t	
n	1	1	

(For example, $t-1 \equiv -t+1 \pmod{2t-2}$, which produces the calculation of k_2 and a_2.) We conclude that $(x, y) = (t, 1)$ is the fundamental solution of $x^2 - dy^2 = 1$ when $d = t^2 - 1$ is positive.

(c) Let $d = t^2 + 2$ for some positive integer t. Then $-t$ is the smallest integer greater than $-\sqrt{d}$, and we compile the following data from Pell's equation algorithm. (Note that $d - (-t)^2 = 2$ and that $t \equiv -t \pmod{2t}$.)

i	0	1	2
a	1	2	1
k	0	$-t$	$-t$
q	t	t	
m	t	t^2+1	
n	1	t	

We conclude that $(x, y) = (t^2 + 1, t)$ is the fundamental solutions of $x^2 - dy^2 = 1$ when $d = t^2 + 2$.

(d) Let $d = t^2 + t$ for some positive integer t. We find again that $-t$ is the smallest integer greater than $-\sqrt{d}$, since $t^2 < d < (t+1)^2 = t^2 + 2t + 1$. With $d - (-t)^2 = t$ and $t \equiv -t \pmod{t}$, we compile the following data from Pell's equation algorithm.

i	0	1	2
a	1	t	1
k	0	$-t$	$-t$
q	t	2	
m	t	$2t+1$	
n	1	2	

Thus $(x, y) = (2t + 1, 2)$ is the fundamental solution of $x^2 - dy^2 = 1$ when $d = t^2 + t$.

(3) Let $v = q + r\sqrt{d}$ where (q, r) is the fundamental solution of $x^2 - dy^2 = 1$. For all integers n, write v^n as $q_n + r_n\sqrt{d}$. Note that

$$v^{k+1} = v^k \cdot v = (q_k + r_k\sqrt{d})(q + r\sqrt{d}) = (qq_k + drr_k) + (qr_k + rq_k)\sqrt{d}$$

for all integers k. Now let $U = \begin{bmatrix} q & dr \\ r & q \end{bmatrix}$ and suppose that $U^k = \begin{bmatrix} q_k & dr_k \\ r_k & q_k \end{bmatrix}$ for some positive integer k. Then

$$U^{k+1} = U \cdot U_k = \begin{bmatrix} q & dr \\ r & q \end{bmatrix} \cdot \begin{bmatrix} q_k & dr_k \\ r_k & q_k \end{bmatrix}$$
$$= \begin{bmatrix} qq_k + drr_k & qdr_k + drq_k \\ rq_k + qr_k & rdr_k + qq_k \end{bmatrix} = \begin{bmatrix} q_{k+1} & dr_{k+1} \\ r_{k+1} & q_{k+1} \end{bmatrix},$$

using the preceding observation. It follows that $U^n = \begin{bmatrix} q_n & dr_n \\ r_n & q_n \end{bmatrix}$ for all positive integers n by induction. The claim also holds for $n = 0$ and for negative integers n, using the

fact that if m is positive, then $v^{-m} = q_m - r_m\sqrt{d}$ (since $(q_m + r_m\sqrt{d})(q_m - r_m\sqrt{d}) = q_m^2 - dr_m^2 = 1$) while $U^{-m} = \begin{bmatrix} q_m & dr_m \\ r_m & q_m \end{bmatrix}^{-1} = \begin{bmatrix} q_m & -dr_m \\ -r_m & q_m \end{bmatrix}$ by properties of matrix inverses.

Section 9.3. Convergence of Continued Fractions.

(1) (a) $\langle -3,1,5,3\rangle = \left\langle -3,1,5+\frac{1}{3}\right\rangle = \left\langle -3,1+\frac{3}{16}\right\rangle = -3+\frac{16}{19} = -\frac{41}{19}$.
(b) $\langle 0,2,2,2,4\rangle = \left\langle 0,2,2,2+\frac{1}{4}\right\rangle = \left\langle 0,2,2+\frac{4}{9}\right\rangle = \left\langle 0,2+\frac{9}{22}\right\rangle = 0+\frac{22}{53} = \frac{22}{53}$.
(c) $\langle 2,1,3,1,4,3\rangle = \left\langle 2,1,3,1,4+\frac{1}{3}\right\rangle = \left\langle 2,1,3,1+\frac{3}{13}\right\rangle = \left\langle 2,1,3+\frac{13}{16}\right\rangle = \left\langle 2,1+\frac{16}{61}\right\rangle = 2+\frac{61}{77} = \frac{215}{77}$.

(2) We calculate $r_i = \frac{m_i}{n_i}$ for $0 \le i \le 5$ for each continued fraction using the following tables.
(a) For $\langle 2,1,2,1,2,1,\ldots\rangle$:

i	0	1	2	3	4	5
q	2	1	2	1	2	1
m	2	3	8	11	30	41
n	1	1	3	4	11	15

(b) For $\langle 3,3,3,3,3,3,\ldots\rangle$:

i	0	1	2	3	4	5
q	3	3	3	3	3	3
m	3	10	33	109	360	1189
n	1	3	10	33	109	360

(c) For $\langle 1,2,3,1,2,3,\ldots\rangle$:

i	0	1	2	3	4	5
q	1	2	3	1	2	3
m	1	3	10	13	36	121
n	1	2	7	9	25	84

(3) (a) $\langle 1,2,w\rangle = \left\langle 1,2+\frac{1}{w}\right\rangle = 1+\frac{w}{2w+1} = \frac{3w+1}{2w+1}$.
(b) $\langle 2,3,5,w\rangle = \left\langle 2,3,5+\frac{1}{w}\right\rangle = \left\langle 2,3+\frac{w}{5w+1}\right\rangle = 2+\frac{5w+1}{16w+3} = \frac{37w+7}{16w+3}$.
(c) $\langle 2,1,3,1,w\rangle = \left\langle 2,1,3,1+\frac{1}{w}\right\rangle = \left\langle 2,1,3+\frac{w}{w+1}\right\rangle = \left\langle 2,1+\frac{w+1}{4w+3}\right\rangle = 2+\frac{4w+3}{5w+4} = \frac{14w+11}{5w+4}$.

(4) (a) $\langle 1,2\rangle = 1+\frac{1}{2} = \frac{3}{2}$ while $\langle 1,3\rangle = 1+\frac{1}{3} = \frac{4}{3}$. So $\langle 1,2\rangle$ is larger than $\langle 1,3\rangle$.
(b) $\langle 1,2,3\rangle = \left\langle 1,2+\frac{1}{3}\right\rangle = 1+\frac{3}{7} = \frac{10}{7}$ while $\langle 1,2,4\rangle = \left\langle 1,2+\frac{1}{4}\right\rangle = 1+\frac{4}{9} = \frac{13}{9}$. Here we find that $\langle 1,2,4\rangle$ is larger that $\langle 1,2,3\rangle$.
(c) $\langle 1,2\rangle = \frac{3}{2}$ is larger than $\langle 1,2,3\rangle = \frac{10}{7}$.
(d) $\langle 1,1,1,1,1,2\rangle = \left\langle 1,1,1,1,\frac{3}{2}\right\rangle = \left\langle 1,1,1,\frac{5}{3}\right\rangle = \left\langle 1,1,\frac{8}{5}\right\rangle = \left\langle 1,\frac{13}{8}\right\rangle = \frac{21}{13} \approx 1.615$ while $\langle 1,1,1,1,1,1,2\rangle = \left\langle 1,1,1,1,1,\frac{3}{2}\right\rangle = \left\langle 1,1,1,1,\frac{5}{3}\right\rangle = \left\langle 1,1,1,\frac{8}{5}\right\rangle = \left\langle 1,1,\frac{13}{8}\right\rangle = \left\langle 1,\frac{21}{13}\right\rangle = \frac{34}{21} \approx 1.619$. So $\langle 1,1,1,1,1,1,2\rangle$ is larger than $\langle 1,1,1,1,1,2\rangle$.

(5) Let x and y be real numbers with $x > y \ge 1$, let $q_0, q_1, \ldots, q_i$ be integers with $q_j > 0$ if $j > 0$, and let v, w, and z be as follows:

$$v = \langle q_0, q_1, \ldots, q_i\rangle, \qquad w = \langle q_0, q_1, \ldots, q_i, x\rangle, \qquad \text{and} \qquad z = \langle q_0, q_1, \ldots, q_i, y\rangle.$$

If $i = 0$, then $v = q_0$, $w = q_0 + \frac{1}{x}$, and $z = q_0 + \frac{1}{y}$. Since $0 < \frac{1}{x} < \frac{1}{y} \le 1$ if $x > y \ge 1$, then $v < w < z$. Now if $i = 1$, we have that $v = \langle q_0, q_1\rangle$, $w = \left\langle q_0, q_1 + \frac{1}{x}\right\rangle$, and $z = \left\langle q_0, q_1 + \frac{1}{y}\right\rangle$.

Now $1 \le q_1 < q_1 + \frac{1}{x} < q_1 + \frac{1}{y}$, so from the case of $i = 0$, it follows that $v > w > z$. Continuing in this way, we see inductively that $v < w < z$ if i is even and $v > w > z$ if i is odd.

Section 9.4. Continued Fraction Expansions of Real Numbers.

(1) The statement $\langle q_0, q_1, q_2, \ldots\rangle = \langle q_0, \langle q_1, q_2, \ldots\rangle\rangle$ is true by Lemma 9.4.3. Suppose that we have established that $\langle q_0, q_1, q_2, \ldots\rangle = \langle q_0, q_1, \ldots, q_k, \langle q_{k+1}, q_{k+2}, \ldots\rangle\rangle$ for some $k \ge 0$. Let $w = \langle q_{k+2}, q_{k+3}, \ldots\rangle$. Then again applying Lemma 9.4.3 and the definition of continued fractions, we have

$$\begin{aligned}\langle q_0, q_1, q_2, \ldots\rangle &= \langle q_0, q_1, \ldots, q_k, \langle q_{k+1}, q_{k+2}, \ldots\rangle\rangle \\ &= \langle q_0, q_1, \ldots, q_k, \langle q_{k+1}, w\rangle\rangle \\ &= \left\langle q_0, q_1, \ldots, q_k, q_{k+1} + \tfrac{1}{w}\right\rangle \\ &= \langle q_0, q_1, \ldots, q_k, q_{k+1}, w\rangle \\ &= \langle q_0, q_1, \ldots, q_k, q_{k+1}, \langle q_{k+2}, q_{k+3}, \ldots\rangle\rangle\end{aligned}$$

The result follows for all $k \ge 0$ by induction.

(2) In each part, we apply calculations from Exercise 9.3.3.
   (a) If $v = \langle 1, 2, v\rangle$, then $v = \frac{3v+1}{2v+1}$. So then v is a solution of $(2v^2 + v) - (3v + 1) = 2v^2 - 2v - 1 = 0$. Since $v > 1$, we conclude that $v = \frac{2+\sqrt{12}}{4} = \frac{1+\sqrt{3}}{2}$.
   (b) If $v = \langle 2, 3, 5, v\rangle$, then $v = \frac{37v+7}{16v+3}$. So $v > 2$ satisfies $(16v^2 + 3v) - (37v + 7) = 16v^2 - 34v - 7 = 0$. We conclude that $v = \frac{17+\sqrt{401}}{16}$.
   (c) If $v = \langle 2, 1, 3, 1, v\rangle$, then $v = \frac{14v+11}{5v+4}$. So $v > 2$ satisfies $(5v^2 + 4v) - (14v + 11) = 5v^2 - 10v - 11 = 0$, and we conclude that $v = \frac{5+4\sqrt{5}}{5}$.

(3) Suppose that $\langle q_0, q_1, \ldots, q_k\rangle = \langle r_0, r_1, \ldots, r_k, r_{k+1}, \ldots\rangle$ with each q_i and r_i a positive integer for $i \ge 1$. By the same argument as in the proof of Theorem 9.4.4, we obtain the equation $q_k = \langle r_k, r_{k+1}, \ldots\rangle = r_k + \frac{1}{w}$, where $w = \langle r_{k+1}, r_{k+2}, \ldots\rangle$. But since w is a real number with $w > r_{k+1} \ge 1$, we know that $0 < \frac{1}{w} < 1$. Thus the equation $\frac{1}{w} = q_k - r_k$ is impossible.

(4) If n is an integer and $v = \langle q_0, q_1, q_2, \ldots\rangle$, then $v + n = \langle n + q_0, q_1, q_2, \ldots\rangle$. Here if $w = \langle q_1, q_2, \ldots\rangle$, then $v = \langle q_0, w\rangle = q_0 + \frac{1}{w}$. But then $v + n = (n + q_0) + \frac{1}{w} = \langle n + q_0, w\rangle = \langle n + q_0, q_1, q_2, \ldots\rangle$, using the definition of continued fractions and Lemma 9.4.3.

(5) If $v = \langle q_0, q_1, q_2, \ldots\rangle$ is larger than 1, then $1 < v < q_0 + 1$, so that q_0 is positive. Thus $\langle 0, q_0, q_1, q_2, \ldots\rangle$ is a continued fraction for a real number w, and $w = \langle 0, \langle q_0, q_1, q_2, \ldots\rangle\rangle = \langle 0, v\rangle = 0 + \frac{1}{v} = \frac{1}{v}$, using Lemma 9.4.3.

(6) Let $v = \langle q_0, q_1, q_2, \ldots\rangle$ be larger than 1, so that $\frac{1}{v} = \langle 0, q_0, q_1, q_2, \ldots\rangle$. If r_i is the i-th convergent of v, then $r_i = \langle q_0, q_1, \ldots, q_i\rangle$ by Corollary 9.3.3. Similarly, if s_i is the i-th convergent of $\frac{1}{v}$, then $s_{i+1} = \langle 0, q_0, q_1, \ldots, q_i\rangle = \langle 0, \langle q_0, q_1, \ldots, q_i\rangle\rangle = \langle 0, r_i\rangle = \frac{1}{r_i}$ by Lemma 9.4.3 and the definition of continued fractions.

Section 9.5. Purely Periodic Continued Fractions.

(1) (a) Let $v = \overline{\langle 2, 5\rangle} = \langle 2, 5, v\rangle = \left\langle 2, 5 + \frac{1}{v}\right\rangle = 2 + \frac{v}{5v+1} = \frac{11v+2}{5v+1}$. Then $v > 2$ satisfies the equation $(5v^2+v)-(11v+2) = 5v^2-10v-2 = 0$, so that $v = \frac{10+\sqrt{140}}{10} = \frac{5+\sqrt{35}}{5} \approx 2.18$. Here $\overline{v} = \frac{5-\sqrt{35}}{5} \approx -0.18$, confirming that v is reduced.

(b) For $v = \langle\overline{2,1,2}\rangle = \langle 2,1,2+\frac{1}{v}\rangle = \left\langle 2,1+\frac{v}{2v+1}\right\rangle = 2+\frac{2v+1}{3v+1} = \frac{8v+3}{3v+1}$, we find that v satisfies $(3v^2+v)-(8v+3) = 3v^2-7v-3 = 0$. So $v = \frac{7+\sqrt{85}}{6} \approx 2.70$ and $\overline{v} = \frac{7-\sqrt{85}}{6} \approx -0.37$.

(c) For $v = \langle\overline{4,3,1,3}\rangle = \langle 4,3,1,3+\frac{1}{v}\rangle = \left\langle 4,3,1+\frac{v}{3v+1}\right\rangle = \left\langle 4,3+\frac{3v+1}{4v+1}\right\rangle = 4+\frac{4v+1}{15v+4} = \frac{64v+17}{15v+4}$, we see that v satisfies $15x^2-60v-17 = 0$. So $v = \frac{30+\sqrt{1155}}{15} \approx 4.27$ and $\overline{v} = \frac{30-\sqrt{1155}}{15} \approx -0.27$.

(2) (a) To find reduced quadratic numbers $v = \frac{-b+\sqrt{b^2-4ac}}{2a}$ with $\Delta = b^2-4ac = 5$, we must have b an odd integer with $-\sqrt{5} < b < 0$, that is, $b = -1$. Now $\frac{-1+\sqrt{5}}{2} < a < \frac{1+\sqrt{5}}{2}$ forces $a = 1$, and $b^2-4ac = 5$ implies that $c = -1$. The only reduced quadratic number of discriminant $\Delta = 5$ is the larger root of $ax^2+bx+c = x^2-x-1$, that is, $v = \frac{1+\sqrt{5}}{2}$. (To verify that v is reduced, note that $v \approx 1.62$ and $\overline{v} = \frac{1-\sqrt{5}}{2} \approx -0.62$.)

(b) For $\Delta = 12$, we follow the same approach as in part (a), compiling the results in the following table.

a	b	c	v	$\overline{v}$
1	-2	-2	$1+\sqrt{3} \approx 2.73$	$1-\sqrt{3} \approx -0.73$
2	-2	-1	$\frac{1+\sqrt{3}}{2} \approx 1.37$	$\frac{1-\sqrt{3}}{2} \approx -0.37$

(c) For $\Delta = 21$:

a	b	c	v	$\overline{v}$
1	-3	-3	$\frac{3+\sqrt{21}}{2} \approx 3.79$	$\frac{3-\sqrt{21}}{2} \approx -0.79$
3	-3	-1	$\frac{3+\sqrt{21}}{6} \approx 1.26$	$\frac{3-\sqrt{21}}{6} \approx -0.26$

(d) For $\Delta = 76$:

a	b	c	v	$\overline{v}$
1	-8	-3	$4+\sqrt{19} \approx 8.36$	$4-\sqrt{19} \approx -0.36$
2	-6	-5	$\frac{3+\sqrt{19}}{2} \approx 3.68$	$\frac{3-\sqrt{19}}{2} \approx -0.68$
3	-4	-5	$\frac{2+\sqrt{19}}{3} \approx 2.12$	$\frac{2-\sqrt{19}}{3} \approx -0.79$
3	-8	-1	$\frac{4+\sqrt{19}}{3} \approx 2.79$	$\frac{4-\sqrt{19}}{3} \approx -0.12$
5	-4	-3	$\frac{2+\sqrt{19}}{5} \approx 1.27$	$\frac{2-\sqrt{19}}{5} \approx -0.47$
5	-6	-2	$\frac{3+\sqrt{19}}{5} \approx 1.47$	$\frac{3-\sqrt{19}}{5} \approx -0.27$

(e) For $\Delta = 145$:

a	b	c	v	$\overline{v}$
1	-11	-6	$\frac{11+\sqrt{145}}{2} \approx 11.52$	$\frac{11-\sqrt{145}}{2} \approx -0.52$
2	-11	-3	$\frac{11+\sqrt{145}}{4} \approx 5.76$	$\frac{11-\sqrt{145}}{4} \approx -0.26$
2	-9	-8	$\frac{9+\sqrt{145}}{4} \approx 5.26$	$\frac{9-\sqrt{145}}{4} \approx -0.76$
3	-11	-2	$\frac{11+\sqrt{145}}{6} \approx 3.84$	$\frac{11-\sqrt{145}}{6} \approx -0.17$
3	-7	-8	$\frac{7+\sqrt{145}}{6} \approx 3.17$	$\frac{7-\sqrt{145}}{6} \approx -0.84$
4	-9	-4	$\frac{9+\sqrt{145}}{8} \approx 2.63$	$\frac{9-\sqrt{145}}{8} \approx -0.38$
4	-7	-6	$\frac{7+\sqrt{145}}{8} \approx 2.38$	$\frac{7-\sqrt{145}}{8} \approx -0.63$
5	-5	-6	$\frac{5+\sqrt{145}}{10} \approx 1.70$	$\frac{5-\sqrt{145}}{10} \approx -0.70$
6	-11	-1	$\frac{11+\sqrt{145}}{12} \approx 1.92$	$\frac{11-\sqrt{145}}{12} \approx -0.09$
6	-7	-4	$\frac{7+\sqrt{145}}{12} \approx 1.59$	$\frac{7-\sqrt{145}}{12} \approx -0.42$
6	-5	-5	$\frac{5+\sqrt{145}}{12} \approx 1.42$	$\frac{5-\sqrt{145}}{12} \approx -0.59$
6	-1	-6	$\frac{1+\sqrt{145}}{12} \approx 1.09$	$\frac{1-\sqrt{145}}{12} \approx -0.92$
8	-9	-2	$\frac{9+\sqrt{145}}{16} \approx 1.32$	$\frac{9-\sqrt{145}}{16} \approx -0.19$
8	-7	-3	$\frac{7+\sqrt{145}}{16} \approx 1.19$	$\frac{7-\sqrt{145}}{16} \approx -0.32$

(3) For each v, we write $v \to_q w$ if $q = \lfloor v \rfloor$ and $w = (v-q)^{-1}$, and follow this process until we return to the original v. These cycles produce the continued fraction expansion of each value that is obtained in the cycle.

(a) For $\Delta = 5$, $\frac{1+\sqrt{5}}{2} \to_1 \frac{1+\sqrt{5}}{2}$ (that is, $\left(\frac{1+\sqrt{5}}{2} - 1\right)^{-1} = \frac{1+\sqrt{5}}{2}$) and thus $\frac{1+\sqrt{5}}{2} = \langle \overline{1} \rangle$.

(b) For $\Delta = 12$, $1+\sqrt{3} \to_2 \frac{1+\sqrt{3}}{2} \to_1 1+\sqrt{3}$. We find that $1+\sqrt{3} = \langle \overline{2,1} \rangle$ and $\frac{1+\sqrt{3}}{2} = \langle \overline{1,2} \rangle$.

(c) For $\Delta = 21$, $\frac{3+\sqrt{21}}{2} \to_3 \frac{3+\sqrt{21}}{6} \to_1 \frac{3+\sqrt{21}}{2}$, with $\frac{3+\sqrt{21}}{2} = \langle \overline{3,1} \rangle$ and $\frac{3+\sqrt{21}}{2} = \langle \overline{1,3} \rangle$.

(d) For $\Delta = 76$,

$$4+\sqrt{19} \to_8 \tfrac{4+\sqrt{19}}{3} \to_2 \tfrac{2+\sqrt{19}}{5} \to_1 \tfrac{3+\sqrt{19}}{2} \to_3 \tfrac{3+\sqrt{19}}{5} \to_1 \tfrac{2+\sqrt{19}}{3} \to_2 4+\sqrt{19}.$$

Starting this cycle at different numbers, we obtain the following continued fraction expansions:

$$4+\sqrt{19} = \langle \overline{8,2,1,3,1,2} \rangle, \quad \tfrac{4+\sqrt{19}}{3} = \langle \overline{2,1,3,1,2,8} \rangle, \quad \tfrac{2+\sqrt{19}}{5} = \langle \overline{1,3,1,2,8,2} \rangle,$$

$$\tfrac{3+\sqrt{19}}{2} = \langle \overline{3,1,2,8,2,1} \rangle, \quad \tfrac{3+\sqrt{19}}{5} = \langle \overline{1,2,8,2,1,3} \rangle, \quad \tfrac{2+\sqrt{19}}{3} = \langle \overline{2,8,2,1,3,1} \rangle.$$

(e) For $\Delta = 145$, we find four distinct cycles, which we combine with the continued fraction expansions of each number as follows.

$$\tfrac{11+\sqrt{145}}{2} = \langle \overline{11,1,1} \rangle \to_{11} \tfrac{11+\sqrt{145}}{12} = \langle \overline{1,1,11} \rangle \to_1 \tfrac{1+\sqrt{145}}{12} = \langle \overline{1,11,1} \rangle.$$

(This cycle returns to the original number at the next step, as do the following cycles.)

$$\tfrac{11+\sqrt{145}}{4} = \langle \overline{5,1,3} \rangle \to_5 \tfrac{9+\sqrt{145}}{16} = \langle \overline{1,3,5} \rangle \to_1 \tfrac{7+\sqrt{145}}{6} = \langle \overline{3,5,1} \rangle.$$

$$\tfrac{11+\sqrt{145}}{6} = \langle \overline{3,1,5} \rangle \to_3 \tfrac{7+\sqrt{145}}{16} = \langle \overline{1,5,3} \rangle \to_1 \tfrac{9+\sqrt{145}}{4} = \langle \overline{5,3,1} \rangle.$$

$$\tfrac{9+\sqrt{145}}{8} = \langle \overline{2,1,1,1,2} \rangle \to_2 \tfrac{7+\sqrt{145}}{12} = \langle \overline{1,1,1,2,2} \rangle$$

$$\to_1 \tfrac{5+\sqrt{145}}{10} = \langle \overline{1,1,2,2,1} \rangle \to_1 \tfrac{5+\sqrt{145}}{12} = \langle \overline{1,2,2,1,1} \rangle \to_1 \tfrac{7+\sqrt{145}}{8} = \langle \overline{2,2,1,1,1} \rangle.$$

Section 9.6. Continued Fractions of Irrational Quadratic Numbers.

(1) (a) Let $v = \langle\overline{1,1,2}\rangle = \langle 1,1,2,v\rangle = \langle 1,1,2+\frac{1}{v}\rangle = \left\langle 1,1+\frac{v}{2v+1}\right\rangle = 1+\frac{2v+1}{3v+1} = \frac{5v+2}{3v+1}$. Then $v > 1$ is a solution of $(3v^2+v)-(5v+2) = 3v^2-4v-2 = 0$, so that $v = \frac{4+\sqrt{40}}{6} = \frac{2+\sqrt{10}}{3}$.

(b) If $v = \langle 4,3,\overline{1,1,2}\rangle$, then $v = \langle 4,3,w\rangle = \langle 4,3+\frac{1}{w}\rangle = 4+\frac{w}{3w+1} = 13w+43w+1$, where $w = \frac{2+\sqrt{10}}{3}$ from part (a). We find that

$$v = \tfrac{38+13\sqrt{10}}{3}\cdot\tfrac{1}{3+\sqrt{10}} = \tfrac{38+13\sqrt{10}}{3}\cdot(-3+\sqrt{10}) = \tfrac{16-\sqrt{10}}{3}.$$

(c) If $w = \langle\overline{2,5}\rangle = \langle 2,5,w\rangle = \langle 2,5+\frac{1}{w}\rangle = 2+\frac{w}{5w+1} = \frac{11w+2}{5w+1}$, we find that w is the larger root of $5x^2-10x-2$, that is, $w = \frac{10+\sqrt{140}}{10} = \frac{5+\sqrt{35}}{5}$. Then $v = \langle 3,7,6,\overline{2,5}\rangle = \langle 3,7,6,w\rangle = \frac{135w+22}{43w+7}$, from which we calculate that $v = \frac{1385+\sqrt{35}}{443}$.

(d) If $w = \langle\overline{3,1,5}\rangle = \langle 3,1,5,w\rangle = \frac{23w+4}{6w+1}$, then w is the larger root of $6x^2-22x-4$, that is, $w = \frac{11+\sqrt{145}}{6}$. Then $v = \langle 2,1,\overline{3,1,5}\rangle = \langle 2,1,w\rangle = \frac{3w+2}{w+1}$, from which we calculate that $v = \frac{55+\sqrt{145}}{24}$.

(e) If $w = \langle\overline{1,2,3}\rangle$, we find that w is the larger root of $7x^2-8x-3$, that is, $w = \frac{4+\sqrt{37}}{7}$. Then $v = \langle 1,2,1,\overline{1,2,3}\rangle = \langle 1,2,1,w\rangle = \frac{4w+3}{3w+2}$, from which we calculate that $v = \frac{74-\sqrt{37}}{49}$.

(2) (a) If $v = \frac{1+\sqrt{5}}{2}$, so that $\overline{v} = \frac{1-\sqrt{5}}{2}$, then $v+\overline{v} = 1$ and $v\cdot\overline{v} = -1$. Thus $f(x) = x^2-x-1$ is the minimum polynomial of v, and $\Delta = 5$ is the discriminant of v. We find that $(v-\lfloor v\rfloor)^{-1} = \frac{2}{-1+\sqrt{5}} = \frac{1+\sqrt{5}}{2} = v$, and conclude that $v = \langle\overline{1}\rangle$.

(b) If $v = \frac{11+5\sqrt{7}}{3}$ and $\overline{v} = \frac{11-5\sqrt{7}}{3}$, then $v+\overline{v} = \frac{22}{3}$ and $v\cdot\overline{v} = -6$. Thus v has minimum polynomial $f(x) = 3x^2-22x-18$ and discriminant $\Delta = (-22)^2-4\cdot 3\cdot -18 = 700$. Using the notation introduced in Exercise 3 of §9.5, we have

$$\tfrac{11+5\sqrt{7}}{3} \to_8 \tfrac{13+5\sqrt{7}}{2} \to_{13} \tfrac{13+5\sqrt{7}}{3} \to_8 \tfrac{11+5\sqrt{7}}{18} \to_1 \tfrac{7+5\sqrt{7}}{7} \to_2 \tfrac{7+5\sqrt{7}}{18} \to_1 \tfrac{11+5\sqrt{7}}{3},$$

which implies that $v = \langle\overline{8,13,8,1,2,1}\rangle$.

(c) If $v = \frac{7-\sqrt{11}}{4}$ and $\overline{v} = \frac{7+\sqrt{11}}{4}$, then $v+\overline{v} = \frac{7}{2}$ and $v\cdot\overline{v} = \frac{19}{8}$. Thus the minimum polynomial of v is $f(x) = 8x^2-28x+19$ and v has discriminant $\Delta = (-28)^2-4\cdot 8\cdot 19 = 176$. Here we find

$$\begin{aligned}\tfrac{7-\sqrt{11}}{4} \to_0 \tfrac{14+2\sqrt{11}}{19} \to_1 5+2\sqrt{11} \to_{11} \tfrac{3+\sqrt{11}}{4} \to_1 \tfrac{2+2\sqrt{11}}{5} \to_1 \tfrac{3+2\sqrt{11}}{7}\\ \to_1 \tfrac{2+\sqrt{11}}{2} \to_2 \tfrac{4+2\sqrt{11}}{7} \to_1 \tfrac{3+2\sqrt{11}}{5} \to_1 \tfrac{1+\sqrt{11}}{4} \to_1 6+2\sqrt{11} \to_{12} \tfrac{3+\sqrt{11}}{4},\end{aligned}$$

and conclude that $v = \langle 0,1,11,\overline{1,1,1,2,1,1,1,12}\rangle$.

(3) (a) If $d = t^2+1$, then $\left\lfloor\sqrt{d}\right\rfloor = t$ and $\frac{1}{\sqrt{d}-t} = \sqrt{d}+t$. Then $\left\lfloor\sqrt{d}+t\right\rfloor = 2t$ and $\frac{1}{(\sqrt{d}+t)-2t} = \frac{1}{\sqrt{d}-t} = \sqrt{d}+t$. The continued fraction algorithm now repeats this value indefinitely, and so $\sqrt{d} = \langle t,\overline{2t}\rangle$. (Using the notation of the preceding exercise, the sequence $\sqrt{d} \to_t (\sqrt{d}+t) \to_{2t} (\sqrt{d}+t)$ produces this periodic continued fraction.)

(b) If $d = t^2-1$ for some $t > 1$, then $\left\lfloor\sqrt{d}\right\rfloor = t-1$ and $\frac{1}{\sqrt{d}-(t-1)} = \frac{\sqrt{d}+(t-1)}{2t-2}$, here using the fact that $d-(t-1)^2 = (t^2-1)-(t^2-2t+1) = 2t-2$. Now since $t-1 < \sqrt{d} < t$, we find that $\left\lfloor\frac{\sqrt{d}+(t-1)}{2t-2}\right\rfloor = 1$ and $\frac{\sqrt{d}+(t-1)}{2t-2}-1 = \frac{\sqrt{d}-(t-1)}{2t-2}$. Then

$\frac{2t-2}{\sqrt{d}-(t-1)} = \frac{(2t-2)(\sqrt{d}+(t-1))}{2t-2} = \sqrt{d}+(t-1)$. But now $\left\lfloor \sqrt{d}+(t-1) \right\rfloor = 2t-2$, with $(\sqrt{d}+(t-1))-(2t-2) = \sqrt{d}-(t-1)$ and we are back to a previous calculation. In other words, we obtain the sequence

$$\sqrt{d} \to_{(t-1)} \frac{\sqrt{d}+(t-1)}{2t-2} \to_1 \sqrt{d}+(t-1) \to_{(2t-2)} \frac{\sqrt{d}+(t-1)}{2t-2},$$

which produces the continued fraction $\sqrt{d} = \left\langle t-1, \overline{1, 2t-2} \right\rangle$.

(c) If $d = t^2+2$, then, following the same method as in parts (a) and (b), we obtain the sequence

$$\sqrt{d} \to_t \frac{\sqrt{d}+t}{2} \to_t \sqrt{d}+t \to_{2t} \frac{\sqrt{d}+t}{2},$$

which produces the continued fraction $\sqrt{d} = \left\langle t, \overline{t, 2t} \right\rangle$.

(d) If $d = t^2+t$, then we obtain the sequence

$$\sqrt{d} \to_t \frac{\sqrt{d}+t}{t} \to_2 \sqrt{d}+t \to_{2t} \frac{\sqrt{d}+t}{t},$$

which produces the continued fraction $\sqrt{d} = \left\langle t, \overline{2, 2t} \right\rangle$.

(4) Let n_i be the denominator of the i-th convergent of the continued fraction $\langle q_0, q_1, q_2, \ldots \rangle$. Since $n_{-2} = 1$ and $n_{-1} = 0$, we have that $n_0 = q_0(0)+1 = 1$ and $n_1 = q_1(1)+0 = q_1$. Thus $\langle q_1 \rangle = q_1 = \frac{n_1}{n_0}$. Suppose now that $\langle q_k, \ldots, q_1 \rangle = \frac{n_k}{n_{k-1}}$ for some $k \geq 1$. Then

$$\langle q_{k+1}, q_k, \ldots, q_1 \rangle = \langle q_{k+1}, \langle q_k, \ldots, q_1 \rangle \rangle = q_{k+1} + \frac{n_{k-1}}{n_k} = \frac{q_{k+1}n_k + n_{k-1}}{n_k} = \frac{n_{k+1}}{n_k},$$

which proves that $\langle q_i, \ldots, q_1 \rangle = \frac{n_i}{n_{i-1}}$ for all $i \geq 1$ by induction.

(5) $v = \langle 1, 1, 3, 1, v \rangle = \left\langle 1, 1, 3, \frac{v+1}{v} \right\rangle = \left\langle 1, 1, \frac{4v+3}{v+1} \right\rangle = \left\langle 1, \frac{5v+4}{4v+3} \right\rangle = \frac{9v+7}{5v+4}$. Thus v is the larger root of $f(x) = 5x^2 - 5x - 7$, that is, $v = \frac{5+\sqrt{165}}{10}$. We know that v is semi-reduced by Proposition 9.6.4, and then v is palindromic since $v + \overline{v} = \frac{5+\sqrt{165}}{10} + \frac{5-\sqrt{165}}{10} = 1$.

(6) $v = \langle 1, 2, 1, v \rangle = \left\langle 1, 2, \frac{v+1}{v} \right\rangle = \left\langle 1, \frac{3v+2}{v+1} \right\rangle = \frac{4v+3}{3v+2}$, and so v is the larger root of $f(x) = 3x^2 - 2x - 3$, that is, $v = \frac{1+\sqrt{10}}{3}$. Since $v + \overline{v} = \frac{1+\sqrt{10}}{3} + \frac{1-\sqrt{10}}{3} = \frac{2}{3}$ is not an integer, then v is not palindromic.

(7) Since v is reduced, then v is semi-reduced, and we have that $v = \langle \overline{q_0, q_1, \ldots, q_{\ell-1}} \rangle = \langle q_0, \overline{q_1, \ldots, q_{\ell-1}, q_0} \rangle$. As noted following Proposition 9.6.7, v is then palindromic if and only if the sequence $q_1, \ldots, q_{\ell-1}$ is a palindrome.

(8) Suppose that v is a semi-reduced number with minimum polynomial $f(x) = ax^2 + bx + c$. Then $v = \frac{-b+\sqrt{b^2-4ac}}{2a}$ and $\overline{v} = \frac{-b-\sqrt{b^2-4ac}}{2a}$, using the fact that a semi-reduced number is the larger root of its minimum polynomial. Then $v + \overline{v} = -\frac{b}{a}$ is an integer if and only if a divides b. We know that $g = \lfloor -\overline{v} \rfloor$ is the unique integer so that $g + v$ is reduced. But

$$g = \lfloor -\overline{v} \rfloor = \left\lfloor \frac{b+\sqrt{b^2-4ac}}{2a} \right\rfloor = \left\lfloor \frac{-b+\sqrt{b^2-4ac}}{2a} + \frac{b}{a} \right\rfloor = \left\lfloor v + \frac{b}{a} \right\rfloor = \lfloor v \rfloor + \frac{b}{a},$$

if $\frac{b}{a}$ is an integer.

(9) Let $v = \frac{3+\sqrt{30}}{3}$, the larger root of $f(x) = 3x^2 - 6x - 7$. From the sequence

$$\frac{3+\sqrt{30}}{3} \to_2 \frac{3+\sqrt{30}}{7} \to_1 \frac{4+\sqrt{30}}{2} \to_4 \frac{4+\sqrt{30}}{7} \to_1 \frac{3+\sqrt{30}}{3},$$

we find that $v = \left\langle \overline{2, 1, 4, 1} \right\rangle$. As noted in Exercise 7, this number is semi-reduced and palindromic. (We can verify this directly by noting that $v + \lfloor -\overline{v} \rfloor > 1$ and that $v + \overline{v}$ is an integer.)

(10) If $v = \langle -2, w\rangle$ where $w = \langle 1, 2, 3, 2, 1, 4, w\rangle$, we can calculate directly that $v = \frac{-44+\sqrt{880}}{11}$. Here $\lfloor -\overline{v}\rfloor = \left\lfloor \frac{44+\sqrt{880}}{11}\right\rfloor = 6$, so that $v + \lfloor -\overline{v}\rfloor = \frac{22+\sqrt{880}}{11} > 1$, and $v + \overline{v} = -8$ is an integer. Thus v is both semi-reduced and palindromic.

Section 10.1. Class Groups of Indefinite Quadratic Forms.

(1) For convenience, we combine the calculation of candidate forms and of equivalence classes of forms and ideals from Exercises 1 and 2 in each part below.

(2) (a) If $\Delta = 17$, then $\phi(x) = x^2 + x - 4$ and $u_\Delta = 2$. From the following table,

x	$-2, 1$	$-1, 0$
$\phi(x)$	-2	-4

we determine that $(\pm 1 : -2)$, $(\pm 2 : -2)$, and $(\pm 2 : -1)$ are candidate forms of discriminant 17. The equivalence algorithm of Theorem 10.1.2 applied to $(1 : -2)$ produces the following data.

i	0	1	2	3
a	1	2	2	1
k	-2	-2	-1	-2

So $(1 : -2) \sim (-2 : -2) \sim (2 : -1) \sim (-1 : -2) \sim (2 : -2) \sim (-2 : -1)$. All candidate forms are equivalent, and there is precisely one class of quadratic forms of discriminant 17. The same is true for ideals of discriminant 17.

(b) If $\Delta = 28$, then $\phi(x) = x^2 - 7$ and $u_\Delta = 2$. From the table,

x	± 2	± 1	0
$\phi(x)$	-3	-6	-7

we find the candidate forms $(\pm 1 : -2)$ and $(\pm 2 : -1)$. Applying the equivalence algorithm to $(1 : -2)$,

i	0	1	2	3	4
a	1	3	2	3	1
k	-2	-2	-1	-1	-2

we determine that $(1 : -2) \sim (2 : -1)$ and $(-1 : -2) \sim (-2 : -1)$, but that these two classes of quadratic forms are distinct. However, since $[1 : -2] = [-1 : -2]$, there is only one class of ideals of discriminant 28.

(c) If $\Delta = 33$, then $\phi(x) = x^2 + x - 8$ and $u_\Delta = 2$.

x	$-3, 2$	$-2, 1$	$-1, 0$
$\phi(x)$	-2	-6	-8

The candidate forms are $(\pm 1 : -3)$, $(\pm 2 : -3)$, and $(\pm 2 : -2)$. Applying the equivalence algorithm to $(1 : -3)$,

i	0	1	2	3	4
a	1	2	3	2	1
k	-3	-3	-2	-2	-3

we determine that $(1 : -3) \sim (-2 : -3) \sim (-2 : -2)$ and $(-1 : -3) \sim (2 : -3) \sim (2 : -2)$, with these two classes of quadratic forms distinct. There is only one class of ideals of discriminant 33.

(d) If $\Delta = 37$, then $\phi(x) = x^2 + x - 9$ and $u_\Delta = 3$.

x	$-3, 2$	$-2, 1$	$-1, 0$
$\phi(x)$	-3	-7	-9

The candidate forms are $(\pm 1 : -3)$, $(\pm 3 : -3)$, and $(\pm 3 : -1)$. Applying the equivalence algorithm to $(1 : -3)$,

i	0	1	2	3
a	1	3	3	1
k	-3	-3	-1	-3

we determine that all of these candidate forms are equivalent. There is only one class of quadratic forms, and one class of ideals of discriminant 37.

(e) If $\Delta = 57$, then $\phi(x) = x^2 + x - 14$ and $u_\Delta = 3$.

x	$-4, 3$	$-3, 2$	$-2, 1$	$-1, 0$
$\phi(x)$	-2	-8	-12	-14

The candidate forms are $(\pm 1 : -4)$, $(\pm 2 : -4)$, $(\pm 2 : -3)$, and $(\pm 3 : -2)$. Applying the equivalence algorithm to $(1 : -4)$,

i	0	1	2	3	4	5	6
a	1	2	4	3	4	2	1
k	-4	-4	-3	-2	-2	-3	-4

we determine that $(1 : -4) \sim (-2 : -4) \sim (-3 : -2) \sim (-2 : -3)$ and that $(-1 : -4) \sim (2 : -4) \sim (3 : -2) \sim (2 : -3)$. There are two classes of quadratic forms of discriminant 57, but only one class of ideals.

(f) If $\Delta = 65$, then $\phi(x) = x^2 + x - 16$ and $u_\Delta = 4$.

x	$-4, 3$	$-3, 2$	$-2, 1$	$-1, 0$
$\phi(x)$	-4	-10	-14	-16

The candidate forms are $(\pm 1 : -4)$, $(\pm 2 : -4)$, $(\pm 2 : -3)$, $(\pm 4 : -4)$, and $(\pm 4 : -1)$. Applying the equivalence algorithm to $(1 : -4)$,

i	0	1	2	3
a	1	4	4	1
k	-4	-4	-1	-4

we find that $(1 : -4) \sim (-4 : -4) \sim (4 : -1) \sim (-1 : -4) \sim (4 : -4) \sim (-4 : -1)$. Applying the same algorithm to $(2 : -4)$,

i	0	1	2	3
a	2	5	2	2
k	-4	-3	-3	-4

we $(2 : -4) \sim (2 : -3) \sim (-2 : -4) \sim (-2 : -3)$. Thus there are two distinct classes of quadratic forms of discriminant 65, and likewise two classes of ideals.

(g) If $\Delta = 88$, then $\phi(x) = x^2 - 22$ and $u_\Delta = 4$.

x	± 4	± 3	± 2	± 1	0
$\phi(x)$	-6	-13	-18	-21	-22

The candidate forms are $(\pm 1 : -4)$, $(\pm 2 : -4)$, $(\pm 3 : -4)$, and $(\pm 3 : -2)$. Applying the equivalence algorithm to $(1 : -4)$,

i	0	1	2	3	4	5	6
a	1	6	3	2	3	6	1
k	-4	-4	-2	-4	-4	-2	-4

we determine that $(1 : -4) \sim (3 : -2) \sim (-2 : -4) \sim (3 : -4)$ and that $(-1 : -4) \sim (-3 : -2) \sim (2 : -4) \sim (-3 : -4)$. There are two classes of quadratic forms of discriminant 88 and one class of ideals.

(h) If $\Delta = 93$, then $\phi(x) = x^2 + x - 23$ and $u_\Delta = 4$.

x	$-5, 4$	$-4, 3$	$-3, 2$	$-2, 1$	$-1, 0$
$\phi(x)$	-3	-11	-17	-21	-23

The only candidate forms are $(\pm 1 : -5)$ and $(\pm 3 : -5)$. From the equivalence algorithm applied to $(1 : -5)$,

i	0	1	2
a	1	3	1
k	-5	-5	-5

we see that $(1 : -5) \sim (-3 : -5)$ and $(-1 : -5) \sim (3 : -5)$. There are two classes of quadratic forms of discriminant 93 and one class of ideals.

(i) If $\Delta = 104$, then $\phi(x) = x^2 - 26$ and $u_\Delta = 5$.

x	± 5	± 4	± 3	± 2	± 1	0
$\phi(x) - 1$	-10	-17	-22	-25	-26	

The candidate forms are $(\pm 1 : -5)$, $(\pm 2 : -4)$, $(\pm 5 : -4)$, and $(\pm 5 : -1)$. Applying the equivalence algorithm to $(1 : -5)$ and to $(2 : -4)$,

i	0	1
a	1	1
k	-5	-5

i	0	1	2	3
a	2	5	5	2
k	-4	-4	-1	-4

we find that $(1 : -5) \sim (-1 : -5)$ and that $(2 : -4) \sim (-5 : -4) \sim (5 : -1) \sim (-2 : -4) \sim (5 : -4) \sim (-5 : -1)$. There are two classes of quadratic forms of discriminant 104 and two classes of ideals.

(j) If $\Delta = 152$, then $\phi(x) = x^2 - 38$ and $u_\Delta = 6$.

x	± 6	± 5	± 4	± 3	± 2	± 1	0
$\phi(x)$	-2	-13	-22	-29	-34	-37	-38

The only candidate forms are $(\pm 1 : -6)$ and $(\pm 2 : -6)$. Applying the equivalence algorithm to $(1 : -6)$,

i	0	1	2
a	1	2	1
k	-6	-6	-6

we see that $(1 : -6) \sim (-2 : -6)$ and that $(-1 : -6) \sim (2 : -6)$. There are two classes of quadratic forms of discriminant 152 and one class of ideals.

Section 10.2. Genera of Quadratic Forms and Ideals.

(1) (a) If $\Delta = 37$, then $\phi(x) = x^2 + x - 9$ and $u_\Delta = 3$. The only genus symbol defined for quadratic forms of discriminant 37 is $\left(\frac{f}{37}\right)$, which must equal 1. From the table

x	$-3, 2$	$-2, 1$	$-1, 0$
$\phi(x)$	-3	-7	-9

we find the candidate forms $(\pm 1 : -3)$, $(\pm 3 : -3)$, and $(\pm 3 : -1)$. Applying the equivalence algorithm to $(1 : -3)$,

i	0	1	2	3
a	1	3	3	1
k	-3	-3	-1	-3

we find that all of these forms are equivalent. So $\mathcal{F}_{37}$ has invariant factor type (1), containing only one class and only one genus. The same is true for the ideal class group $\mathcal{C}_{37}$.

(b) If $\Delta = 40$, then $\phi(x) = x^2 - 10$ and $u_\Delta = 3$. The defined genus symbols are $\left(\frac{2}{f}\right)$ and $\left(\frac{f}{5}\right)$, whose product equals 1.

x	± 3	± 2	± 1	0
$\phi(x)$	-1	-6	-9	-10

Candidate forms are $(\pm 1 : -3)$, $(\pm 2 : -2)$, $(\pm 3 : -2)$, and $(\pm 3 : -1)$. Applying the equivalence algorithm to $(1 : -3)$ and to $(2 : -2)$

i	0	1
a	1	1
k	-3	-3

i	0	1	2	3
a	2	3	3	2
k	-2	-2	-1	-2

we find that $(1 : -3) \sim (-1 : -3)$, with both forms in the genus for which $\left(\frac{2}{f}\right) = 1 = \left(\frac{f}{5}\right)$, and that $(2 : -2) \sim (-3 : -2) \sim (3 : -1) \sim (-2 : -2) \sim (3 : -2) \sim (-3 : -1)$, with each of these forms in the genus for which $\left(\frac{2}{f}\right) = -1 = \left(\frac{f}{5}\right)$. So $\mathcal{F}_{40}$ has invariant factor type (2), with two classes in two genera. The same is true for the ideal class group $\mathcal{C}_{40}$.

(c) If $\Delta = 61$, then $\phi(x) = x^2 + x - 15$ and $u_\Delta = 3$. The only genus symbol defined for quadratic forms of discriminant 61 is $\left(\frac{f}{61}\right)$. From the table

x	$-4, 3$	$-3, 2$	$-2, 1$	$-1, 0$
$\phi(x)$	-3	-9	-13	-15

we find the candidate forms $(\pm 1 : -4)$, $(\pm 3 : -4)$, and $(\pm 3 : -3)$. Applying the equivalence algorithm to $(1 : -4)$,

i	0	1	2	3
a	1	3	3	1
k	-4	-4	-3	-4

we find that all of these forms are equivalent. So $\mathcal{F}_{61}$ has invariant factor type (1), containing only one class and only one genus. The same is true for the ideal class group $\mathcal{C}_{61}$.

(d) If $\Delta = 92$, then $\phi(x) = x^2 - 23$ and $u_\Delta = 4$. The defined genus symbols are $\left(\frac{-1}{f}\right)$ and $\left(\frac{f}{23}\right)$.

x	±4	±3	±2	±1	0
$\phi(x)$	-7	-14	-19	-22	-23

Candidate forms are $(\pm1 : -4)$ and $(\pm2 : -3)$. Applying the equivalence algorithm to $(1 : -4)$

i	0	1	2	3	4
a	1	7	2	7	1
k	-4	-4	-3	-3	-4

we find that $(1 : -4) \sim (2 : -3)$ and $(-1 : -4) \sim (-2 : -3)$. The class of $(1 : -4)$ is in the genus for which $\left(\frac{-1}{f}\right) = 1 = \left(\frac{f}{23}\right)$, and the class of $(-1 : -4)$ is in the genus for which $\left(\frac{-1}{f}\right) = -1 = \left(\frac{f}{23}\right)$. So $\mathcal{F}_{92}$ has invariant factor type (2), with two classes in two genera. On the other hand, since $[1 : -4] = (-1 : -4)$, the ideal class group has only one element.

(e) If $\Delta = 93$, then the defined genus symbols are $\left(\frac{f}{3}\right)$ and $\left(\frac{f}{31}\right)$. In part (h) of Exercise 10.1.2, we found that $\mathcal{F}_{93}$ has two elements, represented by $(1 : -5)$ and $(-1 : -5)$. Both genus symbols equal 1 for the first form, and both equal -1 for the second. So $\mathcal{F}_{93}$ has invariant factor type (2) with two forms in two genera. But since $[1 : -5] = [-1 : -5]$, the ideal class group $\mathcal{C}_{93}$ has only one element.

(f) If $\Delta = 105$, then $\phi(x) = x^2 + x - 26$ and $u_\Delta = 5$. The defined genus symbols are $\left(\frac{f}{3}\right)$, $\left(\frac{f}{5}\right)$, and $\left(\frac{f}{7}\right)$, whose product equals 1. From the table

x	$-5, 4$	$-4, 3$	$-3, 2$	$-2, 1$	$-1, 0$
$\phi(x)$	-6	-14	-20	-24	-26

and the equivalence algorithm applied to $(1 : -5)$ and $(2 : -5)$

i	0	1	2	3	4	5	6
a	1	6	4	5	4	6	1
k	-5	-5	-2	-3	-3	-2	-5

i	0	1	2	3	4
a	2	7	2	3	2
k	-5	-4	-4	-5	-5

we determine that there are precisely four classes of quadratic forms, each in a separate genus, with symbols $\left(\frac{f}{3}\right)$, $\left(\frac{f}{5}\right)$, and $\left(\frac{f}{7}\right)$ as follows.

$$+++ : (1 : -5), \quad -+- : (-1 : -5), \quad --+ : (2 : -5), \quad +-- : (-2 : -5).$$

(For example, $(1 : -5) \sim (4 : -2) \sim (-5 : -3) \sim (4 : -3)$, listing only candidate forms here.) The form class group $\mathcal{F}_{105}$ has invariant factor type $(2, 2)$. On the other hand, since $[1 : -5] = [-1 : -5]$ and $[2 : -5] = [-2 : -5]$, the ideal class group $\mathcal{C}_{105}$ has only two elements and has invariant factor type (2).

(g) If $\Delta = 156$, then $\phi(x) = x^2 - 39$ and $u_\Delta = 6$. The defined genus symbols are $\left(\frac{-1}{f}\right)$, $\left(\frac{f}{3}\right)$, and $\left(\frac{f}{13}\right)$, written in that order below. From the table

x	±6	±5	±4	±3	±2	±1	0
$\phi(x)$	-3	-14	-23	-30	-35	-38	-39

and the equivalence algorithm applied to $(1 : -6)$ and $(2 : -5)$

i	0	1	2
a	1	3	1
k	-6	-6	-6

i	0	1	2	3	4	5	6
a	2	7	5	6	5	7	2
k	-5	-5	-2	-3	-3	-2	-5

we find four classes of quadratic forms, each in a separate genus as follows.

$$+++ : (1:-6), \quad --+ : (-1:-6), \quad +-- : (2:-5), \quad -+- : (-2:-5).$$

The form class group $\mathcal{F}_{156}$ has invariant factor type $(2,2)$, while the ideal class group $\mathcal{C}_{156}$ has invariant factor type (2).

(h) If $\Delta = 328$, then $\phi(x) = x^2 - 82$ and $u_\Delta = 9$, with genus symbols $\left(\frac{2}{f}\right)$ and $\left(\frac{f}{41}\right)$.

x	± 9	± 8	± 7	± 6	± 5	± 4	± 3	± 2	± 1	0
$\phi(x)$	-1	-18	-33	-46	-57	-66	-73	-78	-81	-82

From the following tables for the equivalence algorithm,

i	0	1
a	1	1
k	-9	-9

i	0	1	2	3
a	2	9	9	2
k	-8	-8	-1	-8

i	0	1	2	3
a	3	11	6	3
k	-8	-7	-4	-8

i	0	1	2	3
a	3	6	11	3
k	-7	-8	-4	-7

we find four classes of quadratic forms in two distinct genera.

$$++ : (1:-9), (2:-8) \qquad -- : (3:-8), (3:-7).$$

The form class group $\mathcal{F}_{328}$ and the ideal class group $\mathcal{C}_{328}$ both have invariant factor type (4). (For example, if $A = [3:-8]$, then $A^2 = [9:-8] \sim [2:-8]$ as we can see from the equivalence algorithm applied to $(2:-8)$. Then $A^3 \sim [6:-8] \sim [3:-7]$ and $A^4 \sim [1:-9]$.)

(i) If $\Delta = 440$, then $\phi(x) = x^2 - 110$ and $u_\Delta = 10$, with genus symbols $\left(\frac{-2}{f}\right)$, $\left(\frac{f}{5}\right)$, and $\left(\frac{f}{11}\right)$ (in that order below). From the following table,

x	± 10	± 9	± 8	± 7	± 6	± 5	± 4	± 3	± 2	± 1	0
$\phi(x)$	-10	-29	-46	-61	-74	-85	-94	-101	-106	-109	-110

we find candidate forms $(\pm 1 : -10)$, $(\pm 2 : -10)$, $(\pm 5 : -10)$, and $(\pm 10 : -10)$. The equivalence algorithm applied to $(1:-10)$ and $(2:-10)$,

i	0	1	2
a	1	10	1
k	-10	-10	-10

i	0	1	2
a	2	5	2
k	-10	-10	-10

shows that there are four classes of quadratic forms, each in a separate genus as follows.

$$+++ : (1:-10), \quad -+- : (-1:-10), \quad +-- : (2:-10), \quad --+ : (-2:-10).$$

The form class group $\mathcal{F}_{440}$ has invariant factor type $(2,2)$, while the ideal class group $\mathcal{C}_{440}$ has invariant factor type (2).

(j) If $\Delta = 568$, then $\phi(x) = x^2 - 142$ and $u_\Delta = 11$, with genus symbols $\left(\frac{-2}{f}\right)$ and $\left(\frac{f}{71}\right)$.

x	± 11	± 10	± 9	± 8	± 7	± 6	± 5	± 4	± 3	± 2	± 1	0
$\phi(x)$	-21	-42	-61	-78	-93	-106	-117	-126	-133	-138	-141	-142

From the following tables for the equivalence algorithm,

i	0	1	2	3	4
a	1	21	2	21	1
k	-11	-11	-10	-10	-11

i	0	1	2	3	4	5	6
a	3	14	9	13	6	7	3
k	-11	-10	-4	-5	-8	-10	-11

i	0	1	2	3	4	5	6
a	3	7	6	13	9	14	3
k	-10	-11	-10	-8	-5	-4	-10

we find six classes of quadratic forms in two distinct genera.

$++ : (1 : -11), (3 : -11), (3 : -10)$ $\qquad$ $-- : (-1 : -11), (-3 : -11), (-3 : -10)$.

The form class group $\mathcal{F}_{568}$ has invariant factor type (6), while the ideal class group $\mathcal{C}_{568}$ has invariant factor type (3). (Note that $(-3 : -11) \cdot (-3 : -11) \sim (9 : -5) \sim (3 : -10)$, as shown in the third application of the equivalence algorithm above. Then $(-3 : -11) \cdot (3 : -10) \sim (-1 : -11)$ and so forth, showing that $f = (-3 : -11)$ generates $\mathcal{F}_{568}$.)

Section 10.3. Continued Fractions of Irrational Quadratic Numbers.

(1) (a) $v = \sqrt{41}$ is the larger root of $x^2 - 41$, with discriminant $\Delta = 164$. Since $41 \equiv 1 \pmod 4$,the principal polynomial of discriminant 164 is $\phi(x) = x^2 + 2x - 40$, with smaller root $w = -1 - \sqrt{41} \approx -7.4$. We can calculate the following values of $\phi(x)$.

x	$-7,5$	$-6,4$	$-5,3$	$-4,2$	$-3,1$	$-2,0$	-1
$\phi(x)$	-5	-16	-25	-32	-37	-40	-41

To find the continued fraction of $\sqrt{41}$, we apply the quadratic continued fraction algorithm with $a_0 = 1$ and $k_0 = \frac{b-\varepsilon}{2} = -1$. The smallest $k_1 > w$ that satisfies $k_1 \equiv -k_0 - \varepsilon \pmod{a_0}$ is $k_1 = -7$, and then $a_1 = -\frac{\phi(k_1)}{a_0} = 5$. Now the smallest $k_2 > w$ with $k_2 \equiv -k_1 - \varepsilon \pmod{a_1}$ is $k_2 = -5$, and $a_2 = -\frac{\phi(k_2)}{a_1} = 5$. Continuing in this way, we find eventually that $a_4 = a_1$ and $k_4 = k_1$. Now $q_0 = -\frac{k_0+k_1+\varepsilon}{a_0} = -\frac{-1-7+2}{1} = 6$, then $q_1 = -\frac{k_1+k_2+\varepsilon}{a_1} = -\frac{-7-5+2}{5} = 2$ and so forth. The following table summarizes these calculations and shows that $\sqrt{41} = \langle 6, \overline{2, 2, 12} \rangle$.

i	0	1	2	3	4
a	1	5	5	1	5
k	-1	-7	-5	-7	-7
q	6	2	2	12	

(b) $v = \sqrt{43}$ has minimum polynomial $x^2 - 43$, which is also the principal polynomial of discriminant $\Delta = 4 \cdot 43 = 172$. The smaller root of $\phi(x)$ is $w = -\sqrt{43} \approx -6.6$, and we calculate the following values of $\phi(x)$.

x	± 6	± 5	± 4	± 3	± 2	± 1	0
$\phi(x)$	-7	-18	-27	-34	-39	-42	-43

Applying the quadratic continued fraction algorithm with $a_0 = 1$ and $k_0 = 0$, we obtain the following data.

i	0	1	2	3	4	5	6	7	8	9	10	11
a	1	7	6	3	9	2	9	3	6	7	1	7
k	0	-6	-1	-5	-4	-5	-5	-4	-5	-1	-6	-6
q	6	1	1	3	1	5	1	3	1	1	12	

Thus $\sqrt{43} = \langle 6, \overline{1, 1, 3, 1, 5, 1, 3, 1, 1, 12} \rangle$.

(c) Since $53 \equiv 1 \pmod 4$, we apply the quadratic continued fraction algorithm to $a_0 = 1$ and $k_0 = -1$, with the following values of $\phi(x) = x^2 + 2x - 52$.

x	$-8,6$	$-7,5$	$-6,4$	$-5,3$	$-4,2$	$-3,1$	$-2,0$	-1
$\phi(x)$	-4	-17	-28	-37	-44	-49	-52	-53

From the following data,

i	0	1	2	3	4	5	6
a	1	4	7	7	4	1	4
k	-1	-8	-6	-3	-6	-8	-8
q	7	3	1	1	3	14	

we conclude that $\sqrt{53} = \langle 7, \overline{3, 1, 1, 3, 14} \rangle$.

(d) For $v = \sqrt{89}$, with $\phi(x) = x^2 + 2x - 88$ having smaller root $w = -1 - \sqrt{89} \approx -10.4$, we obtain the following data from the quadratic continued fraction algorithm

i	0	1	2	3	4	5	6
a	1	8	5	5	8	1	8
k	-1	-10	-8	-9	-8	-10	-10
q	9	2	3	3	2	18	

and conclude that $\sqrt{89} = \langle 9, \overline{2, 3, 3, 2, 18} \rangle$.

(e) For $v = \sqrt{97}$, with $\phi(x) = x^2 + 2x - 96$ having smaller root $w = -1 - \sqrt{97} \approx -10.8$, the quadratic continued fraction algorithm

i	0	1	2	3	4	5	6	7	8	9	10	11	12
a	1	16	3	11	8	9	9	8	11	3	16	1	16
k	-1	-10	-8	-9	-4	-6	-5	-6	-4	-9	-8	-10	-10
q	9	1	5	1	1	1	1	1	1	5	1	18	

shows that $\sqrt{97} = \langle 9, \overline{1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18} \rangle$.

(f) For $v = \sqrt{111}$, with $\phi(x) = x^2 - 111$, we obtain the following data from the quadratic continued fraction algorithm

i	0	1	2	3	4	5	6	7
a	1	11	10	3	10	11	1	11
k	0	-10	-1	-9	-9	-1	-10	-10
q	10	1	1	6	1	1	20	

which shows that $\sqrt{111} = \langle 10, \overline{1, 1, 1, 6, 1, 1, 20} \rangle$.

(2) (a) $v = 3 + \sqrt{23}$ and $\overline{v} = 3 - \sqrt{23}$ are roots of the minimum polynomial $f(x) = x^2 - 6x - 14$, with discriminant $\Delta = 92 = \Delta(23, 1)$. The principal polynomial of discriminant 92 is $\phi(x) = x^2 - 23$. To find the continued fraction of v we apply the quadratic continued fraction algorithm with $a_0 = 1$ and $k_0 = \frac{b - \varepsilon}{2} = -3$.

i	0	1	2	3	4	5
a	1	7	2	7	1	7
k	-3	-4	-3	-3	-4	-4
q	7	1	3	1	8	

Since $a_5 = a_1$ and $k_5 = k_1$, we conclude that $v = \langle 7, \overline{1,3,1,8} \rangle$. For $\overline{v}$, we start the same algorithm with $a_0 = -1$ and $k_0 = 3$.

i	0	1	2	3	4	5	6
a	-1	2	7	1	7	2	7
k	3	-5	-3	-4	-4	-3	-3
q	-2	4	1	8	1	3	

Here since a_0 is negative, we select k_1 to be the largest integer less than $w = -\sqrt{23}$ with $k_1 \equiv -3 \pmod 1$, that is, $k_1 = -5$. Now $a_1 = -\frac{\phi(-5)}{-1} = 2$ is positive, so we select k_2 to be the smallest integer greater than w with $k_2 \equiv 5 \pmod 2$, that is, $k_2 = -3$. Continuing the algorithm in this way, we find that $a_6 = a_2$ and $k_6 = k_2$, and conclude that $\overline{v} = \langle -2, 4, \overline{1,8,1,3} \rangle$.

(b) The minimum polynomial of $v = \frac{3+\sqrt{17}}{5}$ and $\overline{v} = \frac{3-\sqrt{17}}{5}$ is $f(x) = 25x^2 - 30x - 8$. The discriminant of $f(x)$ is $\Delta = 1700 = \Delta(17, 10)$, so that $\phi(x) = x^2 + 10x - 400$. For v, we apply the quadratic continued fraction algorithm with $a_0 = 25$ and $k_0 = \frac{-30-10}{2} = -20$. For $\overline{v}$, we apply the same algorithm with $a_0 = -2$ and $k_0 = \frac{30-10}{2} = 10$.

i	0	1	2	3	4	5	6	7
a	25	13	13	25	8	17	8	25
k	-20	-15	-21	-15	-20	-22	-22	-20
q	1	2	2	1	4	2	4	

Here $k_1 = -15$ is the smallest integer greater than $w = \frac{-10-\sqrt{1700}}{2} \approx -25.6$ that is congruent to $-k_0 - \varepsilon = 10$ modulo $a_0 = 25$. Note that $q_0 = -\frac{k_0+k_1+\varepsilon}{a_0} = -\frac{-20-15+10}{25} = 1$, and so forth. Since $a_7 = a_0$ and $k_7 = k_0$, then $v = \langle \overline{1,2,2,1,4,2,4} \rangle$. For $\overline{v}$, we apply the same algorithm with $a_0 = -2$ and $k_0 = \frac{30-10}{2} = 10$.

i	0	1	2	3	4	5	6	7	8	9	10
a	-25	47	8	17	8	25	13	13	25	8	17
k	10	-45	-12	-22	-22	-20	-15	-21	-15	-20	-22
q	-1	2	3	2	4	1	2	2	1	4	

In this case, $k_1 = -45$ is the largest integer less than w congruent to $-k_0 - \varepsilon = -20$ modulo 25. So $a_1 = -\frac{\phi(-45)}{-25} = 47$ and now $k_2 = -12$ is the smallest integer greater than w congruent to $-k_1 - \varepsilon = 35$ modulo 47. Continuing in this way, we obtain $a_{10} = a_3$ and $k_{10} = k_3$, and conclude that $\overline{v} = \langle -1, 1, 3, \overline{2,4,1,2,2,1,4} \rangle$.

(c) $v = \frac{-5+2\sqrt{13}}{3}$ and $\overline{v} = \frac{-5-2\sqrt{13}}{3}$ have minimum polynomial $f(x) = 3x^2 + 10x - 9$. The discriminant of $f(x)$ is $\Delta = 208 = \Delta(13, 4)$, so that $\phi(x) = x^2 + 4x - 48$. For v, we apply the quadratic continued fraction algorithm with $a_0 = 3$ and $k_0 = \frac{10-4}{2} = 3$.

i	0	1	2	3	4	5	6	7
a	3	9	4	9	3	1	3	9
k	3	-7	-6	-6	-7	-9	-9	-7
q	0	1	2	1	4	14	4	

We conclude that $v = \langle 0, \overline{1,2,1,4,14,4} \rangle$. For $\overline{v}$, we begin the algorithm with $a_0 = -3$ and $k_0 = \frac{-10-4}{2} = -7$.

i	0	1	2	3	4	5	6	7	8	9
a	-3	16	1	3	9	4	9	3	1	3
k	-7	-12	-8	-9	-7	-6	-6	-7	-9	-9
q	-5	1	13	4	1	2	1	4	14	

We find that $\overline{v} = \langle -5, 1, 13, \overline{4,1,2,1,4,14} \rangle$.

(d) $v = 13 + 4\sqrt{113}$ and $\overline{v} = 13 - 4\sqrt{113}$ have minimum polynomial $f(x) = x^2 - 26x - 7$. The discriminant of $f(x)$ is $\Delta = 704 = \Delta(11, 4)$, and $\phi(x) = x^2 - 176$. For v, we apply the quadratic continued fraction algorithm with $a_0 = 1$ and $k_0 = \frac{-26-0}{2} = -13$, and conclude from the following data that $v = \langle \overline{26,3,1,3} \rangle$.

i	0	1	2	3	4
a	1	7	16	7	1
k	-13	-13	-8	-8	-13
q	26	3	1	3	

For $\overline{v}$, we begin the algorithm with $a_0 = -1$ and $k_0 = 13$, and find that $\overline{v} = \langle -1, 1, 2, \overline{1,3,26,3} \rangle$.

i	0	1	2	3	4	5	6	7
a	-1	20	7	16	7	1	7	16
k	13	-14	-6	-8	-8	-13	-13	-8
q	-1	1	2	1	3	26	3	

(3) (a) $v = 1 + \sqrt{94}$ is the larger root of $f(x) = x^2 - 2x - 93$, with discriminant $\Delta = 376 = \Delta(94, 1)$. We compile the following values of $\phi(x) = x^2 - 94$, the principal polynomial of discriminant 376.

x	± 9	± 8	± 7	± 6	± 5	± 4	± 3	± 2	± 1	0
$\phi(x)$	-13	-30	-45	-58	-69	-78	-85	-90	-93	-94

Applying the quadratic continued fraction algorithm with $a_0 = 1$ and $k_0 = \frac{-2-0}{2} = -1$ yields the following data.

i	0	1	2	3	4	5	6	7	8	9
a	1	13	6	5	9	10	3	15	2	15
k	-1	-9	-4	-8	-7	-2	-8	-7	-8	-8
q	10	1	2	3	1	1	5	1	8	1

i	10	11	12	13	14	15	16	17
a	3	10	9	5	6	13	1	13
k	-7	-8	-2	-7	-8	-4	-9	-9
q	5	1	1	3	2	1	18	

We obtain the first repetition with $a_{17} = a_1$ and $k_{17} = k_1$, and thus conclude that $v = \langle 10, \overline{1,2,3,1,1,5,1,8,1,5,1,1,3,2,1,18} \rangle$.

(b) $v = \frac{5-\sqrt{114}}{3}$ is the smaller root of $f(x) = 9x^2 - 30x - 89$, with discriminant $\Delta = 4104 = \Delta(114, 3)$. We apply the quadratic continued fraction algorithm with $\phi(x) = x^2 - 1026$,

$a_0 = -9$, and $k_0 = \frac{30-0}{2} = 15$.

i	0	1	2	3	4	5	6	7	8
a	-9	7	18	25	14	9	50	7	18
k	15	-33	-30	-24	-26	-30	-24	-26	-30
q	-2	9	3	2	4	6	1	8	

Here $k_1 = -33$ is the largest integer smaller than $w = -\sqrt{1026} \approx -32.03$ congruent to $-k_0 - \varepsilon = -15$ modulo 9. Then $a_1 = -\frac{\phi(-33)}{-9} = 7$ and $k_2 = -30$ is the smallest integer greater than w congruent to $-k_1 - \varepsilon = 33$ modulo 7. Continuing in this way, we find that $a_8 = a_2$ and $k_8 = k_2$, and conclude that $v = \left\langle -2, 9, \overline{3, 2, 4, 6, 1, 8} \right\rangle$.

(c) $v = \frac{-4+\sqrt{65}}{2}$ is the larger root of $f(x) = 4x^2 + 16x - 49$, with discriminant $\Delta = 1040 = \Delta(65, 4)$. So $\phi(x) = x^2 + 4x - 256$, and we apply the quadratic continued fraction algorithm with $a_0 = 4$ and $k_0 = \frac{16-4}{2} = 6$. The following data

i	0	1	2	3
a	4	1	4	1
k	6	-18	-18	-18
q	2	32	8	

shows that $v = \left\langle 2, \overline{32, 8} \right\rangle$.

(d) $v = \frac{3+\sqrt{67}}{2}$ is the larger root of $f(x) = 2x^2 - 6x - 29$, with discriminant $\Delta = 268 = \Delta(67, 1)$. We compile the following values of $\phi(x) = x^2 - 67$, the principal polynomial of discriminant 268.

x	± 8	± 7	± 6	± 5	± 4	± 3	± 2	± 1	0
$\phi(x)$	-3	-18	-31	-42	-51	-58	-63	-66	-67

Applying the quadratic continued fraction algorithm with $a_0 = 2$ and $k_0 = -3$ yields the following data.

i	0	1	2	3	4	5	6	7	8	9	10	11
a	2	9	7	6	3	1	3	6	7	9	2	9
k	-3	-7	-2	-5	-7	-8	-8	-7	-5	-2	-7	-7
q	5	1	1	2	5	16	5	2	1	1	7	

Since $a_{11} = a_1$ and $k_{11} = k_1$, we have $v = \left\langle 5, \overline{1, 1, 2, 5, 16, 5, 2, 1, 1, 7} \right\rangle$.

(e) $v = \frac{4-\sqrt{83}}{7}$ is the smaller root of $f(x) = 49x^2 - 56x - 67$, with discriminant $\Delta = 16268 = \Delta(83, 7)$. Applying the quadratic continued fraction algorithm with $\phi(x) = x^2 - 4067$, and with $a_0 = -49$ and $k_0 = 28$, we obtain the following data.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13
a	-49	38	71	41	43	61	58	49	2	49	58	61	43	41
k	28	-77	-37	-34	-48	-38	-23	-35	-63	-63	-35	-23	-38	-48
q	-1	3	1	2	2	1	1	2	63	2	1	1	2	2

i	14	15	16	17	18	19	20	21	22	23	24	25	26
a	71	38	67	49	74	17	98	17	74	49	67	38	71
k	-34	-37	-39	-28	-21	-53	-49	-49	-53	-21	-28	-39	-37
q	1	2	1	1	1	6	1	6	1	1	1	2	

The first repetition occurs with $a_{26} = a_2$ and $k_{26} = k_2$, so that

$$v = \left\langle -1, 3, \overline{1, 2, 2, 1, 1, 2, 63, 2, 1, 1, 2, 2, 1, 2, 1, 1, 1, 6, 1, 6, 1, 1, 1, 2} \right\rangle.$$

(f) $v = \frac{-7+\sqrt{113}}{4}$ is the larger root of $f(x) = 2x^2 + 7x - 8$, with discriminant $\Delta = 113$. Using the following values of $\phi(x) = x^2 + x - 28$,

x	$-5, 4$	$-4, 3$	$-3, 2$	$-2, 1$	$-1, 0$
$\phi(x)$	-8	-16	-22	-26	-28

we apply the quadratic continued fraction algorithm with $a_0 = 2$ and $k_0 = \frac{7-1}{2} = 3$.

i	0	1	2	3	4	5	6	7	8
a	2	8	1	8	2	4	4	2	8
k	3	-4	-5	-5	-4	-5	-4	-5	-4
q	0	1	9	1	4	2	2	4	

We conclude that $v = \langle 0, \overline{1, 9, 1, 4, 2, 2, 4} \rangle$.

Section 10.4. Equivalence of Indefinite Quadratic Forms.

(1) For each i, write $\phi(k_i) = -a_i \cdot -c_i$ and $\phi'(k_i) = b_i$. If $\overline{U_i} = \begin{bmatrix} q_i & 1 \\ -1 & 0 \end{bmatrix}$ and we let $(-a_i : k_i) \circ \overline{U_i} = (m : \ell)$, then

$$m = -a_i(q_i)^2 + b_i q_i(-1) - c_i(-1)^2 = -a_i q_i^2 - b_i q_i - c_i$$

and

$$\ell = -a_i(q_i)(1) + b_i(1)(-1) - c_i(-1)(0) + k_i = -a_i q_i - k_i - \varepsilon = k_{i+1},$$

using the fact that $b_i = 2k_i + \varepsilon$ along with equation (10.3.2). From equation (10.3.3), we have that

$$\phi(k_{i+1}) = a_i(a_i q_i^2 + b_i q_i + c_i) = -a_i(-a_i q_i^2 - b_i q_i - c_i) = -a_i m.$$

But then by equation (10.3.1), $a_{i+1} = -\frac{\phi(k_{i+1})}{a_i} = m$, and so $(-a_i : k_i) \circ \overline{U_i} = (a_{i+1} : k_{i+1})$.

(2) If i is odd, then

$$W_i\overline{U_i} = \begin{bmatrix} m_{i-1} & -m_{i-2} \\ n_{i-1} & -n_{i-2} \end{bmatrix} \cdot \begin{bmatrix} q_i & 1 \\ -1 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} m_{i-1}q_i + m_{i-2} & m_{i-1} \\ n_{i-1}q_i + n_{i-2} & n_{i-1} \end{bmatrix} = \begin{bmatrix} m_i & m_{i-1} \\ n_i & n_{i-1} \end{bmatrix} = W_{i+1}$$

since $i + 1$ is even.

(3) By definition of the numerator and denominator sequences, we have that

$$W_0 = \begin{bmatrix} m_{-1} & m_{-2} \\ n_{-1} & n_{-2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad W_1 = \begin{bmatrix} m_0 & -m_{-1} \\ n_0 & -n_{-1} \end{bmatrix} = \begin{bmatrix} q_0 & -1 \\ 1 & 0 \end{bmatrix} = U_0.$$

Now $W_2 = W_1 \cdot \overline{U_1} = U_0 \cdot \overline{U_1}$ by Exercise 2, then $W_3 = W_2 \cdot U_2 = U_0 \cdot \overline{U_1} \cdot U_2$ as in the proof of Theorem 10.4.2, and so forth. We obtain the general expression for W_t as claimed.

Section 11.1. The Continued Fraction of a Quadratic Form.

(1) For $1 \le r \le 20$, the following are the values of $\frac{q}{r}$ that are closest to $\sqrt{2}$ in absolute value.

$$\tfrac{1}{1}, \tfrac{3}{2}, \tfrac{4}{3}, \tfrac{6}{4}, \tfrac{7}{5}, \tfrac{8}{6}, \tfrac{10}{7}, \tfrac{11}{8}, \tfrac{13}{9}, \tfrac{14}{10}, \tfrac{16}{11}, \tfrac{17}{12}, \tfrac{18}{13}, \tfrac{20}{14}, \tfrac{21}{15}, \tfrac{23}{16}, \tfrac{24}{17}, \tfrac{25}{18}, \tfrac{27}{19}, \tfrac{28}{20}.$$

Direct calculation shows that $|\frac{q}{r} - \sqrt{2}| < \frac{1}{2r^2}$ only for the following fractions in this list: $\frac{1}{1}$, $\frac{2}{3}$, $\frac{7}{5}$, and $\frac{17}{12}$. The continued fraction of $\sqrt{2}$ is $\langle 1, \overline{2} \rangle$, and the following table shows that each value listed above is a convergent of this continued fraction.

i	0	1	2	3	4
q	1	2	2	2	2
m	1	3	7	17	41
n	1	2	5	12	29

(2) For $1 \le r \le 20$, the following are the values of $\frac{q}{r}$ that are closest to $\sqrt{3}$ in absolute value.

$$\tfrac{2}{1}, \tfrac{3}{2}, \tfrac{5}{3}, \tfrac{7}{4}, \tfrac{9}{5}, \tfrac{10}{6}, \tfrac{12}{7}, \tfrac{14}{8}, \tfrac{16}{9}, \tfrac{17}{10}, \tfrac{19}{11}, \tfrac{21}{12}, \tfrac{23}{13}, \tfrac{24}{14}, \tfrac{26}{15}, \tfrac{28}{16}, \tfrac{29}{17}, \tfrac{31}{18}, \tfrac{33}{19}, \tfrac{35}{20}.$$

Here $|\frac{q}{r} - \sqrt{3}| < \frac{1}{2r^2}$ only for the following fractions in this list: $\frac{2}{1}$, $\frac{7}{4}$, and $\frac{26}{15}$. The continued fraction of $\sqrt{3}$ is $\langle 1, \overline{1, 2} \rangle$, and we verify by the following table that each value listed above is a convergent of this continued fraction.

i	0	1	2	3	4	5
q	1	1	2	1	2	1
m	1	2	5	7	19	26
n	1	1	3	4	11	15

(Note that not all convergents satisfy this condition however. For instance, we find that $|\frac{19}{11} - \sqrt{3}| \approx 0.0048$ while $\frac{1}{2 \cdot 11^2} \approx 0.0041$.)

Section 11.2. Units and Automorphs.

(1) Suppose that $u = q + rz \neq \pm 1$ is a unit in $D = D_\Delta$ for some positive discriminant Δ. With $-u$, u^{-1}, and $-u^{-1}$ also units, we can assume that $u > 1$. Since $N(u) = u\overline{u} = \pm 1$, either u^{-1} or $-u^{-1}$ equals $\overline{u}$. In any case, we can assume that $q + rz > q + r\overline{z}$, which implies that $r\sqrt{\Delta}$ is positive. ($(q + rz) - (q + r\overline{z}) = r(z - \overline{z}) = r\sqrt{\Delta}$ in every case.) Likewise, $q + rz > -q - r\overline{z}$, implying that $2q + \varepsilon r > 0$. Since $\sqrt{\Delta}$ and ε are positive for every discriminant $\Delta > 0$, it follows that q and r must both be positive. There are finitely many elements $s + tz < u$ with s and t both positive, and so there must be a smallest unit $u > 1$ in D (assuming again that there is at least one such unit).

(2) Suppose that $D = D_\Delta$ has a unit $u > 1$ and that u is the smallest such unit. Let v be some unit of D, and assume that $v > 1$. (We can replace v by $-v$, v^{-1}, or $-v^{-1}$ if not.) If $u > 1$ then the positive integer powers of u get arbitrarily large, so there must be some positive integer n so that $u^n \le v < u^{n+1}$. But now $1 \le u^{-n}v < u$, and $u^{-n}v$ is a unit of D since its norm is ± 1. We must conclude that $u^{-n}v = 1$, that is, $v = u^n$, to avoid contradicting the definition of u. Including negatives and inverses of these units, together with ± 1, we then see that every unit of D must be equal to $\pm u^n$ for some integer n.

(3) In each part, we calculate the fundamental unit of D_Δ by applying the equivalence algorithm to $(1 : 0)$, the principal form of discriminant Δ.

(a) For $\Delta = 21$, with principal polynomial $\phi(x) = x^2 + x - 5$ and basis element $z = \frac{1+\sqrt{21}}{2}$, we obtain the following data.

i	0	1	2	3
a	1	3	1	3
k	0	-2	-2	-2
q	1	1	3	
m	1	2		
n	1	1		

We conclude that the fundamental unit of D_{21} is $2+z=\frac{5+\sqrt{21}}{2}$.

(b) For $\Delta=37$, with $\phi(x)=x^2+x-8$ and $z=\frac{1+\sqrt{37}}{2}$, we find from the table

i	0	1	2	3	4
a	1	3	3	1	3
k	0	-3	-1	-3	-3
q	2	1	1	5	
m	2	3	5		
n	1	1	2		

that the fundamental unit of D_{37} is $5+2z=6+\sqrt{37}$.

(c) For $\Delta=40$, with $\phi(x)=x^2-10$ and $z=\sqrt{10}$:

i	0	1	2
a	1	1	1
k	0	-3	-3
q	3	6	
m	3		
n	1		

The fundamental unit of D_{40} is $3+z=3+\sqrt{10}$.

(d) For $\Delta=41$, with $\phi(x)=x^2+x-10$ and $z=\frac{1+\sqrt{41}}{2}$:

i	0	1	2	3	4	5	6
a	1	4	2	2	4	1	4
k	0	-3	-2	-3	-2	-3	-3
q	2	1	2	2	1	5	
m	2	3	8	19	27		
n	1	1	3	7	10		

The fundamental unit of D_{41} is $27+10z=32+5\sqrt{41}$.

(e) For $\Delta=53$, with $\phi(x)=x^2+x-13$ and $z=\frac{1+\sqrt{53}}{2}$:

i	0	1	2
a	1	1	1
k	0	-4	-4
q	3	7	
m	3		
n	1		

The fundamental unit of D_{53} is $3+z=\frac{7+\sqrt{53}}{2}$.

(f) For $\Delta=76$, with $\phi(x)=x^2-19$ and $z=\sqrt{19}$:

i	0	1	2	3	4	5	6	7
a	1	3	5	2	5	3	1	3
k	0	-4	-2	-3	-3	-2	-4	-4
q	4	2	1	3	1	2	8	
m	4	9	13	48	61	170		
n	1	2	3	11	14	39		

The fundamental unit of D_{76} is $170+39z=170+39\sqrt{19}$.

(g) For $\Delta = 92$, with $\phi(x) = x^2 - 23$ and $z = \sqrt{23}$:

i	0	1	2	3	4	5
a	1	7	2	7	1	7
k	0	-4	-3	-3	-4	-4
q	4	1	3	1	8	
m	4	5	10	24		
n	1	1	4	5		

The fundamental unit of D_{92} is $24 + 5z = 24 + 5\sqrt{23}$.

(h) For $\Delta = 104$, with $\phi(x) = x^2 - 26$ and $z = \sqrt{26}$:

i	0	1	2
a	1	1	1
k	0	-5	-5
q	5	10	
m	5		
n	1		

The fundamental unit of D_{104} is $5 + z = 5 + \sqrt{26}$.

(i) For $\Delta = 232$, with $\phi(x) = x^2 - 58$ and $z = \sqrt{58}$:

i	0	1	2	3	4	5	6	7	8
a	1	9	6	7	7	6	9	1	9
k	0	-7	-2	-4	-3	-4	-2	-7	-7
q	7	1	1	1	1	1	1	14	
m	7	8	15	23	38	61	99		
n	1	1	2	3	5	8	13		

The fundamental unit of D_{232} is $99 + 13z = 19 + 13\sqrt{58}$.

(j) For $\Delta = 276$, with $\phi(x) = x^2 - 69$ and $z = \sqrt{69}$:

i	0	1	2	3	4	5	6	7	8	9
a	1	5	4	11	3	11	4	5	1	5
k	0	-8	-7	-5	-6	-6	-5	-7	-8	-8
q	8	3	3	1	4	1	3	3	16	
m	8	25	83	108	515	623	2384	7775		
n	1	3	10	13	62	75	287	936		

The fundamental unit of D_{276} is $7775 + 936z = 7775 + 936\sqrt{69}$.

(4) We determined a collection of class representatives for quadratic forms of each discriminant Δ in Exercise 10.2.1. The tables compiled in that exercise are extended below, with Theorem 11.2.2 applied to construct a generator U for the group of automorphs for each representative (that is, so that $\mathrm{Aut}(f) = \{\pm U^n \mid n \in \mathbb{Z}\}$).

(a) Each element of $\mathcal{F}_{37}$ is equivalent to $f = (1 : -3)$. Using $\phi(x) = x^2 + x - 9$, we obtain the following data from the equivalence/continued fraction algorithm applied to this form.

i	0	1	2	3	4	5	6
a	1	3	3	1	3	3	1
k	-3	-3	-1	-3	-3	-1	-3
q	5	1	1	5	1	1	
m	5	6	11	61	72	133	
n	1	1	2	11	13	24	

We conclude that $\mathrm{Aut}(f) = \{\pm U^n \mid n \in \mathbb{Z}\}$ for $U = \begin{bmatrix} 133 & 72 \\ 24 & 13 \end{bmatrix}$.

(b) Each form in $\mathcal{F}_{40}$ is equivalent to $f = (1 : -3)$ or to $g = (2 : -2)$. With $\phi(x) = x^2 - 10$, we compile the following data.

i	0	1	1
a	1	1	1
k	-3	-3	-3
q	6	6	6
m	6	37	
n	1	6	

i	0	1	2	3	4	5	6
a	2	3	3	2	3	3	2
k	-2	-2	-1	-2	-2	-1	-2
q	2	1	1	2	1	1	
m	2	3	5	13	18	31	
n	1	1	2	5	7	12	

So $U = \begin{bmatrix} 37 & 6 \\ 6 & 1 \end{bmatrix}$ and $V = \begin{bmatrix} 31 & 18 \\ 12 & 7 \end{bmatrix}$ are generating automorphs of f and of g respectively.

(c) Each form in $\mathcal{F}_{61}$ is equivalent to $f = (1 : -4)$. With $\phi(x) = x^2 + x - 15$, the following data

i	0	1	2	3	4	5	6
a	1	3	3	1	3	3	1
k	-4	-4	-3	-4	-4	-3	-4
q	7	2	2	7	2	2	
m	7	15	37	274	585	1444	
n	1	2	5	37	79	195	

shows that $\mathrm{Aut}(f) = \{\pm U^n \mid n \in \mathbb{Z}\}$ for $U = \begin{bmatrix} 1444 & 585 \\ 195 & 79 \end{bmatrix}$.

(d) Each form in $\mathcal{F}_{92}$ is equivalent to $f = (1 : -4)$ or to $-\overline{f} = (-1 : -4)$. Using $\phi(x) = x^2 - 23$, we compile the following data.

i	0	1	2	3	4
a	1	7	2	7	1
k	-4	-4	-3	-3	-4
q	8	1	3	1	
m	8	9	35	44	
n	1	1	4	5	

By Theorem 11.2.2, $U = \begin{bmatrix} 44 & 35 \\ 5 & 4 \end{bmatrix}$ and $\overline{U} = \begin{bmatrix} 44 & -35 \\ -5 & 4 \end{bmatrix}$ are generating automorphs for f and for $-\overline{f}$ respectively.

(e) Each form in $\mathcal{F}_{93}$ is equivalent to $f = (1 : -5)$ or to $-\overline{f} = (-1 : -4)$. With $\phi(x) = x^2 + x - 23$, we compile the following data

i	0	1	2
a	1	3	1
k	-5	-5	-5
q	9	3	
m	9	28	
n	1	3	

which shows that $U = \begin{bmatrix} 28 & 9 \\ 3 & 1 \end{bmatrix}$ and $\overline{U} = \begin{bmatrix} 28 & -9 \\ -3 & 1 \end{bmatrix}$ are generating automorphs for f and for $-\overline{f}$ respectively.

(f) Each form in $\mathcal{F}_{105}$ is equivalent to $f = (1 : -5)$, to $-\overline{f} = (-1 : -5)$, to $g = (2 : -5)$, or to $-\overline{g} = (-2 : -5)$. With $\phi(x) = x^2 + x - 26$, we compile the following tables.

i	0	1	2	3	4	5	6
a	1	6	4	5	4	6	1
k	-5	-5	-2	-3	-3	-2	-5
q	9	1	1	1	1	1	
m	9	10	19	29	48	77	
n	1	1	2	3	5	8	

i	0	1	2	3	4
a	2	7	2	3	2
k	-5	-4	-4	-5	-5
q	4	1	4	3	
m	4	5	24	77	
n	1	1	5	16	

We conclude that $U = \begin{bmatrix} 77 & 48 \\ 8 & 5 \end{bmatrix}$, $\overline{U} = \begin{bmatrix} 77 & -48 \\ -8 & 5 \end{bmatrix}$, $V = \begin{bmatrix} 77 & 24 \\ 16 & 5 \end{bmatrix}$, and $\overline{V} = \begin{bmatrix} 77 & -24 \\ -16 & 5 \end{bmatrix}$ are generating automorphs for f, for $-\overline{f}$, for g, and for $-\overline{g}$ respectively.

Section 11.3. Existence of Representations by Indefinite Forms.

(1) Using the Chinese Remainder Theorem (in the form of Theorem **??**), we find that for arbitrary a, b, and c, the system of congruences

$$x \equiv a \pmod 4, \qquad x \equiv b \pmod 5, \qquad x \equiv c \pmod 7$$

has a simultaneous solution $x \equiv -35a + 56b - 20c \pmod{140}$.

(a) $\left(\frac{-1}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{p}{7}\right) = 1$ if and only if $p \equiv 1 \pmod 4$, $p \equiv 1$ or $4 \pmod 5$, and $p \equiv 1$, 2, or $4 \pmod 7$. Substituting each possible triple for a, b, and c in the system of congruences, the formula above produces six possibilities for p modulo 140.

a	b	c	$x = -35a + 56b - 20c$	$x \bmod 140$
1	1	1	1	1
1	1	2	-19	121
1	1	4	-59	81
1	4	1	169	29
1	4	2	149	9
1	4	4	109	109

(b) $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{p}{5}\right) = -1 = \left(\frac{p}{7}\right)$ if and only if $p \equiv 1 \pmod 4$, $p \equiv 2$ or $3 \pmod 5$, and $p \equiv 3$, 5, or $6 \pmod 7$.

a	b	c	$x = -35a + 56b - 20c$	$x \bmod 140$
1	2	3	17	17
1	2	5	-23	117
1	2	6	-43	97
1	3	3	73	73
1	3	5	33	33
1	3	6	13	13

(c) $\left(\frac{p}{5}\right) = 1$ and $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{7}\right)$ if and only if $p \equiv 3 \pmod 4$, $p \equiv 1$ or $4 \pmod 5$, and $p \equiv 3$, 5, or $6 \pmod 7$.

a	b	c	$x = -35a + 56b - 20c$	$x \bmod 140$
3	1	3	-109	31
3	1	5	-149	131
3	1	6	-169	111
3	4	3	59	59
3	4	5	19	19
3	4	6	-1	139

(d) $\left(\frac{p}{7}\right) = 1$ and $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{5}\right)$ if and only if $p \equiv 3 \pmod 4$, $p \equiv 2$ or $3 \pmod 5$, and $p \equiv 1$, 2, or $4 \pmod 7$.

a	b	c	$x = -35a + 56b - 20c$	$x \bmod 140$
3	2	1	-13	127
3	2	2	-33	107
3	2	4	-73	67
3	3	1	43	43
3	3	2	23	23
3	3	4	-17	123

(2) (a) It was established in Exercise 10.1.2 part (b) that every quadratic form of discriminant $\Delta = 28$ is equivalent either to $(1 : -2)$ or to $(-1 : -2)$, with these two not equivalent to each other. Note that $(1 : -2) \sim (1 : 0)$ and that $(-1 : -2) \sim (-1 : 0)$, so we can use the forms $f(x, y) = x^2 - 7y^2$ and $g(x, y) = -x^2 + 7y^2$ as representatives of $\mathcal{F}_{28}$.

(b) If $p \neq 2, 7$ is prime, then p is represented by a form of discriminant 28 if and only if $\left(\frac{28}{p}\right) = \left(\frac{7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{7}\right) = 1$. Note that $\left(\frac{-1}{f}\right) = 1 = \left(\frac{f}{7}\right)$ and that $\left(\frac{-1}{g}\right) = -1 = \left(\frac{g}{7}\right)$. Thus if $\left(\frac{-1}{p}\right) = 1 = \left(\frac{p}{7}\right)$, then p is represented by f, while if $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{7}\right)$, then p is represented by g. Since $g = -f$, it is clear that f represents p if and only if g represents $-p$.

(3) (a) Exercise 10.2.1 part (b) shows that $\mathcal{F}_{40}$ consists of the classes of $(1 : -3)$ and $(2 : -2)$, with $(1 : -3) \sim (-1 : -3)$ and $(2 : -2) \sim (-2 : -2)$. Since $(1 : -3) \sim (1 : 0)$ and $(2 : -2) \sim (2 : 0)$, we can use $f(x, y) = x^2 - 10y^2$ and $g(x, y) = 2x^2 - 5y^2$ as representatives of these classes.

(b) A prime $p \neq 2, 5$ is represented by one of these forms if and only if $\left(\frac{40}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{5}\right) = 1$. If $\left(\frac{2}{p}\right) = 1 = \left(\frac{p}{5}\right)$, then p is represented by f (since $\left(\frac{2}{f}\right) = 1 = \left(\frac{f}{5}\right)$). With $f \sim -f$, then $-p$ is also represented by f. Likewise, if $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{5}\right)$, then p and $-p$ are represented by g.

(4) (a) By Exercise 10.1.2 part (e), $\mathcal{F}_{57}$ consists of the classes of $(1 : -4)$ and $(-1 : -4)$, with $(-1 : -4) \sim (2 : -4)$. We can use $f = (1 : 0) = x^2 + xy - 14y^2$ and $g = (2 : 0) = 2x^2 + xy - 7y^2$ as representatives of these classes. Note that $f \sim -g$ and $g \sim -f$.

(b) A prime $p \neq 3, 19$ is represented by one of these forms if and only if $\left(\frac{57}{p}\right) = \left(\frac{-3}{p}\right)\left(\frac{-19}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{p}{19}\right) = 1$. If $\left(\frac{p}{3}\right) = 1 = \left(\frac{p}{19}\right)$, then p is represented by f and $-g$, so that $-p$ is represented by g. Similarly, if $\left(\frac{p}{3}\right) = -1 = \left(\frac{p}{19}\right)$, then p is represented by g and $-f$, and so $-p$ is represented by f.

(5) (a) By Exercise 10.1.2 part (f), $\mathcal{F}_{65}$ consists of the classes of $(1 : -4)$ and $(2 : -4)$, with $(1 : -4) \sim (-1 : -4)$ and $(2 : -4) \sim (-2 : -4)$. We can use $f = (1 : 0) =$

$x^2 + xy - 16y^2$ and $g = (2 : 0) = 2x^2 + xy - 8y^2$ as representatives of these classes, with $f \sim -f$ and $g \sim -g$.

(b) A prime $p \neq 5, 13$ is represented by one of these forms if and only if $\left(\frac{65}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{13}{p}\right) = \left(\frac{p}{5}\right)\left(\frac{p}{13}\right) = 1$. If $\left(\frac{p}{5}\right) = 1 = \left(\frac{p}{13}\right)$, then p is represented by f and $-f$, so that $-p$ is represented by f. If $\left(\frac{p}{5}\right) = -1 = \left(\frac{p}{13}\right)$, then p is represented by g and $-g$, and so $-p$ is represented by g.

(6) (a) By Exercise 10.2.1 part (d), $\mathcal{F}_{92}$ consists of the classes of $(1 : -4)$ and $(-1 : -4)$. We can use $f(x, y) = x^2 - 23y^2$ and $g(x, y) = -x^2 + 23y^2$ as representatives of these classes. Since $g = -f$, then f represents an integer n if and only if g represents $-n$.

(b) A prime $p \neq 2, 23$ is represented by one of these forms if and only if $\left(\frac{92}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-23}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{23}\right) = 1$. If $\left(\frac{-1}{p}\right) = 1 = \left(\frac{p}{23}\right)$, then p is represented by f and so $-p$ is represented by g. If $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{23}\right)$, then p is represented by g and $-p$ is represented by f.

Section 11.4. Constructing Representations by Indefinite Forms.

(1) In each part, we apply the equivalence algorithm to $(a : k)$, where $a = p$ and $\phi(x) = x^2 - 6$, until we obtain an i for which $a_i = 1$. If $\phi(x, y) = x^2 - 6y^2$, we use Theorem 11.4.1 to construct a solution of $\phi(x, y) = p$ or $\phi(x, y) = -p$, as illustrated. (Other answers are possible.)

(a) With $p = 23$ and $k = 11$, we obtain the following data from the equivalence/continued fraction algorithm. (As noted in Theorem 11.4.1, we need only the denominator terms in the convergents of the continued fraction.)

i	0	1	2	3
a	23	-6	5	1
k	11	12	-6	1
q	-1	1	1	
n	1	1	2	

Here $k_1 = 12$ is the smallest integer for which $k_1 \equiv -11 \pmod{23}$ and $k_1 > -\sqrt{6}$, and then $a_1 = -\frac{\phi(12)}{23} = -6$. Now with a_2 negative, we need $k_2 < -\sqrt{6}$ as large as possible with $k_2 \equiv -12 \pmod 6$, and find that $k_2 = -6$ and then $a_2 = -\frac{\phi(-6)}{-6} = 5$. Finally, $k_3 = 1$ is the smallest $k_3 > -\sqrt{6}$ for which $k_3 \equiv 6 \pmod 5$, so that $a_3 = -\frac{\phi(1)}{5} = 1$. Now with $i = 3$ odd, we find that $f_3(n_1, n_2) = f_3(1, 2) = 23$, where $f_3 = (-1 : 1)$, that is, $f_3(x, y) = -x^2 + 2xy + 5y^2$. Note that $-f_3(x, y) = x^2 - 2xy - 5y^2 = (x - y)^2 - 6y^2 = \phi(x - y, y)$. Since $-f_3(1, 2) = -23$, then $\phi(1 - 2, 2) = \phi(-1, 2) = -23$.

(b) With $p = 53$ and $k = 18$:

i	0	1	2	3
a	53	-23	6	1
k	18	35	-12	0
q	-1	1	2	
n	1	1	3	

Here $i = 3$ is odd. If $f_3 = (-1 : 0) = -x^2 + 6y^2$, then $f_3(n_1, n_2) = f_3(1, 3) = 53$. Since $f_3 = -\phi$, we immediately conclude that $\phi(1, 3) = -53$.

(c) With $p = 67$ and $k = 26$:

i	0	1	2	3	4
a	67	-25	10	-3	1
k	26	41	-16	6	-3
q	-1	1	1	1	
n	1	1	2	3	

Since $i = 4$ is even, we let $f_4 = (1 : -3) = x^2 - 6xy + 3y^2$, and have that $f_4(n_2, -n_3) = f_4(2, -3) = 67$. Note that $f_4(x, y) = x^2 - 6xy + 3y^2 = (x - 3y)^2 - 6y^2 = \phi(x - 3y, y)$. We conclude that $\phi(2 - 3(-3), -3) = \phi(11, -3) = 67$.

(d) With $p = 73$ and $k = 15$:

i	0	1	2	3	4
a	73	-46	3	2	1
k	15	58	-12	0	-2
q	-1	1	4	1	
n	1	1	5	6	

Here $f_4 = (1 : -2) = x^2 - 4xy - 2y^2$, and $f_4(n_2, -n_3) = f_4(5, -6) = 73$. Since $f_4(x, y) = x^2 - 4xy - 2y^2 = (x - 2y)^2 - 6y^2 = \phi(x - 2y, y)$, we conclude that $\phi(5 - 2(-6), -6) = \phi(17, -6) = 73$.

(2) In each part, we apply Theorem 11.4.1 using a solution of $\phi(x) \equiv 0 \pmod{p}$ found by trial-and-error. Other approaches and other final answers are possible.

(a) If $p = 53$, then $\left(\frac{-1}{p}\right) = 1 = \left(\frac{p}{7}\right)$. Thus we know by Exercise 11.3.2 that p is represented by $\phi(x, y) = x^2 - 7y^2$. The congruence $x^2 - 7 \equiv 0 \pmod{53}$ has $x = 22$ as a solution. We apply Theorem 11.4.1 with $a = 53$ and $k = 22$.

i	0	1	2	3
a	53	-18	9	-1
k	22	31	-13	4
q	-1	1	1	
n	1	1	2	

Here $f_3 = (-(-1) : 4)$, that is, $f_3(x, y) = x^2 + 8xy + 9y^2 = (x + 4y)^2 - 7y^2 = \phi(x + 4y, y)$, and Theorem 11.4.1 implies that $f_3(n_1, n_2) = f_3(1, 2) = 53$. We conclude that $\phi(1 + 4(2), 2) = \phi(9, 2) = 53$.

(b) If $p = 47$, then $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{7}\right)$. Exercise 11.3.2 shows that $-p$ is represented by $\phi(x, y) = x^2 - 7y^2$, and we find that $x = 17$ is a solution of $x^2 - 7 \equiv 0 \pmod{47}$. Let $a = 47$ and $k = 17$.

i	0	1	2	3
a	47	-19	6	1
k	17	30	-11	-1
q	-1	1	2	
n	1	1	3	

If $f_3 = (-1 : -1)$, that is, $f_3(x, y) = -x^2 - 2xy + 6y^2$, then $f_3(n_1, n_2) = f_3(1, 3) = 47$. Then we see that $-f_3(x, y) = x^2 + 2xy - 6y^2 = (x + y)^2 - 7y^2 = \phi(x + y, y)$. Therefore $-f_3(1, 3) = \phi(4, 3) = -47$. As another option, we can apply the equivalence algorithm

with $a = -47$ and $k = 17$, obtaining the following data.

i	0	1	2
a	-47	6	1
k	17	-17	-1
q	0	3	
n	1	3	

Here with $f_2 = (1 : -1)$, that is, $f_2(x, y) = x^2 - 2xy - 6y^2 = (x-y)^2 - 7y^2 = \phi(x-y, y)$, then $f_2(n_0, -n_1) = f_2(1, -3) = -47$, and so $\phi(1 - (-3), -3) = \phi(4, -3) = -47$.

(c) If $p = 31$, then $\left(\frac{2}{p}\right) = 1 = \left(\frac{p}{5}\right)$. By Exercise 11.3.3, then p and $-p$ are both represented by $\phi(x, y) = x^2 - 10y^2$. We find that $x = 14$ is a solution of $x^2 - 10 \equiv 0 \pmod{31}$, and apply Theorem 11.4.1 with $a = 31$ and $k = 14$.

i	0	1	2	3	4
a	31	-9	6	1	1
k	14	17	-8	2	-3
q	-1	1	1	1	
n	1	1	2	3	

Here $f_4 = (1 : -3)$, that is, $f_4(x, y) = x^2 - 6xy - y^2 = (x-3y)^2 - 10y^2 = \phi(x-3y, y)$, and Theorem 11.4.1 implies that $f_4(n_2, -n_3) = f_4(2, -3) = 31$. We conclude that $\phi(2 - 3(-3), -3) = \phi(11, -3) = 31$.

(d) Using the data of Exercise 3, we also see that $f_3 = (-1 : 2)$ and $f_3(n_1, n_2) = f_3(1, 2) = 31$. Here $-f_3(x, y) = x^2 - 4xy - 6y^2 = (x-2y)^2 - 10y^2 = \phi(x-2y, y)$, so we see that $-31 = -f_3(1, 2) = \phi(-3, 2)$.

(e) If $p = 43$, then $\left(\frac{2}{p}\right) = -1 = \left(\frac{p}{5}\right)$, so that p and $-p$ are both represented by $g(x, y) = 2x^2 - 5y^2$. We find that $x = 15$ is a solution of $x^2 - 10 \equiv 0 \pmod{43}$.

i	0	1	2	3	4	5	6
a	43	-18	5	2	3	3	2
k	15	28	-10	0	-2	-1	-2
q	-1	1	2	1	1	1	
n	1	1	3	4	7	11	

Here $f_6 = (2 : -2)$, that is, $f_6(x, y) = 2x^2 - 4xy - 3y^2 = 2(x^2 - 2xy + y^2) - 5y^2 = g(x-y, y)$, and $f_6(n_4, -n_5) = f_6(7, -11) = 43$. We conclude that $g(7-(-11), -11) = g(18, -11) = 43$.

(f) From the data of Exercise 3, we have that $f_3(n_1, n_2) = f_3(1, 3) = 43$, where $f_3 = (-2 : 0) = -g$. Thus $g(1, 3) = -43$.

(g) If $p = 41$, then $\left(\frac{p}{3}\right) = -1 = \left(\frac{p}{19}\right)$. By Exercise 11.3.4, p is represented by $g(x, y) = 2x^2 + xy - 7y^2$ and $-p$ is represented by $f(x, y) = x^2 + xy - 14y^2$. We find that $x = 18$ is a solution of $x^2 + x - 14 \equiv 0 \pmod{41}$. Following the alternative approach of part (b) of this exercise, we apply the equivalence algorithm to $(a : k) = (-41 : 18)$.

i	0	1	2
a	-41	8	1
k	18	-19	2
q	0	2	
n	1	2	

We find that $f_2 = (1:2)$, that is,

$$f_2(x,y) = x^2 + 5xy - 8y^2 = (x+2y)^2 + (x+2y)y - 14y^2 = f(x+2y, y).$$

Theorem 11.4.1 shows that $f_2(n_0, -n_1) = f_2(1,-2) = -41$, and so $f(1+2(-2), -2) = f(-3,-2) = -41$.

(h) With $\Delta = 57$, we apply the equivalence algorithm to $(a:k) = (41:18)$.

i	0	1	2	3	4
a	41	-12	8	1	2
k	18	22	-11	2	-4
q	-1	1	1	1	
n	1	1	2	3	

If $f_4 = (2:-4)$, so that

$$f_4(x,y) = 2x^2 - 7xy - y^2 = 2(x-2y)^2 + (x-2y)y - 7y^2 = g(x-2y, y)$$

we have that $f_4(n_2, -n_3) = f_4(2,-3) = 41$. Thus $g(2-2(-3), -3) = g(8,-3) = 41$.

(i) If $p = 29$, then $\left(\frac{p}{5}\right) = 1 = \left(\frac{p}{13}\right)$. By Exercise 11.3.5, $\phi(x,y) = x^2 + xy - 16y^2$ represents both p and $-p$. We find that $x = 11$ is a solution of $x^2 + x - 16 \equiv 0 \pmod{29}$. We can solve both $\phi(x,y) = 29$ and $\phi(x,y) = -29$ by applying the equivalence algorithm to $(a:k) = (29:11)$.

i	0	1	2	3	4	5	6	7
a	29	-10	4	4	1	4	4	1
k	11	17	-8	-1	-4	-4	-1	-4
q	-1	1	2	1	7	1	1	
n	1	1	3	4	31	35	66	

Here $f_4 = (1:-4)$, that is,

$$f_4(x,y) = x^2 - 7xy - 4y^2 = (x-4y)^2 + (x-4y)y - 16y^2 = \phi(x-4y, y).$$

Now $f_4(n_2, -n_3) = f_4(3,-4) = 29$, and so $\phi(3-4(-4), -4) = \phi(19,-4) = 29$.

(j) From part (i), we also have that if $f_7 = (-1:-4)$, then $f_7(n_5, n_6) = f_7(35, 66) = 29$. Now

$$-f_7(x,y) = x^2 + 7xy - 4y^2 = (x+3y)^2 + (x+3y)y - 16y^2 = \phi(x+3y, y),$$

so we also find that $\phi(35 + 3(66), 66) = \phi(233, 66) = -29$.

(k) If $p = 83$, then $\left(\frac{p}{5}\right) = -1 = \left(\frac{p}{13}\right)$, so that $g(x,y) = 2x^2 + xy - 8y^2$ represents both p and $-p$. We can solve both $g(x,y) = 83$ and $g(x,y) = -83$, beginning with the calculation that $x = 13$ satisfies $x^2 + x - 16 \equiv 0 \pmod{83}$.

i	0	1	2	3	4	5
a	83	-58	2	5	2	2
k	13	69	-12	-3	-3	-4
q	-1	1	7	1	3	
n	1	1	8	9	35	

For $f_2 = (2:-12)$, that is,

$$f_2(x,y) = 2x^2 - 23xy + 58y^2 = 2(x-6y)^2 + (x-6y)y - 8y^2 = g(x-6y, y),$$

we have that $f_2(n_0, -n_1) = f_2(1,-1) = 83$. Thus $g(1-6(-1), -1) = g(7,-1) = 83$.

(l) From part (k), we also have that if $f_5 = (-2 : -4)$, then $f_5(n_3, n_3) = f_5(9, 35) = 83$. Now

$$-f_5(x, y) = 2x^2 + 7xy - 2y^2 = 2(x + 2y)^2 + (x + 2y)(-y) - 8(-y)^2 = g(x + 2y, -y),$$

so we also find that $g(9 + 2(35), -35) = g(79, -35) = -83$.

(m) If $p = 29$, then $\left(\frac{-1}{p}\right) = 1 = \left(\frac{p}{23}\right)$. So $x^2 - 23 \equiv 0 \pmod{29}$ has solutions, which we find to be $x = \pm 9$, and Exercise 11.3.6 shows that $\phi(x, y) = x^2 - 23y^2$ represents p. We apply the equivalence algorithm to $(a : k) = (29 : -9)$ below. (This turns out to require fewer steps than if we use $(29 : 9)$.)

i	0	1	2
a	29	-2	1
k	-9	9	-5
q	0	2	
n	1	2	

Here $f_2 = (1 : -5)$, so $f_2(x, y) = x^2 - 10xy + 2y^2 = (x - 5y)^2 - 23y^2 = \phi(x - 5y, y)$. We have that $f_2(n_0, -n_1) = f_2(1, -2) = \phi(1 - 5(-2), -2) = \phi(11, -2) = 29$.

(n) If $p = 79$, then $\left(\frac{-1}{p}\right) = -1 = \left(\frac{p}{23}\right)$. Here $x^2 - 23 \equiv 0 \pmod{79}$ has solutions, which we find to be $x = \pm 24$, and $\phi(x, y) = x^2 - 23y^2$ represents $-p$. We apply the equivalence algorithm to $(a : k) = (-79 : 24)$ below.

i	0	1	2
a	-79	7	1
k	24	-24	-4
q	0	4	
n	1	4	

Here $f_2 = (1 : -4)$, so $f_2(x, y) = x^2 - 8xy - 7y^2 = (x - 4y)^2 - 23y^2 = \phi(x - 4y, y)$. We have that $f_2(n_0, -n_1) = f_2(1, -4) = \phi(1 - 4(-4), -4) = \phi(17, -4) = -79$.

Section 12.1. Divisibility Properties of Quadratic Recursive Sequences.

(1) In each part, we use the fact that F_n is divisible by $F_{n/p}$ if p is a prime that divides n. Thus F_n is divisible by the least common multiple of these expressions.

(a) F_{15} is divisible by $\text{lcm}(F_3, F_5) = \text{lcm}(2, 5) = 2 \cdot 5$. We have that $F_{15} = 610 = 2 \cdot 5 \cdot 61$.

(b) F_{18} is divisible by $\text{lcm}(F_6, F_9) = \text{lcm}(8, 34) = 2^3 \cdot 17$. We find that $F_{18} = 2584 = 2^3 \cdot 17 \cdot 19$.

(c) F_{20} is divisible by $\text{lcm}(F_4, F_{10}) = \text{lcm}(3, 55) = 3 \cdot 5 \cdot 11$. Here $F_{20} = 6765 = 3 \cdot 5 \cdot 11 \cdot 41$.

(d) F_{24} is divisible by $\text{lcm}(F_8, F_{12}) = \text{lcm}(21, 144) = 2^4 \cdot 3^2 \cdot 7$. We find that $F_{24} = 46368 = 2^5 \cdot 3^2 \cdot 7 \cdot 23$.

(e) F_{30} is divisible by $\text{lcm}(F_6, F_{10}, F_{15}) = \text{lcm}(8, 55, 610) = 2^3 \cdot 5 \cdot 11 \cdot 61$. We find that $F_{30} = 832040 = 2^3 \cdot 5 \cdot 11 \cdot 31 \cdot 61$.

(f) F_{36} is divisible by $\text{lcm}(F_{12}, F_{18}) = \text{lcm}(144, 2584) = 2^4 \cdot 3^2 \cdot 17 \cdot 19$. We find that $F_{36} = 14930352 = 2^4 \cdot 3^3 \cdot 17 \cdot 19 \cdot 107$.

(2) In each part, let $r_0 = 0$ and $r_1 = 1$. We list the values of r_n for $0 \le n \le 10$ and obtain a formula for r_n in general. Verification of Theorem 12.1.8 is omitted, aside from part (a) and special cases in other parts.

(a) If $r_n = 2r_{n-2}$, then the sequence begins $0, 1, 0, 2, 0, 4, 0, 8, 0, 16, 0, \ldots$. The characteristic polynomial of the sequence is $x^2 - 2$, with roots $\sqrt{2}$ and $-\sqrt{2}$. By Theorem

12.1.2,

$$r_n = \frac{(\sqrt{2})^n - (-\sqrt{2})^n}{\sqrt{2} - (-\sqrt{2})} = \begin{cases} 0, & \text{if } n \text{ is even,} \\ 2^q, & \text{if } n = 2q+1 \text{ is odd.} \end{cases}$$

Here $-t = -2$. Note that if m and n are both even or both odd, then

$$r_m r_{n+1} - r_{m+1} r_n = 0 = (-2)^n r_{m-n}.$$

If $m = 2k+1$ and $n = 2\ell$ with $k \geq \ell$, then

$$r_m r_{n+1} - r_{m+1} r_n = 2^k \cdot 2^\ell = (-2)^n \cdot 2^{k-\ell} = (-2)^n r_{m-n}.$$

If $m = 2k$ and $n = 2\ell + 1$ with $k > \ell$ so that $m - n = 2(k - \ell - 1) + 1$, then

$$r_m r_{n+1} - r_{m+1} r_n = -2^{k+1} \cdot 2^\ell = (-2)^n \cdot 2^{k-\ell-1} = (-2)^n r_{m-n}.$$

(b) The characteristic polynomial of $r_n = 2r_{n-1} + r_{n-2}$ is $x^2 - 2x - 1$ with roots $1 + \sqrt{2}$ and $1 - \sqrt{2}$. This sequence begins $0, 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, \ldots$, with n-th term

$$r_n = \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2\sqrt{2}}.$$

Here $-t = -1$. To illustrate Theorem 12.1.8, note that if $m = 8$ and $n = 6$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_8 \cdot r_7 - r_9 \cdot r_6 = 408 \cdot 169 - 985 \cdot 70 = 2 = (-1)^6 \cdot r_2,$$

while if $m = 9$ and $n = 1$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_9 \cdot r_2 - r_{10} \cdot r_1 = 985 \cdot 2 - 2378 \cdot 1 = -408 = (-1)^1 \cdot r_8.$$

(c) The characteristic polynomial of $r_n = 2r_{n-1} - 3r_{n-2}$ is $x^2 - 2x + 3$ with roots $1 + \sqrt{-2}$ and $1 - \sqrt{-2}$. This sequence begins $0, 1, 2, 1, -4, -11, -10, 13, 56, 73, -22, \ldots$, with n-th term

$$r_n = \frac{(1+\sqrt{-2})^n - (1-\sqrt{-2})^n}{2\sqrt{-2}}.$$

Here $-t = 3$. If $m = 8$ and $n = 6$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_8 \cdot r_7 - r_9 \cdot r_6 = 56 \cdot 13 - 73 \cdot (-10) = 1458 = 3^6 \cdot r_2,$$

while if $m = 9$ and $n = 1$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_9 \cdot r_2 - r_{10} \cdot r_1 = 73 \cdot 2 - (-22) \cdot 1 = 168 = 3^1 \cdot r_8.$$

(d) The characteristic polynomial of $r_n = 2r_{n-1} + 3r_{n-2}$ is $x^2 - 2x - 3 = (x-3)(x+1)$. This sequence begins $0, 1, 2, 7, 20, 61, 182, 547, 1640, 4921, 14762, \ldots$, with n-th term

$$r_n = \frac{3^n - (-1)^n}{3 - (-1)} = \frac{3^n - (-1)^n}{4}.$$

Here $-t = -3$. If $m = 8$ and $n = 6$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_8 \cdot r_7 - r_9 \cdot r_6 = 1640 \cdot 547 - 4921 \cdot 182 = 1458 = (-3)^6 \cdot r_2,$$

while if $m = 9$ and $n = 1$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_9 \cdot r_2 - r_{10} \cdot r_1 = 4921 \cdot 2 - 14762 \cdot 1 = -4972 = (-3)^1 \cdot r_8.$$

(e) The characteristic polynomial of $r_n = 2r_{n-1} - 2r_{n-2}$ is $x^2 - 2x + 2$ with roots $1+i$ and $1-i$. This sequence begins $0, 1, 2, 2, 0, -4, -8, -8, 0, 16, 32, \ldots$, with n-th term

$$r_n = \frac{(1+i)^n - (1-i)^n}{2i}.$$

Here $-t = 2$. If $m = 8$ and $n = 6$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_8 \cdot r_7 - r_9 \cdot r_6 = 0(-8) - 16(-8) = 128 = 2^6 \cdot r_2,$$

while if $m = 9$ and $n = 1$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_9 \cdot r_2 - r_{10} \cdot r_1 = 16 \cdot 2 - 32 \cdot 1 = 0 = 2^1 \cdot r_8.$$

(f) The characteristic polynomial of $r_n = 5r_{n-1} - 6r_{n-2}$ is $x^2 - 5x + 6 = (x-3)(x-2)$. This sequence begins $0, 1, 5, 19, 65, 211, 665, 2059, 6305, 19171, 58025, \ldots$, with n-th term

$$r_n = \frac{3^n - 2^n}{3-2} = 3^n - 2^n.$$

Here $-t = 6$. If $m = 8$ and $n = 6$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_8 \cdot r_7 - r_9 \cdot r_6 = 6305 \cdot 2059 - 19171 \cdot 665 = 233280 = 6^6 \cdot r_2,$$

while if $m = 9$ and $n = 1$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_9 \cdot r_2 - r_{10} \cdot r_1 = 19171 \cdot 5 - 58025 \cdot 1 = 37830 = 6^1 \cdot r_8.$$

(g) The characteristic polynomial of $r_n = 3r_{n-1} - 4r_{n-2}$ is $x^2 - 3x + 4$ with roots $\frac{3+\sqrt{-7}}{2}$ and $\frac{3-\sqrt{-7}}{2}$. This sequence begins $0, 1, 3, 5, 3, -11, -45, -91, -93, 85, 627, \ldots$, with n-th term

$$r_n = \frac{\left(\frac{3+\sqrt{-7}}{2}\right)^n - \left(\frac{3-\sqrt{-7}}{2}\right)^n}{\sqrt{-7}}.$$

Here $-t = 4$. If $m = 8$ and $n = 6$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_8 \cdot r_7 - r_9 \cdot r_6 = -93(-91) - 85(-45) = 12288 = 4^6 \cdot r_2,$$

while if $m = 9$ and $n = 1$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_9 \cdot r_2 - r_{10} \cdot r_1 = 85 \cdot 3 - 627 \cdot 1 = -372 = 4^1 \cdot r_8.$$

(h) The characteristic polynomial of $r_n = 3r_{n-1} - 5r_{n-2}$ is $x^2 - 3x + 5$ with roots $\frac{3+\sqrt{-11}}{2}$ and $\frac{3-\sqrt{-11}}{2}$. This sequence begins $0, 1, 3, 4, -3, -29, -72, -71, 147, 796, 1653, \ldots$, with n-th term

$$r_n = \frac{\left(\frac{3+\sqrt{-11}}{2}\right)^n - \left(\frac{3-\sqrt{-11}}{2}\right)^n}{\sqrt{-11}}.$$

Here $-t = 5$. If $m = 8$ and $n = 6$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_8 \cdot r_7 - r_9 \cdot r_6 = 147(-71) - 796(-72) = 46875 = 5^6 \cdot r_2,$$

while if $m = 9$ and $n = 1$, then

$$r_m r_{n+1} - r_{m+1} r_n = r_9 \cdot r_2 - r_{10} \cdot r_1 = 796 \cdot 3 - 1653 \cdot 1 = 735 = 5^1 \cdot r_8.$$

Section 12.2. Periodicity of Quadratic Recursive Sequences.

(1) (a) If $f(x) = x^2 + 1$ is the characteristic polynomial of the quadratic recursive sequence r_n, that is, if $r_n = -r_{n-2}$ with $r_0 = 0$ and $r_1 = 1$, then the sequence begins $0, 1, 0, -1, 0, 1, \ldots$. The discriminant of $f(x)$ is $\Delta = -4$. If p divides Δ, that is, $p = 2$, then $\text{sub}_p(r_n) = 2$ divides p and $\text{ord}_p(r_n) = 2$ divides $p(p-1) = 2$. (Note that $-1 \equiv 1 \pmod 2$.) If $\left(\frac{\Delta}{p}\right) = 1$ so that $p \equiv 1 \pmod 4$, then $\text{sub}_p(r_n) = 2$ and $\text{ord}_p(r_n) = 4$ both divide $p-1$. If $\left(\frac{\Delta}{p}\right) = -1$ so that $p \equiv 3 \pmod 4$, then $\text{sub}_p(r_n) = 2$ divides $p+1$ and $\text{ord}_p(r_n) = 4$ divides $(p+1)(p-1)$. Thus the claims of Corollary 12.2.7 are satisfied by this sequence.

(b) The discriminant of $f(x) = x^2 + 2$ is $\Delta = -8$, and the quadratic recursive sequence r_n with characteristic polynomial $f(x)$ begins

$$0, 1, 0, -2, 0, 4, 0, -8, 0, 16, 0, -32, 0, 64, \ldots.$$

Here $\text{sub}_p(r_n) = 2$ for every prime p. Since $-2 \equiv 1 \pmod 3$, $16 \equiv 1 \pmod 5$, and $64 \equiv 1 \pmod 7$, we find that $\text{ord}_3(r_n) = 2$ (dividing $p-1 = 2$), $\text{ord}_5(r_n) = 8$ (dividing $(p+1)(p-1) = 24$), and $\text{ord}_7(r_n) = 12$ (dividing $(p+1)(p-1) = 48$). These results are consistent with Corollary 12.2.7 since $\left(\frac{-8}{3}\right) = 1$ while $\left(\frac{-8}{5}\right) = -1 = \left(\frac{-8}{7}\right)$.

(c) Let $f(x) = x^2 + x + 1$ with discriminant $\Delta = -3$. The quadratic recursive sequence with characteristic polynomial $f(x)$ begins $0, 1, -1, 0, 1, -1, \ldots$, so that $\text{sub}_p(r_n) = 3$ and $\text{ord}_p(r_n) = 3$ for every prime p. These values are consistent with Corollary 12.2.7 since 3 divides p if p divides Δ (that is, $p = 3$), 3 divides $p-1$ if $\left(\frac{\Delta}{p}\right) = 1$ (this occurs when $p \equiv 1 \pmod 3$), and 3 divides $p+1$ if $\left(\frac{\Delta}{p}\right) = -1$ (that is, $p \equiv 2 \pmod 3$).

(d) Let $f(x) = x^2 + x + 2$ with discriminant $\Delta = -7$. The quadratic recursive sequence with characteristic polynomial $f(x)$ begins as follows, when reduced modulo various primes.

$$\text{Modulo 3:} \qquad 0, 1, 2, 2, 0, 2, 1, 1, 0, 1, \ldots,$$

so that $\text{sub}_3(r_n) = 4$ and $\text{ord}_3(r_n) = 8$.

$$\text{Modulo 5:} \qquad 0, 1, 4, 4, 3, 4, 0, 2, \ldots,$$

with $\text{sub}_5(r_n) = 6$ and (using Proposition 12.2.2 and the fact that $\text{ord}_5(2) = 4$) $\text{ord}_5(r_n) = 24$.

$$\text{Modulo 7:} \qquad 0, 1, 6, 6, 3, 6, 2, 0, 3, \ldots,$$

with $\text{sub}_7(r_n) = 7$ and (since $\text{ord}_7(3) = 6$) $\text{ord}_7(r_n) = 42$. These results are consistent with Corollary 12.2.7 since $\left(\frac{-7}{3}\right) = -1 = \left(\frac{-7}{5}\right)$ and 7 divides -7.

(e) Let $f(x) = x^2 + 2x + 1$ with discriminant $\Delta = 0$. If r_n is the quadratic recursive sequence with characteristic polynomial $f(x)$, then we find, using Theorem 12.1.2, that $r_n = (-1)^{n-1}n$ for all $n \geq 0$. If follows that $\text{sub}_p(r_n) = p$ for every prime p, while $\text{ord}_p(r_n) = 2p$ for every odd prime p. (This is true because $r_{p+1} = (-1)^p(p+1) \equiv -1 \pmod p$ and $\text{ord}_p(-1) = 2$.) These claims are consistent with Corollary 12.2.7 since every prime p divides Δ.

(f) Let $f(x) = x^2 + 2x + 2$ with discriminant $\Delta = -4$. We find that the corresponding quadratic recursive sequence begins as follows, when it is reduced modulo various primes.

$$\text{Modulo 3:} \qquad 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, \ldots,$$

so that $\text{sub}_3(r_n) = 4$ and $\text{ord}_3(r_n) = 8$.

$$\text{Modulo 5:} \qquad 0, 1, 3, 2, 0, 1, 3, 2, 0, \ldots,$$

with $\text{sub}_5(r_n) = 4$ and $\text{ord}_5(r_n) = 4$.

$$\text{Modulo 7:} \qquad 0, 1, 5, 2, 0, 3, 1, 6, 0, \ldots,$$

with $\text{sub}_7(r_n) = 4$ and (since $\text{ord}_7(3) = 6$) $\text{ord}_7(r_n) = 24$. These results are consistent with Corollary 12.2.7 since $\left(\frac{-4}{3}\right) = -1 = \left(\frac{-4}{7}\right)$, while $\left(\frac{-4}{5}\right) = 1$.

(g) If $f(x) = x^2 - x + 2$, with discriminant $\Delta = -7$, then the corresponding quadratic recursive sequence begins as follows.

$$\text{Modulo 3:} \qquad 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, \ldots,$$

so that $\text{sub}_3(r_n) = 4$ and $\text{ord}_3(r_n) = 8$.

$$\text{Modulo 5:} \qquad 0, 1, 1, 4, 2, 4, 0, 2, \ldots,$$

with $\text{sub}_5(r_n) = 6$ and $\text{ord}_5(r_n) = 24$ (since $\text{ord}_5(2) = 4$).

$$\text{Modulo 7:} \qquad 0, 1, 1, 6, 4, 6, 5, 0, 4, \ldots,$$

with $\text{sub}_7(r_n) = 7$ and $\text{ord}_7(r_n) = 21$ (since $\text{ord}_7(4) = 3$). Here $\left(\frac{-7}{3}\right) = -1 = \left(\frac{-7}{5}\right)$ and 7 divides -7.

(h) If $f(x) = x^2 + x - 2$, with discriminant $\Delta = 9$, then:

$$\text{Modulo 3:} \qquad 0, 1, 2, 0, 1, 2, 0, 1, \ldots,$$

with $\text{sub}_3(r_n) = 3 = \text{ord}_3(r_n)$.

$$\text{Modulo 5:} \qquad 0, 1, 4, 3, 0, 1, 4, 3, \ldots,$$

with $\text{sub}_5(r_n) = 4 = \text{ord}_5(r_n)$.

$$\text{Modulo 7:} \qquad 0, 1, 6, 3, 2, 4, 0, 1, \ldots,$$

with $\text{sub}_7(r_n) = 6 = \text{ord}_7(r_n)$. Here 3 divides Δ but $\left(\frac{\Delta}{p}\right) = 1$ for every other odd prime p.

(i) If $f(x) = x^2 - 2x - 1$, with discriminant $\Delta = 8$, then:

$$\text{Modulo 3:} \qquad 0, 1, 2, 2, 0, 2, 1, 1, 0, 1, \ldots,$$

with $\text{sub}_3(r_n) = 4$ and $\text{ord}_3(r_n) = 8$.

$$\text{Modulo 5:} \qquad 0, 1, 2, 0, 2, 4, 0, 4, 3, 0, 3, 1, 0, 1, \ldots,$$

with $\text{sub}_5(r_n) = 3$ and $\text{ord}_5(r_n) = 12$.

$$\text{Modulo 7:} \qquad 0, 1, 2, 5, 5, 1, 0, 1, \ldots,$$

with $\text{sub}_7(r_n) = 6 = \text{ord}_7(r_n)$. Here $\left(\frac{8}{3}\right) = -1 = \left(\frac{8}{5}\right)$, while $\left(\frac{8}{7}\right) = 1$.

(j) If $f(x) = x^2 - 2x - 2$, with discriminant $\Delta = 12$, then:

$$\text{Modulo 3:} \qquad 0, 1, 2, 0, 1, 2, 0, 1, \ldots,$$

with $\text{sub}_3(r_n) = 3 = \text{ord}_3(r_n)$.

$$\text{Modulo 5:} \qquad 0, 1, 2, 1, 1, 4, 0, 3, \ldots,$$

with $\text{sub}_5(r_n) = 6$ and $\text{ord}_5(r_n) = 24$ (since $\text{ord}_5(3) = 4$).

$$\text{Modulo 7:} \qquad 0, 1, 2, 6, 2, 2, 1, 6, 0, 5, \ldots,$$

with $\text{sub}_7(r_n) = 8$ and $\text{ord}_7(r_n) = 48$ (since $\text{ord}_7(5) = 6$. Here 3 divides 12 while $\left(\frac{12}{5}\right) = -1 = \left(\frac{12}{7}\right)$.

Section 12.3. Suborder Functions.

(1) Using Propositions 12.3.2 and 12.3.4, it suffices to find $\text{sub}_p(c)$ for $3 \le c \le \frac{p-1}{2}$.

(a) If $p = 7$ and $c = 3$, then $\left(\frac{c+2}{p}\right) = \left(\frac{5}{7}\right) = -1$ and $\left(\frac{c-2}{p}\right) = \left(\frac{1}{7}\right) = 1$. By Theorem 12.3.5, $m = \text{sub}_7(3)$ divides $p+1 = 8$ with $e_2(m) = e_2(8)$. The only possibility is $\text{sub}_7(3) = 8$ and then $\text{sub}_7(-3) = 8$ also. We compile the values of the suborder function on $\mathbb{F}_7$ as follows.

c	0	1	2	3
$\text{sub}_7(c)$	4	6	1	8
$\text{sub}_7(-c)$		3	2	8

(b) Let $p = 13$. For each of $c = 3$, $c = 5$, and $c = 6$, we find that $\left(\frac{c+2}{p}\right) = -1$ and $\left(\frac{c-2}{p}\right) = 1$. In those cases, $m = \text{sub}_{13}(c)$ divides $p + 1 = 14$ with $e_2(m) = e_2(14)$. We must have $\text{sub}_{13}(c) = 14$ and then $\text{sub}_{13}(-c) = 7$, since $\text{sub}_{13}(c) = 2$ only for $c = -2$. If $c = 4$, then $\left(\frac{c+2}{p}\right) = -1$ and $\left(\frac{c-2}{p}\right) = -1$, so that $m = \text{sub}_{13}(4)$ divides $p - 1 = 12$ with $e_2(m) = e_2(12)$. We conclude that $\text{sub}_{13}(4) = 12 = \text{sub}_{13}(-4)$ since $\text{sub}_{13}(c) = 4$ only for $c = 0$. We summarize these results as follows.

c	0	1	2	3	4	5	6
$\text{sub}_{13}(c)$	4	6	1	14	12	14	14
$\text{sub}_{13}(-c)$		3	2	7	12	7	7

(c) Let $p = 17$. We find that $\left(\frac{c+2}{p}\right) = -1$ and $\left(\frac{c-2}{p}\right) = 1$ for $c = 3$ and $c = 4$. Here $m = \text{sub}_{17}(c)$ divides $p + 1 = 18$ with $e_2(m) = e_2(18)$, and so $\text{sub}_{17}(c) = 18$ and $\text{sub}_{17}(-c) = 9$. (Both $\text{sub}_{17}(c) = 6$ and $\text{sub}_{17}(c) = 2$ occur only in one instance.) For $c = 5$ and $c = 8$, we have $\left(\frac{c+2}{p}\right) = -1$ and $\left(\frac{c-2}{p}\right) = -1$. Here $m = \text{sub}_{17}(c)$ divides $p - 1 = 16$ with $e_2(m) = e_2(16)$, and we conclude that $\text{sub}_{17}(c) = 16 = \text{sub}_{17}(-c)$. If $c = 6$, then $\left(\frac{c+2}{p}\right) = 1$ and $\left(\frac{c-2}{p}\right) = 1$, so that $m = \text{sub}_{17}(c)$ divides $p - 1 = 16$ with $e_2(m) < e_2(16)$. Here we conclude that $\text{sub}_{17}(c) = 8 = \text{sub}_{17}(-c)$. Finally, if $c = 7$, then $\left(\frac{c+2}{p}\right) = 1$ and $\left(\frac{c-2}{p}\right) = -1$. Here $m = \text{sub}_{17}(c)$ divides $p + 1 = 18$ with $e_2(m) < e_2(18)$, and we conclude that $\text{sub}_{17}(c) = 9$ and $\text{sub}_{17}(-c) = 18$. To summarize:

c	0	1	2	3	4	5	6	7	8
$\text{sub}_{17}(c)$	4	6	1	18	18	16	8	9	16
$\text{sub}_{17}(-c)$		3	2	9	9	16	8	18	16

(d) Let $p = 19$. Here if $c = 4$ or $c = 5$, we find that $\left(\frac{c+2}{p}\right) = 1$ and $\left(\frac{c-2}{p}\right) = -1$. So then $m = \text{sub}_{19}(c)$ divides $p + 1 = 20$ with $e_2(m) < e_2(20)$. This occurs if $m = 10$ or $m = 5$, and we cannot immediately rule out either possibility. Instead we can calculate $\text{sub}_{19}(c)$ as the order of the quadratic sequence defined by the characteristic polynomial $x^2 - cx + 1$. Modulo 19, the sequence with $c = 4$ begins $0, 1, 4, -4, -1, 0, 1, \ldots$, while the sequence with $c = 5$ begins $0, 1, 5, 5, 1, 0, -1, -5, -5, -1, 0, 1, \ldots$. We conclude that $\text{sub}_{19}(4) = 5$ and $\text{sub}_{19}(5) = 10$. For all other values of c, we can determine $\text{sub}_{19}(c)$ with the same approach as in the previous parts. We omit the details and compile the results as follows.

c	0	1	2	3	4	5	6	7	8	9
$\text{sub}_{19}(c)$	4	6	1	9	5	10	20	9	20	9
$\text{sub}_{19}(-c)$		3	2	18	10	5	20	18	20	18

(2) In parts (a)–(e), the characteristic polynomial of r_n is $x^2 - 2x - 1$, with suborder number $c_p(f) = s^2(-t)^{-1} - 2 = 4(-1)^{-1} - 2 = -6$ for each prime p. In parts (f)–(j), the characteristic polynomial of r_n is $x^2 - x + 3$, and we find that $c_p(f) = s^2(-t)^{-1} - 2 = 3^{-1} - 2$ is the solution of the congruence $3c \equiv -5 \pmod{p}$.

(a) If $r_n = 2r_{n-1} + r_{n-2}$ with $r_0 = 0$ and $r_1 = 1$, then this sequence modulo 7 begins

$$0, 1, 2, -2, -2, 1, 0, \ldots.$$

So $\mathrm{sub}_7(r_n) = 6$. Since $c = -6 = 1$ in $\mathbb{F}_7$, we find, using the table in Exercise 1 part (a), that $\mathrm{sub}_7(c) = 6$ as well.

(b) Modulo 11, the same sequence begins

$$0, 1, 2, 5, 1, -4, 4, 4, 1, -5, 2, -1, 0, \ldots,$$

so that $\mathrm{sub}_{11}(r_n) = 12$. Since $-6 = 5$ in $\mathbb{F}_{11}$, an example in §12.3 shows that $\mathrm{sub}_{13}(c) = 12$ also.

(c) Modulo 13, the sequence begins

$$0, 1, 2, 5, -1, 3, 5, 0, \ldots,$$

with $\mathrm{sub}_{13}(r_n) = 7$. The table in Exercise 1 part (b) shows that $\mathrm{sub}_{13}(-6) = 7$ also.

(d) Modulo 17:

$$0, 1, 2, 5, -5, -5, 2, -1, 0 \ldots,$$

with $\mathrm{sub}_{17}(r_n) = 8$. We find that $\mathrm{sub}_{17}(-6) = 8$ as well, from the table in part (c) of Exercise 1.

(e) Modulo 19:

$$0, 1, 2, 5, -7, -9, -6, -2, 9, -3, 3, 3, 9, 2, -6, 9, -7, -5, 2, -1, 0, \ldots,$$

with $\mathrm{sub}_{19}(r_n) = 20$. By Exercise 1 part (d), we find that $\mathrm{sub}_{19}(-6) = 20$ as well.

(f) In the remaining parts, let $r_n = r_{n-1} - 3r_{n-2}$ with $r_0 = 0$ and $r_1 = 1$. Modulo 7, this sequence begins

$$0, 1, 1, -2, 2, 1, 2, -1, 0 \ldots,$$

so that $\mathrm{sub}_7(r_n) = 8$. The solution of $3c \equiv -5 \pmod{7}$ is $c = 3$, and $\mathrm{sub}_7(3) = 8$ as well, using part (a) of Exercise 1.

(g) Modulo 11:

$$0, 1, 1, -2, -5, 1, 5, 2, -2, 3, -2, 0, \ldots,$$

with $\mathrm{sub}_{11}(r_n) = 11$. The solution of $3c \equiv -5 \pmod{11}$ is $c = 2$. We have that $\mathrm{sub}_{11}(2) = 1$, and that the suborder of r_n modulo $p = 11$ equals p, as in Theorem 12.3.3.

(h) Modulo 13:

$$0, 1, 1, -2, -5, 1, 3, 0 \ldots,$$

with $\mathrm{sub}_{13}(r_n) = 7$. The solution of $3c \equiv -5 \pmod{13}$ is $c = -6$, and $\mathrm{sub}_{13}(-6) = 7$ also.

(i) Modulo 17:

$$0, 1, 1, -2, -5, 1, -1, -4, -1, -6, -3, -2, 7, -4, -8, 4, -6, -1, 0 \ldots,$$

with $\mathrm{sub}_{11}(r_n) = 18$. The solution of $3c \equiv -5 \pmod{17}$ is $c = 4$, and $\mathrm{sub}_{17}(4) = 18$ as well from part (c) of Exercise 1.

(j) Modulo 19:

$$0, 1, 1, -2, -5, 1, -3, -6, 3, 2, -7, 6, 8, 9, 4, -4, 3, -4, 6, -1, 0 \ldots,$$

with $\text{sub}_{13}(r_n) = 20$. The solution of $3c \equiv -5 \pmod{19}$ is $c = -8$, and $\text{sub}_{19}(-8) = 20$ also, from part (d) of Exercise 1.

Section 12.4. Suborder Sequences.

(1) The suborder sequence of $c = 3$ (that is, $c_{n+1} = 3c_n - c_{n-1}$ with $c_0 = 2$ and $c_1 = 3$) modulo $p = 17$ begins as follows:

$$2, 3, 7, 1, -4, 4, -1, -7, -3, -2, -3, -7, -1, 4, -4, 1, 7, 3, 2, \ldots.$$

We find that $m = 18$ is the smallest positive integer for which $c_m = 2$, and conclude that $\text{sub}_{17}(3) = 18$. Furthermore, $\text{sub}_{17}(c_k) = \frac{18}{\gcd(18,k)}$ for all $k \geq 0$. For instance, $c_5 = 4$ and $c_7 = -7$ also have suborder 18; $c_2 = 7$, $c_4 = -4$, and $c_8 = -3$ have suborder 9; $c_3 = 1$ has suborder 6; and so forth. Similarly, the suborder sequence of $c = 5$ modulo $p = 17$ begins:

$$2, 5, 6, 8, 0, -8, -6, -5, -2, -5, -6, -8, 0, 8, 6, 5, 2, \ldots.$$

Here $c_{16} = 2$, and we conclude that $c_1 = 5$, $c_3 = 8$, $c_5 = -8$, and $c_7 = -5$ have suborder 16; $c_2 = 6$ and $c_6 = -6$ have suborder 8; and so forth. From these two sequences, we determine all elements whose suborder is a divisor of 18 or 16, that is, all elements of $\mathbb{F}_{17}$.

(2) The suborder sequence of $c = 3$ modulo $p = 37$ begins as follows:

$$2, 3, 7, 18, 10, 12, -11, -8, -13, 6, -6, 13, 8, 11, -12, -10, -18, -7, -3, -2,$$

$$-3, -7, -18, -10, -12, 11, 8, 13, -6, 6, -13, -8, -11, 12, 10, 18, 7, 3, 2, \ldots.$$

Here $c_{38} = 2$. Values of c_n with $\gcd(n, 38) = 1$ have suborder 38 (for example $c_1 = 3$, $c_3 = 18$, $c_5 = 12$, and so forth); those with $\gcd(n, 38) = 2$ have suborder 19 (such as $c_2 = 7$, $c_4 = 10$, $c_6 = -11$, and so forth). The suborder sequence of $c = 4$ modulo $p = 37$ begins

$$2, 4, 14, 15, 9, -16, 1, -17, 5, 0, -5, 17, -1, 16, -9, -15, -14, -4, -2,$$

$$-4, -14, -15, -9, 16, -1, 17, -5, 0, 5, -17, 1, -16, 9, 15, 14, 4, 2, \ldots.$$

This time we find that $c_{36} = 2$. Values of c_n with $\gcd(n, 36) = 1$ (such as $c_1 = 4$, $c_5 = -16$, $c_7 = -17$, and so forth) have suborder 36; those with $\gcd(n, 36) = 2$ ($c_2 = 14$, $c_{10} = -5$, $c_{14} = -9$) have suborder 18; those with $\gcd(n, 36) = 3$ ($c_3 = 15$, $c_{15} = -15$) have suborder 12; those with $\gcd(n, 36) = 4$ ($c_4 = 9$, $c_8 = 5$, $c_{16} = -14$) have suborder 9, and so forth. All elements of $\mathbb{F}_{37}$ appear in one of these sequences, so we determine the entire suborder function on $\mathbb{F}_{37}$.

(3) The suborder sequence of $c = 3$ modulo $p = 43$ begins as follows:

$$2, 3, 7, 18, 4, -6, 21, -17, 14, 16, -9, 0, 9, -16, -14, 17, -21, 6, -4, -18, -7, -3, -2,$$

$$-3, -7, -18, -4, 6, -21, 17, -14, -16, 9, 0, -9, 16, 14, -17, 21, -6, 4, 18, 7, 3, 2, \ldots,$$

with $c_{44} = 2$. Values of c_n with $\gcd(n, 44) = 1$ (for example $c_1 = 3$, $c_3 = 18$, $c_5 = -6$, and so forth) have suborder 44; those with $\gcd(n, 44) = 2$ ($c_2 = 7$, $c_6 = 21$, $c_{10} = -9$, $c_{14} = -14$, $c_{18} = -4$) have suborder 22; those with $\gcd(n, 44) = 4$ ($c_4 = 4$, $c_8 = 14$, $c_{12} = 9$, $c_{16} = -21$, $c_{20} = -7$) have suborder 11, and so forth. The suborder sequence of $c = 5$ modulo $p = 43$ begins

$$2, 5, -20, -19, 11, -12, 15, 1, -10, -8, 13, -13, 8, 10, -1, -15, 12, -11, 19, 20, -5, -2,$$

$$-5, 20, 19, -11, 12, -15, -1, 10, 8, -13, 13, -8, -10, 1, 15, -12, 11, -19, -20, 5, 2, \ldots,$$

with $c_{42} = 2$. Values of c_n with $\gcd(n, 42) = 1$ ($c_1 = 5$, $c_5 = -12$, $c_{11} = -13$, $c_{13} = 10$, $c_{17} = -11$, $c_{19} = 20$) have suborder 42; those with $\gcd(n, 42) = 2$ ($c_2 = -20$, $c_4 = 11$, $c_8 = -10$, $c_{10} = 13$, $c_{16} = 12$, $c_{20} = -5$) have suborder 21; those with $\gcd(n, 36) = 3$ ($c_3 = -19$, $c_9 = -8$, $c_{15} = -15$) have suborder 14; those with $\gcd(n, 42) = 6$ ($c_6 = 15$, $c_{12} = 8$, $c_{18} = 19$) have suborder 7, and so forth. All elements of $\mathbb{F}_{43}$ appear in one of these sequences.

(4) Let c_k be the k-th term in the suborder sequence of c modulo an odd prime p, and let m be the suborder of c modulo p.

(a) Suppose that $m = 2k + 1$ for some integer k. Then $k + 1 \equiv -k \pmod{m}$, and so $c_k = c_{k+1}$ by part (2) of Theorem 12.4.1. On the other hand, suppose that $c_k = c_{k+1}$ for some integer k. Then then either $k + 1 \equiv k \pmod{m}$ or $k + 1 \equiv -k \pmod{m}$, again by part (2) of Theorem 12.4.1. The first case is possible only when $m = 1$ and $c = c_1 = 2$. The second possibility implies that m divides $2k+1$. But then $m = 2\ell+1$ is odd, and we must conclude that $c_{\ell+1} = c_\ell$ as above. Thus $m = 2k + 1$ for some integer k if and only if k is the *smallest* integer for which $c_k = c_{k+1}$.

(b) Suppose that $m = 4k$ for some integer k. Using part (5) of Theorem 12.4.1, we have that $2 = c_{2(2k)} = c_{2k}^2 - 2$, so that $c_{2k}^2 = 4$. Since $2k < m$, we cannot have $c_{2k} = 2$, and thus $c_{2k} = -2$. But now using part (5) of Theorem 12.4.1 again, we see that $-2 = c_{2k} = c_k^2 - 2$ and conclude that $c_k = 0$. Conversely, if $c_k = 0$ for some k, then $c_{2k} = 0^2 - 2 = -2$ and $c_{4k} = (-2)^2 - 2 = 2$. Thus $m = 4k$ if and only if k is the smallest integer for which $c_k = 0$.

(c) Suppose that $m = 6k$ for some integer k. Then $4k \equiv -2k \pmod{m}$ so that $c_{4k} = c_{2k}$ by part (2) of Theorem 12.4.1. But now we have $c_{2k} = c_{2(2k)} = c_{2k}^2 - 2$ by part (5) of the same theorem. Thus c_{2k} satisfies the equation $x^2 - x - 2 = (x - 2)(x + 1) = 0$, so that either $c_{2k} = 2$ or $c_{2k} = -1$ in the field $\mathbb{F}_p$. The first case is impossible if $m = 6k$, and thus $c_{2k} = -1$. But now $-1 = c_{2k} = c_k^2 - 2$ and so $c_k = 1$ or $c_k = -1$. It is established in part (4) of Corollary 12.4.3 that the second case implies that $c_{3k} = 2$, contrary to our assumption. Thus $c_k = 1$. Conversely, if $c_k = 1$, then $c_{2k} = c_k^2 - 2 = -1$, so that $c_{3k} = c_{2k} \cdot c_k - c_k = -2$ by part (4) of Theorem 12.4.1, and then $c_{6k} = c_{3k}^2 - 2 = 2$. So $m = 6k$ if and only if k is the smallest positive integer for which $c_k = 1$.

(5) (a) The suborder sequence of $c = 4$ modulo $p = 61$ (that is, $c_{n+1} = 4c_n - c_{n-1}$ with $c_0 = 2$ and $c_1 = 4$) begins as follows:

$$2, 4, 14, -9, 11, -8, 18, 19, -3, 30, 1, -26, 17, -28, -7, 0, \ldots.$$

From the fact that $c_{10} = 1$, or using $c_{15} = 0$, we determine that $\mathrm{sub}_{61}(4) = 60$ (by parts (5) and (3) of Corollary 12.4.3). Now we know that $c_{30-k} = -c_k$ for $0 \le k \le 15$, and $c_{60-k} = c_k$ for $0 \le k \le 30$ (by parts (3) and (2) of Theorem 12.4.1). By Corollary 12.4.2, we then find that the suborders of $c_1 = 4$, $c_7 = 19$, $c_{11} = -26$, $c_{13} = -28$, $c_{17} = 28$, $c_{19} = 26$, $c_{23} = -19$, and $c_{29} = -4$ are all equal to 60; the suborders of $c_2 = 14$, $c_{14} = -7$, $c_{22} = -c_8 = 3$, and $c_{26} = -c_4 = -11$ all equal 30; the suborders of $c_4 = 11$, $c_8 = -3$, $c_{16} = -c_{14} = 7$, and $c_{28} = -c_2$ all equal 15; the suborders of $c_3 = -9$, $c_9 = 30$, $c_{21} = -30$, and $c_{27} - 9$ all equal 20; the suborders of $c_5 = -8$ and $c_{25} = 8$ equal 12; the suborders of $c_6 = 18$ and $c_{18} = -c_{12} = -17$ equal 10; and the suborders of $c_{12} = 17$ and $c_{24} = -c_6 = -18$ equal 5 (along with the usual elements of suborder 6, 4, 3, 2, and 1).

(b) The suborder sequence of $c = 5$ modulo $p = 61$ begins:

$$2, 5, 23, -12, -22, 24, 20, 25, -6, 16, 25, -13, -29, -10, -21, 27, -27, \ldots,$$

with $c_{15} = -c_{16}$. It follows that $\text{sub}_{61}(5) = 4(15) + 2 = 62$ by part (2) of Corollary 12.4.3, and that $c_{31-k} = -c_k$ for $0 \le k \le 15$ by part (3) of Theorem 12.4.1. Thus $\text{sub}_{61}(c_k) = 62$ if $1 \le k < 31$ is odd, that is, for the following values: 5, -12, 24, 25, 16, -13, -10, 27, 21, 29, -25, 6, -20, 22, and -23, while $\text{sub}_{61}(c_k) = 31$ if $1 \le k < 31$ is even, that is, for 23, -22, 20, -6, 25, -29, -21, -27, 10, 13, -16, -25, -24, 12, and -5.

(c) The suborder sequence of $c = 3$ modulo $p = 67$ begins:

$$2, 3, 7, 18, -20, -11, -13, -28, -4, 16, -15, 6, 33, 26, -22, -25, 14, 0, \ldots.$$

Since $c_{17} = 0$, then $\text{sub}_{67}(3) = 68$, and $c_{34-k} = -c_k$ for $0 \le k \le 17$. It follows that $\text{sub}_{67}(c_k) = 68$ for odd values of k with $1 \le k \le 33$ and $k \ne 17$, that is, for 3, 18, -11, -28, 16, 6, 26, -25, 25, -26, -6, -16, 28, 11, -18, and -3; while $c_2 = 7$, $c_6 = -13$, $c_{10} = -15$, $c_{14} = -22$, $c_{18} = -14$, $c_{22} = -33$, $c_{26} = 4$, and $c_{30} = 20$ have suborder 34; and $c_4 = -20$, $c_8 = -4$, $c_{12} = 33$, $c_{16} = 14$, $c_{20} = 22$, $c_{24} = 15$, $c_{28} = 13$, and $c_{32} = -7$ have suborder 17.

(d) The suborder sequence of $c = 5$ modulo $p = 67$ begins:

$$2, 5, 23, -24, -9, -21, -29, 10, 12, -17, -30, 1, -32, -27, 31, -9, 8, -8, \ldots.$$

Here $c_{11} = 1$ so that $\text{sub}_{67}(5) = 6(11) = 66$. (Also, since $c_{16} = -c_{17}$, we know that $\text{sub}_{67}(5) = 4(16) + 2 = 66$.) Thus $c_{33-k} = -c_k$ for $1 \le k \le 16$, and we can compute the following values of the suborder function: $c_1 = 5$, $c_5 = -21$, $c_7 = 10$, $c_{13} = -27$, $c_{17} = -8$, $c_{19} = -31$, $c_{23} = 30$, $c_{25} = -12$, $c_{29} = 9$, and $c_{31} = -23$ have suborder 66; $c_2 = 23$, $c_4 = -9$, $c_8 = 12$, $c_{10} = -30$, $c_{14} = 31$, $c_{16} = 8$, $c_{20} = 27$, $c_{26} = -10$, $c_{28} = 21$, and $c_{32} = -5$ have suborder 33; $c_3 = -24$, $c_9 = -17$, $c_{15} = -19$, $c_{21} = 32$, and $c_{27} = 29$ have suborder 22; and $c_6 = -29$, $c_{12} = -32$, $c_{18} = 19$, $c_{24} = 17$, and $c_{30} = 24$ have suborder 11.

(6) The characteristic polynomial of the quadratic sequence $r_n = 2r_{n-1} + r_{n-2}$ is $f(x) = x^2 - 2x - 1$, with suborder number $c_p(f) = 2^2(-1)^{-1} - 2 = -6$ for every prime p.

(a) Modulo $p = 29$, the sequence begins $0, 1, 2, 5, 12, 0, \ldots$, so that $\text{sub}_{29}(r_n) = 5$. Table 12.1 shows that $\text{sub}_{29}(6) = 10$, and so $\text{sub}_{29}(-6) = 5$ by Proposition 12.3.4.

(b) Modulo $p = 31$, the sequence begins

$$0, 1, 2, 5, 12, -2, 8, 14, 5, -7, -9, 6, 3, 12, -4, 4,$$

$$4, 12, -3, 6, 9, -7, -5, 14, -8, -2, -12, 5, -2, 1, 0, \ldots,$$

with $\text{sub}_{31}(r_n) = 30$. This is consistent with the calculation of $\text{sub}_{31}(6) = 15$ in Table 12.1.

(c) Modulo $p = 37$, the sequence begins

$$0, 1, 2, 5, 12, -8, -4, -16, 1, -14, 10, 6, -15, 13, 11, -2, 7, 12, -6, 0, \ldots$$

so that $\text{sub}_{37}(r_n) = 19$, consistent with the calculation of $\text{sub}_{37}(6) = 38$ in Table 12.1.

(d) Modulo $p = 41$, we find $0, 1, 2, 5, 12, -12, -12, 5, -2, 1, 0, \ldots$, with $\text{sub}_{41}(r_n) = 10$. From Table 12.1, we see that $\text{sub}_{41}(6) = 5$.

(e) Modulo $p = 43$:

$$0, 1, 2, 5, 12, -14, -16, -3, 21, -4, 13, -21, 14, 7, -15, 20, -18, -16, -7, 13, 19, 8, -8,$$

$$-8, 19, -13, -7, 16, -18, -20, -15, -7, 14, 21, 13, 4, 21, 3, -16, 14, 12, -5, 2, -1, 0, \ldots,$$

so that $\text{sub}_{43}(r_n) = 44$. This is consistent with the Table 12.1 value of $\text{sub}_{43}(6) = 44$, using Proposition 12.3.4, since this number is divisible by 4.

(f) Modulo $p = 47$:

$$0, 1, 2, 5, 12, -18, 23, -19, -15, -2, -19, 7, -5, -3, -11, 22, -14,$$
$$-6, 21, -11, -1, -13, 20, -20, -20, -13, 1, -11, -21, -6, 14, 22, 11,$$
$$-3, 5, 7, 19, -2, 15, -19, -23, -18, -12, 5, -2, 1, 0, \ldots,$$

so that $\text{sub}_{47}(r_n) = 46$, consistent with the Table 12.1 value of $\text{sub}_{47}(6) = 23$.

(7) In each part, we use Theorem 12.3.5 to determine preliminary possibilities for $\text{sub}_p(c)$, then calculate the suborder subsequence (d_n) of c modulo p and describe the implications of that sequence via Theorem 12.4.5. Finally we calculate the suborder sequence (c_n) of c modulo p to confirm these claims.

(a) If $c = 3$ and $p = 53$, then $\left(\frac{c+2}{p}\right) = \left(\frac{5}{53}\right) = -1$ and $\left(\frac{c-2}{p}\right) = \left(\frac{1}{53}\right) = 1$, so that $m = \text{sub}_{53}(3)$ divides $p+1 = 54$ with $e_2(m) = e_2(54) = 1$. We can rule out $m = 2$ and $m = 6$ by Proposition 12.3.2, and so $m = 18$ or $m = 54$. The suborder subsequence with $d_0 = 3$ and $d_n = d_{n-1}^2 - 2$ for $n > 0$ begins

$$3, 7, -6, -19, -12, -17, 22, 5, 23, -3, 7, \ldots.$$

We see that $d_{10} = d_1$, confirming that $e_2(m) = 1$. Furthermore $t = 10 - 1 = 9$ is the smallest positive integer with $2^t \equiv \pm 1 \pmod{m/2}$. Since $2^3 \equiv -1 \pmod 9$, we eliminate the possibility that $m = 18$, and conclude that $m = 54$. (One can verify that $2^9 \equiv -1 \pmod{27}$.) The suborder sequence of $c = 3$ modulo $p = 53$ (that is, $c_0 = 2$, $c_1 = 3$, and $c_{n+1} = 3 \cdot c_n - c_{n-1}$ for $n > 1$) begins

$$2, 3, 7, 18, -6, 17, 4, -5, -19, 1, \ldots.$$

Since $c_9 = 1$, we know that $m = \text{sub}_{53}(3) = 6(9) = 54$ by part (5) of Corollary 12.4.3.

(b) Let $c = 8$ and $p = 53$. Then $\left(\frac{c+2}{p}\right) = \left(\frac{10}{53}\right) = 1$ and $\left(\frac{c-2}{p}\right) = \left(\frac{6}{53}\right) = 1$, so that $m = \text{sub}_{53}(8)$ divides $p - 1 = 52$ with $e_2(m) < e_2(52)$. We can eliminate $m = 1$ and 2, and conclude that $m = 13$ or 26. The suborder subsequence of c begins

$$8, 9, 26, -15, 11, 13, 8, \ldots,$$

with $d_6 = d_0$. Thus $e_2(m) = 0$ and we must have $m = 13$. We can confirm that $t = 6$ is the smallest positive integer with $2^t \equiv -1 \pmod{13}$. The suborder sequence of $c = 8$ modulo $p = 53$ begins

$$2, 8, 9, 11, 26, -15, 13, 13, \ldots.$$

With $c_6 = c_7$, we confirm that $m = \text{sub}_{53}(8) = 2(6) + 1 = 13$ by part (1) of Corollary 12.4.3.

(c) Let $c = 6$ and $p = 59$. Since $\left(\frac{c+2}{p}\right) = \left(\frac{8}{59}\right) = -1$ and $\left(\frac{c-2}{p}\right) = \left(\frac{4}{59}\right) = 1$, we know that $m = \text{sub}_{59}(6)$ divides $p + 1 = 60$ with $e_2(m) = e_2(60) = 2$. So $m = 12$, 20, or 60. ($\text{sub}_p(c) = 4$ only when $c = 0$ in $\mathbb{F}_p$.) The suborder subsequence with $d_0 = 6$ and $d_n = d_{n-1}^2 - 2$ for $n > 0$ begins

$$6, -25, -26, 25, -26, \ldots,$$

with $d_4 = d_0$. (This confirms that $e_2(m) = 2$.) Here $t = 4 - 2 = 2$ is the smallest positive integer for which $2^t \equiv \pm 1 \pmod{m/4}$. Since $2^1 = 2 \equiv -1 \pmod 3$, we can eliminate the possibility that $m = 12$. Then since $2^2 = 4 \equiv -1 \pmod 5$ but $4 \not\equiv \pm 1 \pmod{15}$, we conclude that $m = 20$. The suborder sequence of $c = 6$ modulo $p = 59$ begins

$$2, 6, -25, 21, -26, 0, \ldots,$$

which confirms that $m = \text{sub}_{59}(6) = 4(5) = 20$ by part (3) of Corollary 12.4.3.

(d) Let $c = 7$ and $p = 59$. Here $\left(\frac{c+2}{p}\right) = \left(\frac{9}{59}\right) = 1$ and $\left(\frac{c-2}{p}\right) = \left(\frac{5}{59}\right) = 1$, so we know that $m = \text{sub}_{59}(7)$ divides $p - 1 = 58$ with $e_2(m) < e_2(58)$. The only possibility is $m = 29$ (since $m = 1$ only for $c = 2$ in $\mathbb{F}_p$). The suborder subsequence with $d_0 = 8$ and $d_n = d_{n-1}^2 - 2$ for $n > 0$ begins

$$7, -12, 24, -16, 18, 27, 19, 5, 23, -4, 14, 17, -8, 3, 7, \ldots,$$

with $d_{14} = d_0$. We can confirm that $t = 14$ is the smallest positive integer for which $2^t \equiv \pm 1 \pmod{29}$. From the suborder sequence for $c = 7$,

$$2, 7, -12, 27, 24, 23, 19, -8 - 16, 14, -4, 17, 5, 18, 3, 3, \ldots,$$

with $c_{14} = c_{15}$, we also see that $m = \text{sub}_{59}(7) = 2(14) + 1 = 29$.

(e) Let $c = 3$ and $p = 61$. Then $\left(\frac{c+2}{p}\right) = \left(\frac{5}{61}\right) = 1$ and $\left(\frac{c-2}{p}\right) = \left(\frac{1}{61}\right) = 1$, so that $m = \text{sub}_{61}(3)$ divides $p - 1 = 60$ with $e_2(m) < e_2(60)$. We can eliminate $m = 1$, 2, 3, and 6 by Proposition 12.3.2, but remaining possibilities are $m = 5$, 10, 15, or 30. The suborder subsequence with $d_0 = 3$ and $d_n = d_{n-1}^2 - 2$ for $n > 0$ begins

$$3, 7, -14, 11, -3, 7, \ldots,$$

with $d_5 = d_1$. It follows that $e_2(m) = 1$ (so that $m = 10$ or 30) and that $t = 5 - 1 = 4$ is the smallest positive integer for which $2^t \equiv \pm 1 \pmod{m/2}$. Since $2^2 = 4 \equiv -1 \pmod 5$, we can eliminate the possibility that $m = 10$, and conclude that $m = 30$. The suborder sequence with $c = 3$,

$$2, 3, 7, 18, -14, 1, \ldots,$$

confirms that $\text{sub}_{61}(3) = 6(5) = 30$.

(f) If $c = 4$ and $p = 61$, then $\left(\frac{c+2}{p}\right) = \left(\frac{6}{61}\right) = -1$ and $\left(\frac{c-2}{p}\right) = \left(\frac{2}{61}\right) = -1$. Thus $m = \text{sub}_{61}(4)$ divides $p - 1 = 60$ with $e_2(m) = e_2(60)$. Possibilities are $m = 12$, 20, or 60. The suborder subsequence with $d_0 = 4$ and $d_n = d_{n-1}^2 - 2$ for $n > 0$ begins

$$4, 14, 11, -3, 7, -14, 11, \ldots,$$

with $d_6 = d_2$. This confirms that $e_2(m) = 2$, and we know further that $t = 6 - 2 = 4$ is the smallest positive integer for which $2^t \equiv \pm 1 \pmod{m/4}$. Since $2^1 = 2 \equiv -1 \pmod 3$ and $2^2 = 4 \equiv -1 \pmod 5$, the only possibility is $m = 60$ (with $2^4 = 16 \equiv 1 \pmod{15}$). The suborder sequence with $c = 4$,

$$2, 4, 14, -9, 11, -8, 18, 19, -3, 30, 1, \ldots,$$

confirms that $\text{sub}_{61}(4) = 6(10) = 60$.

(8) In each part, we consider divisors m of $p - 1$ or $p + 1$ other than 1, 2, 3, 4, and 6, and confirm, using Table 13.1, that the number of elements c of $\mathbb{F}_p$ with $\text{sub}_p(c) = m$ is $\frac{\phi(m)}{2}$. (There is precisely one element with $m = 1$, 2, 3, 4, 6 for $p > 3$ by Proposition 12.3.2.)

(a) Let $p = 17$. For divisors of $p - 1 = 16$, we find that $\text{sub}_{17}(c) = 8$ for $c = \pm 6$ and $\text{sub}_{17}(c) = 16$ for $c = \pm 5, \pm 8$. We verify that $\frac{\phi(8)}{2} = 2$ and $\frac{\phi(16)}{2} = 4$. For divisors of $p + 1 = 18$, we have $\text{sub}_{17}(c) = 9$ for $c = -3, -4, 7$ and $\text{sub}_{17}(c) = 18$ for $c = 3, 4, -7$. Here $\frac{\phi(9)}{2} = 3 = \frac{\phi(18)}{2}$.

(b) Let $p = 19$. For divisors of $p - 1 = 18$, we find $\text{sub}_{19}(c) = 9$ for $c = 3, 7, 9$ and $\text{sub}_{19}(c) = 18$ for $c = -3, -7, -9$. For divisors of $p + 1 = 20$, we have $\text{sub}_{19}(c) = 5$ for $c = 4, -5$, $\text{sub}_{19}(c) = 10$ for $c = -4, 5$, and $\text{sub}_{19}(c) = 20$ for $c = \pm 6, \pm 8$. These are the predicted number of values in each case.

(c) Let $p = 29$. For divisors of $p-1 = 28$, we have $\text{sub}_{29}(c) = 7$ for $c = 3, 7, -11$, $\text{sub}_{29}(c) = 14$ for $c = -3, -7, 11$, and $\text{sub}_{29}(c) = 28$ for $c = \pm 10, \pm 12, \pm 13$. For divisors of $p+1 = 30$, we have $\text{sub}_{29}(c) = 5$ for $c = 5, -6$, $\text{sub}_{29}(c) = 10$ for $c = -5, 6$, $\text{sub}_{29}(c) = 15$ for $c = 4, -8, -9, 14$, and $\text{sub}_{29}(c) = 30$ for $c = -4, 8, 9, -14$.

(d) Let $p = 31$. For divisors of $p-1 = 30$, we have $\text{sub}_{31}(c) = 5$ for $c = 12, -13$, $\text{sub}_{31}(c) = 10$ for $c = -12, 13$, $\text{sub}_{31}(c) = 15$ for $c = 3, 6, 7, -15$, and $\text{sub}_{31}(c) = 30$ for $c = -3, -6, -7, 15$. For divisors of $p+1 = 32$, we have $\text{sub}_{31}(c) = 8$ for $c = \pm 8$, $\text{sub}_{31}(c) = 16$ for $c = \pm 5, \pm 14$, and $\text{sub}_{31}(c) = 32$ for $c = \pm 4, \pm 9, \pm 10, \pm 11$.

(e) Let $p = 37$. For divisors of $p-1 = 36$, we have $\text{sub}_{37}(c) = 9$ for $c = 5, 9, -14$, $\text{sub}_{37}(c) = 12$ for $c = \pm 15$, $\text{sub}_{37}(c) = 18$ for $c = -5, -9, 14$, and $\text{sub}_{37}(c) = 36$ for $c = \pm 4, \pm 16, \pm 17$. For divisors of $p+1 = 38$, we have $\text{sub}_{37}(c) = 19$ for

$$c = -3, -6, 7, 8, 10, -11, -12, -13, -18$$

and $\text{sub}_{37}(c) = 38$ for

$$c = 3, 6, -7, -8, -10, 11, 12, 13, 18.$$

(Note that $\frac{\phi(19)}{2} = 9 = \frac{\phi(38)}{2}$.)

(f) Let $p = 43$. For divisors of $p-1 = 42$, we have $\text{sub}_{43}(c) = 7$ for $c = 8, 15, 19$, $\text{sub}_{43}(c) = 14$ for $c = -8, -15, -19$, $\text{sub}_{43}(c) = 21$ for $c = -5, -10, 11, 12, 13, -20$, and $\text{sub}_{43}(c) = 42$ for $c = 5, 10, -11, -12, -13, 20$. For divisors of $p+1 = 44$, we have $\text{sub}_{43}(c) = 11$ for $c = 4, -7, 9, 14, -21$, $\text{sub}_{43}(c) = 22$ for $c = -4, 7, -9, -14, 21$, and $\text{sub}_{43}(c) = 44$ for $c = \pm 3, \pm 6, \pm 16, \pm 17, \pm 18$.

(g) Let $p = 47$. For divisors of $p-1 = 46$, we have $\text{sub}_{47}(c) = 23$ for

$$c = 4, 5, 6, 10, -13, 14, 16, -17, 19, -21, 23$$

and $\text{sub}_{47}(c) = 46$ for

$$c = -4, -5, -6, -10, 13, -14, -16, 17, -19, 21, -23.$$

For divisors of $p+1 = 48$, we have $\text{sub}_{47}(c) = 8$ for $c = \pm 7$, $\text{sub}_{47}(c) = 12$ for $c = \pm 12$, $\text{sub}_{47}(c) = 16$ for $c = \pm 3, \pm 18$, $\text{sub}_{47}(c) = 24$ for $c = \pm 15, \pm 22$, and $\text{sub}_{47}(c) = 48$ for $c = \pm 8, \pm 9, \pm 11, \pm 20$.

Section 13.1. Recursive Sequences and Automorphs.

(1) In each part, applying the equivalence algorithm of Theorem 10.1.2 to the quadratic form $\phi = (1:0)$ produces the smallest solution $(x, y) = (q, r)$ in positive integers of $\phi(x, y) = 1$, as in Theorem 11.1.1. We omit those calculations.

(a) For $\Delta = 8$, the smallest positive solution of $\phi(x, y) = x^2 - 2y^2 = 1$ is $(q, r) = (3, 2)$. Here $b = 0$ (for $\phi(x, y) = x^2 + bxy + cy^2$), and so the sequence of Theorem 13.1.2 is defined by $a_n = 6a_{n-1} - a_{n-2}$ with $a_0 = 0$ and $a_1 = 1$. The following table lists the terms of this sequence for $1 \le n \le 4$, along with the four smallest positive solutions $(x, y) = (q_n, r_n)$ of $x^2 - 2y^2 = 1$, produced by the equations $q_n = a_n q - a_{n-1} = 3a_n - a_{n-1}$ and $r_n = a_n r = 2a_n$ of $x^2 - 2y^2 = 1$.

n	1	2	3	4
a_n	1	6	35	204
q_n	3	17	99	577
r_n	2	12	70	408

(b) For $\Delta = 12$, $(q, r) = (2, 1)$ is the smallest positive solution of $\phi(x, y) = x^2 - 3y^2 = 1$, and we let $a_n = 4a_{n-1} - a_{n-2}$ with $a_0 = 0$ and $a_1 = 1$. We obtain all other positive

solutions of $\phi(x,y)=1$ as (q_n,r_n) with $q_n=2a_n-a_{n-1}$ and $r_n=a_n$. The first four solutions are as in the following table.

n	1	2	3	4
a_n	1	4	15	56
q_n	2	7	26	97
r_n	1	4	15	56

(c) For $\Delta=13$, $\phi(x,y)=x^2+xy-3y^2=1$ has smallest positive solution $(q,r)=(4,3)$. Here we let $a_n=(2q+br)a_{n-1}-a_{n-2}=11a_{n-1}-a_{n-2}$ (where $b=1$ is the coefficient of xy in $\phi(x,y)$) and with $a_0=0$ and $a_1=1$ as always. All positive integer solutions (q_n,r_n) of $\phi(x,y)=1$ are given by $q_n=4a_n-a_{n-1}$ and $r_n=3a_n$.

n	1	2	3	4
a_n	1	11	120	1309
q_n	4	43	469	5116
r_n	3	33	360	3927

(d) For $\Delta=17$, $\phi(x,y)=x^2+xy-4y^2=1$ has smallest positive solution $(q,r)=(25,16)$. So $a_n=66a_{n-1}-a_{n-2}$, with $q_n=25a_n-a_{n-1}$ and $r_n=16a_n$ producing all positive solutions of $\phi(x,y)=1$.

n	1	2	3	4
a_n	1	66	4355	287364
q_n	25	1649	108809	7179745
r_n	16	1056	69680	4597824

(e) For $\Delta=21$, $(q,r)=(2,1)$ is the smallest positive solution of $\phi(x,y)=x^2+xy-5y^2=1$, and $a_n=5a_{n-1}-a_{n-2}$. Here $q_n=2a_n-a_{n-1}$ and $r_n=a_n$ produce all positive solutions of $\phi(x,y)=1$.

n	1	2	3	4
a_n	1	5	24	115
q_n	2	9	43	206
r_n	1	5	24	115

(f) For $\Delta=24$, $(q,r)=(5,2)$ is the smallest positive solution of $\phi(x,y)=x^2-6y^2=1$, and $a_n=10a_{n-1}-a_{n-2}$. So $q_n=5a_n-a_{n-1}$ and $r_n=2a_n$ produce all positive solutions of $\phi(x,y)=1$.

n	1	2	3	4
a_n	1	10	99	980
q_n	5	49	485	4801
r_n	2	20	198	1960

(g) For $\Delta=28$, $(q,r)=(8,3)$ is the smallest positive solution of $\phi(x,y)=x^2-7y^2=1$, and $a_n=16a_{n-1}-a_{n-2}$. Here $q_n=8a_n-a_{n-1}$ and $r_n=3a_n$ produce all positive solutions of $\phi(x,y)=1$.

n	1	2	3	4
a_n	1	16	255	4064
q_n	8	127	2024	32257
r_n	3	48	765	12192

(h) For $\Delta = 33$, $\phi(x, y) = x^2 + xy - 8y^2 = 1$ has smallest positive solution $(q, r) = (19, 8)$. So $a_n = 46a_{n-1} - a_{n-2}$, and $q_n = 19a_n - a_{n-1}$ and $r_n = 8a_n$ produce all positive solutions of $\phi(x, y) = 1$.

n	1	2	3	4
a_n	1	46	2115	97244
q_n	19	873	40139	1845521
r_n	8	368	16920	777952

(i) For $\Delta = 37$, $\phi(x, y) = x^2 + xy - 9y^2 = 1$ has smallest positive solution $(q, r) = (61, 24)$. So $a_n = 146a_{n-1} - a_{n-2}$, and $q_n = 61a_n - a_{n-1}$ and $r_n = 24a_n$ produce all positive solutions of $\phi(x, y) = 1$.

n	1	2	3	4
a_n	1	146	21315	3111844
q_n	61	8905	1300069	189801169
r_n	24	3504	511560	74684256

(j) For $\Delta = 40$, $(q, r) = (19, 6)$ is the smallest positive solution of $\phi(x, y) = x^2 - 10y^2 = 1$, and $a_n = 38a_{n-1} - a_{n-2}$. Here $q_n = 19a_n - a_{n-1}$ and $r_n = 6a_n$ produce all positive solutions of $\phi(x, y) = 1$.

n	1	2	3	4
a_n	1	38	1443	54796
q_n	19	721	27379	1039681
r_n	6	228	8658	328776

(k) For $\Delta = 41$, $\phi(x, y) = x^2 + xy - 10y^2 = 1$ has smallest positive solution $(q, r) = (1729, 640)$. So $a_n = 4098a_{n-1} - a_{n-2}$, and $q_n = 1729a_n - a_{n-1}$ and $r_n = 640a_n$ produce all positive solutions of $\phi(x, y) = 1$.

n	1	2	3	4
a_n	1	4098	16793603	68820180996
q_n	1729	7085441	29036135489	118990076148481
r_n	640	2622720	10747905920	44044915837440

Section 13.2. An Application to Pell's Equation.

(1) We apply Pell's equation algorithm (Theorem 9.2.2) to $d = 847$ compiling the following data.

i	0	1	2	3	4	5	6	7	8	9	10
a	1	6	37	19	9	7	9	19	37	6	1
k	0	-29	-25	-12	-26	-28	-28	-26	-12	-25	-29
q	29	9	1	2	6	8	5	2	1	9	58
m	29	262	291	844	5355	43684	267459	578602	846061	8193151	
n	1	9	10	29	184	1501	9190	19881	29071	281520	

Here $k_1 = -29$ is the smallest integer with $d - k_1^2$ is positive, and so $a_1 = \frac{847-(-29)^2}{1} = 6$. Now $k_2 = -25$ is the smallest integer with $k_2 \geq -29$ for which $k_2 \equiv -k_1 \pmod{a_1}$, and then $a_2 = \frac{847-(-25)^2}{6} = 37$. Continuing this process, we find that $a_{10} = 1$, and the terms of the q_i, m_i, and n_i sequences are as defined in Theorem 9.2.2. The fundamental solution of $x^2 - 847y^2 = 1$ is given by $(m_9, n_9) = (8193151, 281520)$.

(2) In parts (a)–(e), the fundamental solution of $x^2 - 2y^2 = 1$ is $(q, r) = (3, 2)$, and so we let $a_n = 6a_{n-1} - a_{n-2}$ with $a_0 = 0$ and $a_1 = 1$.

(a) Let $d = 18 = 2 \cdot 3^2$, so that $p = 3$. Since p divides q, we know that p divides r_2. Thus

$$(3 + 2\sqrt{2})^2 = 17 + 12\sqrt{2} = 17 + 4\sqrt{18}$$

is the fundamental solution of $x^2 - 18y^2 = 1$. We can verify this with the Pell's equation algorithm of Theorem 9.2.2 applied to $d = 18$.

i	0	1	2
a	1	2	1
k	0	-4	-4
q	4	4	8
m	4	17	
n	1	4	

(b) Let $d = 50 = 2 \cdot 5^2$, with $p = 5$. Here $\left(\frac{2}{5}\right) = -1$, so the smallest m for which p divides r_m is a divisor of $\frac{p+1}{2} = 3$. Since p does not divide $r_1 = 2$, we conclude that $m = 3$, and so

$$(3 + 2\sqrt{2})^3 = 99 + 70\sqrt{2} = 99 + 14\sqrt{50}$$

is the fundamental solution of $x^2 - 50y^2 = 1$. The following table verifies this claim.

i	0	1	2
a	1	1	1
k	0	-7	-7
q	7	14	14
m	7	99	
n	1	14	

(c) Let $d = 98 = 2 \cdot 7^2$, with $p = 7$. Since $\left(\frac{2}{7}\right) = 1$, the smallest m for which p divides r_m is a divisor of $\frac{p-1}{2} = 3$. Again, p does not divide $r_1 = 2$, so we conclude that $m = 3$, and

$$(3 + 2\sqrt{2})^3 = 99 + 70\sqrt{2} = 99 + 10\sqrt{98}$$

is the fundamental solution of $x^2 - 98y^2 = 1$. To verify:

i	0	1	2	3	4
a	1	17	2	17	1
k	0	-9	-8	-8	-9
q	9	1	8	1	18
m	9	10	89	99	
n	1	1	9	10	

(d) Let $d = 242 = 2 \cdot 11^2$, with $p = 11$. Here $\left(\frac{2}{11}\right) = -1$, so the smallest m for which p divides r_m is a divisor of $\frac{p+1}{2} = 6$. From previous calculations, we see that p does not divide $r_1 = 2$, $r_2 12$, or $r_3 = 70$, and so we conclude that $m = 6$.

$$(3 + 2\sqrt{2})^6 = (99 + 70\sqrt{2})^2 = 19601 + 13860\sqrt{2} = 19601 + 1260\sqrt{242}$$

is the fundamental solution of $x^2 - 242y^2 = 1$. To verify:

i	0	1	2	3	4	5	6	7	8	9	10
a	1	17	14	7	23	2	23	7	14	17	1
k	0	-15	-2	-12	-9	-14	-14	-9	-12	-2	-15
q	15	1	1	3	1	14	1	3	1	1	30
m	15	16	31	109	140	2069	2209	8696	10905	19601	
n	1	1	2	7	9	133	142	559	701	1260	

(e) Let $d = 450 = 2 \cdot 15^2$, with $p = 11$. In part (a), we saw that 3 divides r_2 and so divides r_{2k} for every k. Likewise from part (b), we have that 5 divides r_3 and so divides r_{3k} for every k. Thus 15 divides r_6.

$$(3 + 2\sqrt{2})^6 = 19601 + 13860\sqrt{2} = 19601 + 924\sqrt{450}$$

is the fundamental solution of $x^2 - 450y^2 = 1$.

i	0	1	2	3	4	5	6	7	8
a	1	9	25	14	9	14	25	9	1
k	0	−21	−15	−10	−18	−18	−10	−15	−21
q	21	4	1	2	4	2	1	4	42
m	21	85	106	297	1294	2885	4179	19601	
n	1	4	5	14	61	136	197	924	

(f) The fundamental solution of $x^2 - 5y^2 = 1$ is $(q, r) = (9, 4)$, or $v = 9 + 4\sqrt{5}$. Since 2 divides r, then $9 + 2\sqrt{20}$ is the fundamental solution of $x^2 - 20y^2 = 1$. We verify this with the Pell's equation algorithm as follows.

i	0	1	2
a	1	4	1
k	0	−4	−4
q	4	2	8
m	4	9	
n	1	2	

(g) Since 3 divides q in the fundamental solution of $x^2 - 5y^2 = 1$, then

$$(9 + 4\sqrt{5})^2 = 161 + 72\sqrt{5} = 161 + 24\sqrt{45}$$

is the fundamental solution of $x^2 - 45y^2 = 1$. To verify:

i	0	1	2	3	4	5	6
a	1	9	4	5	4	9	1
k	0	−6	−3	15	−5	−3	−6
q	6	1	2	2	2	1	12
m	6	7	20	47	114	161	
n	1	1	3	7	17	24	

(h) Since 2 divides r and 3 divides q in the fundamental solution of $x^2 - 5y^2 = 1$, we also find that

$$(9 + 4\sqrt{5})^2 = 161 + 72\sqrt{5} = 161 + 12\sqrt{180}$$

is the fundamental solution of $x^2 - 180y^2 = 1$. To verify:

i	0	1	2	3	4
a	1	11	9	11	1
k	0	−13	−9	−9	−13
q	13	2	2	2	26
m	13	27	67	161	
n	1	2	5	12	

(i) The fundamental solution of $x^2 - 7y^2 = 1$ is $q + r\sqrt{7} = 8 + 3\sqrt{7}$. Since 3 divides r, we also have that $8 + \sqrt{63}$ is the fundamental solution of $x^2 - 63y^2 = 1$. To verify:

i	0	1	2
a	1	14	1
k	0	-7	-7
q	7	1	14
m	7	8	
n	1	1	

(j) The fundamental solution of $x^2 - 10y^2 = 1$ is $q + r\sqrt{7} = 19 + 3\sqrt{10}$. Again 3 divides r, so we also have that $19 + \sqrt{90}$ is the fundamental solution of $x^2 - 90y^2 = 1$.

i	0	1	2
a	1	9	1
k	0	-9	-9
q	9	2	18
m	9	19	
n	1	1	

Section 13.3. Quadratic Subdomains of Positive Discriminant.

(1) For each Δ, we let (q, r) be the smallest positive solution of $\phi(x, y) = 1$, where $\phi(x, y) = x^2 + \varepsilon xy + \frac{\varepsilon^2 - \Delta}{4} y^2$. If $a_n = (2q + \varepsilon r)a_{n-1} - a_{n-2}$ with $a_0 = 0$ and $a_1 = 1$, then s_p is the smallest positive integer so that p divides $r a_{s_p}$, and the order of the kernel of the projection homomorphism from $\mathcal{F}_{p^2\Delta}$ to $\mathcal{F}_\Delta$ is given by $|K(\Delta, p)| = \frac{p - \left(\frac{\Delta}{p}\right)}{s_p}$. If p divides r, then $s_p = 1$; otherwise s_p is the suborder of the sequence a_n modulo p. Notice that for each Δ, the suborder number of the characteristic polynomial of a_n (as in Theorem 12.3.3) is $c = (2q + \varepsilon r)^2 - 2$ for every prime p.

(a) If $\Delta = 8$, then $(q, r) = (3, 2)$ and $a_n = 6a_{n-1} - a_{n-2}$, with suborder number $c = 34$. We list c modulo odd primes p, along with s_p, and $|K(\Delta, p)|$ for each prime $p < 20$ in the following table.

p	2	3	5	7	11	13	17	19
c	$-$	-2	-1	-1	1	-5	0	-4
s_p	1	2	3	3	6	7	4	10
$\lvert K\rvert$	2	2	2	2	2	2	4	2

Here $s_2 = 1$ since $r = 2$, and calculation of s_p for all other primes comes from Proposition 12.3.2 or Table 12.1.

(b) If $\Delta = 12$, then $(q, r) = (2, 1)$ and $a_n = 4a_{n-1} - a_{n-2}$, with suborder number $c = 14$.

p	2	3	5	7	11	13	17	19
c	$-$	2	-1	0	3	1	-3	-5
s_p	2	3	3	4	5	6	9	5
$\lvert K\rvert$	1	1	2	2	2	2	2	4

When 2 does not divide r, as in this case, then $s_2 = 2$ or 3 depending on whether $2q + \varepsilon r$ is even or odd. Note that when $c \equiv 2 \pmod{p}$, then the suborder of the sequence a_n modulo p equals p. (See Theorem 12.3.3.)

(c) If $\Delta = 13$, then $(q, r) = (4, 3)$ and $a_n = 11a_{n-1} - a_{n-2}$, with suborder number $c = 119$.

p	2	3	5	7	11	13	17	19
c	$-$	2	-1	0	-2	2	0	5
s_p	3	1	3	4	2	13	4	10
$\lvert K\rvert$	1	2	2	2	6	1	4	2

Here $s_3 = 1$ since 3 divides r.

(d) If $\Delta = 17$, then $(q, r) = (25, 16)$ and $a_n = 66a_{n-1} - a_{n-2}$, with $c = 4354$.

p	2	3	5	7	11	13	17	19
c	$-$	-2	-1	0	-2	-1	2	3
s_p	1	2	3	4	2	3	17	9
$\lvert K\rvert$	1	2	2	2	6	4	1	2

(e) If $\Delta = 21$, then $(q, r) = (2, 1)$ and $a_n = 5a_{n-1} - a_{n-2}$, with $c = 23$.

p	2	3	5	7	11	13	17	19
c	$-$	2	-2	2	1	-3	6	4
s_p	3	3	2	7	6	7	8	5
$\lvert K\rvert$	1	1	2	1	2	2	2	4

(f) If $\Delta = 24$, then $(q, r) = (5, 2)$ and $a_n = 10a_{n-1} - a_{n-2}$, with $c = 98$.

p	2	3	5	7	11	13	17	19
c	$-$	2	-2	0	-1	-6	-4	3
s_p	1	3	2	4	3	7	9	9
$\lvert K\rvert$	2	1	2	2	4	2	2	2

(g) If $\Delta = 28$, then $(q, r) = (8, 3)$ and $a_n = 16a_{n-1} - a_{n-2}$, with $c = 254$.

p	2	3	5	7	11	13	17	19
c	$-$	2	-1	2	1	-6	-1	7
s_p	2	1	3	7	6	7	3	9
$\lvert K\rvert$	1	2	2	1	2	2	6	2

(h) If $\Delta = 33$, then $(q, r) = (19, 8)$ and $a_n = 46a_{n-1} - a_{n-2}$, with $c = 2114$.

p	2	3	5	7	11	13	17	19
c	$-$	2	-1	0	2	-5	6	5
s_p	1	3	3	4	11	7	8	10
$\lvert K\rvert$	1	1	2	2	1	2	2	2

(i) If $\Delta = 37$, then $(q, r) = (61, 24)$ and $a_n = 146a_{n-1} - a_{n-2}$, with $c = 21314$.

p	2	3	5	7	11	13	17	19
c	$-$	2	-1	-1	-4	-6	-4	-4
s_p	1	1	3	3	5	7	9	10
$\lvert K\rvert$	3	2	2	2	2	2	2	2

(j) If $\Delta = 40$, then $(q, r) = (19, 6)$ and $a_n = 38a_{n-1} - a_{n-2}$, with $c = 1442$.

p	2	3	5	7	11	13	17	19
c	$-$	2	2	0	1	-1	-3	-2
s_p	1	1	5	4	6	3	9	2
$\lvert K\rvert$	2	3	1	2	2	4	2	10

(k) If $\Delta = 41$, then $(q, r) = (1729, 640)$ and $a_n = 4098a_{n-1} - a_{n-2}$, with $c = 16793602$.

p	2	3	5	7	11	13	17	19
c	$-$	-2	2	0	1	-6	-1	-4
s_p	1	2	1	4	6	7	3	10
$\lvert K\rvert$	3	2	5	2	2	2	6	2