Chapter 7
The Pell Equation

Complex quadratic number rings have finitely many units; in the real quadratic case, the rings of integers of $\mathbb{Q}(\sqrt{m})$ seem to contain a unit ε of infinite order:

m	2	3	5	6	7
ε	$1+\sqrt{2}$	$2+\sqrt{3}$	$\frac{1}{2}(1+\sqrt{5})$	$5+2\sqrt{6}$	$8+3\sqrt{7}$

The existence of nontrivial units $\varepsilon = \frac{x+y\sqrt{m}}{2}$ in real quadratic number fields $\mathbb{Q}(\sqrt{m})$ is equivalent to the solvability of the *Pell equation* $x^2 - my^2 = \pm 4$ in nonzero integers for all squarefree values of $m > 0$. In this chapter we will prove that the equation $x^2 - my^2 = 1$ has a nontrivial[1] solution in integers whenever $m > 0$ is not a square, and we will provide methods for computing units in real quadratic number fields.

Before we prove the solvability of the Pell equation, we make a few remarks on the connection between the equations $x^2-my^2 = \pm 4$ and the equation $x^2-my^2 = 1$ and on how to compute the fundamental unit of $\mathbb{Q}(\sqrt{m})$ from the minimal nontrivial solution of $x^2 - my^2 = 1$ and vice versa.

Consider for example the case $m = 13$. Here the fundamental unit of the ring of integers $\mathcal{O}_k$ of the quadratic number field $k = \mathbb{Q}(\sqrt{13})$ is $\varepsilon = \frac{3+\sqrt{13}}{2}$, which corresponds to the solution $(3, 1)$ of the Pell equation $x^2 - 13y^2 = -4$. The unit $\varepsilon^3 = 18 + 5\sqrt{13}$ is a unit in the order $\mathbb{Z}[\sqrt{13}\,]$ and corresponds to the fundamental solution $(18, 5)$ of the Pell equation $x^2 - 13y^2 = -1$. Finally the unit $\varepsilon^6 = 649 + 180\sqrt{13}$ corresponds to the minimal nontrivial solution $(649, 180)$ of the Pell equation $x^2 - 13y^2 = 1$.

[1]By this we mean solutions with $y \neq 0$.

F. Lemmermeyer, *Quadratic Number Fields*, Springer Undergraduate Mathematics Series, https://doi.org/10.1007/978-3-030-78652-6_7

Proposition 7.1 *If* $k = \mathbb{Q}(\sqrt{m})$ *for some squarefree integer* $m \equiv 1 \bmod 4$*, and if* ε *is a unit in* $\mathcal{O}_k$*, then* ε^3 *is a unit in the order* $\mathbb{Z}[\sqrt{m}\,]$.

In other words, if $t^2 - mu^2 = \pm 4$*, then* $T^2 - mU^2 = \pm 1$*, where*

$$T + U\sqrt{m} = \Big(\frac{t + u\sqrt{m}}{2}\Big)^3.$$

Proof If $t^2 - my^2 = \pm 4$ for odd integers t and u, then reducing this equation modulo 8 shows that $m \equiv 5 \bmod 8$. In this case, the prime ideal (2) is inert in $\mathbb{Q}(\sqrt{m})$; hence, the group of coprime residue classes modulo 2 has order $N(2) - 1 = 3$, and this in turn implies that $\varepsilon^3 \equiv 1 \bmod 2$. □

Clearly, if ε is a unit with norm -1, then ε^2 is a unit with norm $+1$. Thus if we want to compute a fundamental unit from the unit $x + y\sqrt{m}$ corresponding to the smallest positive solution of the Pell equation $x^2 - my^2 = 1$, then we have to check whether ε is a square, a cube, or a sixth power of a unit in $\mathbb{Q}(\sqrt{m})$.

We will explain how to do this in the case at hand. Assume we have the minimal positive solution (649, 180) of the Pell equation $x^2 - 13y^2 = 1$; then $\eta = 649 + 180\sqrt{13}$ is a unit with norm 1 (and the smallest positive unit with norm 1 in the domain $\mathbb{Z}[\sqrt{13}\,]$).

For checking whether $\sqrt{\eta} \in \mathbb{Q}(\sqrt{13})$, we use the real approximations

$$\begin{aligned} \eta &= 649 + 180\sqrt{13} \approx 1297.9992295\ldots, \\ \eta' &= 649 - 180\sqrt{13} \approx \quad\;\; 0.0007704\ldots. \end{aligned}$$

Clearly, the trace $\eta + \eta' = 2 \cdot 649$ is an integer. If η is a square, then the trace of $\sqrt{\eta}$ must also be an integer. We find

$$\begin{aligned} \sqrt{\eta} &\approx 36.0277563773\ldots, \\ \sqrt{\eta'} &\approx \;\; 0.0277563773\ldots. \end{aligned}$$

This shows[2] that $\frac{1}{2}(\sqrt{\eta} - \sqrt{\eta'}) \approx 18$ and $\frac{\sqrt{\eta}+\sqrt{\eta'}}{2\sqrt{13}} \approx 5$ are very close to integers, which in turn suggests that $\sqrt{\eta} = 18 + 10\sqrt{13}$. Now we can readily verify that $(18 + 5\sqrt{13})^2 = \eta$. Observe that $18 - 5\sqrt{13} < 0$, which is why $18 - 5\sqrt{3} \approx -\sqrt{\eta'}$.

In a similar way we can check that η is a cube and in fact a sixth power:

$$\begin{aligned} \sqrt[6]{\eta} &\approx 3.30277563773\ldots, \\ \sqrt[6]{\eta'} &\approx 0.30277563773\ldots, \end{aligned}$$

[2] See Exercise 7.1.

and this time

$$\frac{\sqrt[6]{\eta} - \sqrt[6]{\eta'}}{2} \approx 1.5 \quad \text{and} \quad \frac{\sqrt[6]{\eta} + \sqrt[6]{\eta'}}{2\sqrt{13}} \approx 0.5$$

suggests that $\sqrt[6]{\eta} = \frac{3+\sqrt{13}}{2}$, which can then be verified.

7.1 The Solvability of the Pell Equation

The history of the Pell equation in Europe[3] begins with Fermat's challenge in 1657. In that year, Fermat posed the following problem (among others) and asked his contemporaries, in particular the English mathematicians John Wallis and William Brouncker, for a solution:

> Given an arbitrary natural number, which is assumed to be not a square, there are infinitely many square numbers with the property that after adding 1 to the product of one of these square numbers with the given number, another square is produced [...]. We ask e.g. for a square that produces another square after adding 1 to the product with 149 or 109 or 433 etc.

Thus Fermat asked for solutions of equations such as $Na^2 + 1 = b^2$ for positive nonsquare integers N, in particular for the values $N = 149, 109$, and 433. Brouncker and Wallis solved these equations in rational numbers,[4] and Fermat remarked that he hardly would have posed a problem that any "three-day-arithmetician" could have solved. Brouncker then succeeded in solving Fermat's equation for any given value, but Fermat complained that Brouncker had not shown that his method would always work' and claimed that such a proof is possible using his method of infinite descent. Whether Fermat himself had such a proof is an open question.

Long before Fermat, Indian mathematicians such as Brahmagupta (ca. 598–670) and Bhaskara II (1114–1185) had developed a method for solving the Diophantine equation $Nx^2 + 1 = y^2$; this became known in Europe only rather late and did not have, as far as we know, any influence on the development of number theory in the West.[5]

Leonhard Euler later studied the equation $Na^2 + 1 = b^2$ in several articles, and Joseph-Louis Lagrange succeeded in proving the solvability in integers. His first proof, which already used what later became known as Dirichlet's pigeonhole

[3] Strictly speaking, the investigation of Platon's side and diagonal numbers by Theon may be seen as the only serious investigation of a Pell equation in ancient Greece. Equations of Pell type also figure prominently in the Cattle Problem of Archimedes; it is not known, however, whether there were any attempts at solving this problem before it was discovered by Lessing in 1773.

[4] We have derived the rational parametrization of Pell conics in Theorem 3.1.

[5] An excellent account of Indian mathematics was given by Kim Plofker [104]. For an investigation of the Indian method of solving the equation $Nx^2 + 1 = y^2$, see [114].

principle, was streamlined and generalized by Dirichlet: In his unit theorem, he proved the existence of nontrivial units in all number fields except $\mathbb{Q}$ and complex quadratic number fields.

Below we will prove the solvability of the Pell equation $x^2 - my^2 = 1$ for all natural numbers m that are not squares. The essential idea behind this proof is due to Lagrange, who derived the necessary lemmas from the theory of continued fractions. Dirichlet later replaced Lagrange's arguments by repeated applications of his pigeonhole principle, which simplified the proof considerably. The proof is more or less by descent: From the solvability of an equation $x^2 - my^2 = c$ for some value of $c > 1$, we will deduce the solvability of $x^2 - my^2 = c'$ for some $c' < c$. In order to make this argument work, we will have to exploit the fact that these equations $x^2 - my^2 = c$ have infinitely many solutions.

Dirichlet's pigeonhole principle[6] may be stated as follows:

> If $N + 1$ pearls are put into N pigeonholes, then there must be a pigeonhole containing at least two pearls.

For finding solutions of equations such as $x^2 - my^2 = c$, we observe that if m is large and c is small, then $x^2 \approx my^2$ implies that $\frac{x}{y}$ is an approximation of $\sqrt{m}$. In order to find such approximations, one may use, as Lagrange did, the theory of continued fractions; if we are content with proving the existence of solutions, we may use Dirichlet's pigeonhole principle.

Theorem 7.2 *The equation $x^2 - my^2 = 1$ is solvable in nonzero integers x, y whenever $m > 0$ is not a square.*

We begin with the following lemma.

Lemma 7.3 *If ξ_1 and ξ_2 are two nonzero real numbers such that ξ_1/ξ_2 is irrational, then for any $N \in \mathbb{N}$ there exist integers $A, B \in \mathbb{Z}$, which are not both 0 and satisfy the following inequalities:*

$$|A\xi_1 + B\xi_2| \le \frac{1}{N}(|\xi_1| + |\xi_2|), \quad |A| \le N, \ |B| \le N. \tag{7.1}$$

Proof We assume that ξ_1 and ξ_2 are both positive (otherwise we just have to change the signs of a and b in the proof below). The irrationality of ξ_1/ξ_2 implies that the function

$$f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{R} : (a, b) \longmapsto a\xi_1 + b\xi_2 \tag{7.2}$$

is injective (see Exercise 7.7.17).

There are $(N + 1)^2$ pairs of integers $(a, b) \in [0, N] \times [0, N]$, and for these we have $0 \le f(a, b) \le N(|\xi_1| + |\xi_2|)$. If we divide the interval $[0, N(|\xi_1| + |\xi_2|)]$

[6] It seems that this principle was given a name rather late (in the twentieth century?); a pigeonhole is a drawer, so the last thing you would like to put there are pigeons.

into N^2 subintervals of equal length $\frac{1}{N}(|\xi_1| + |\xi_2|)$, then since $(N+1)^2 > N^2$ there must exist, according to Dirichlet's pigeonhole principle, at least two pairs $(a, b) \neq (a', b')$ with $|f(a, b) - f(a', b')| \leq \frac{1}{N}(|\xi_1| + |\xi_2|)$. Now we set $A = a - a'$ and $B = b - b'$; these integers have the desired properties. □

Corollary 7.4 *Assume that $m \in \mathbb{N}$ is not a square. Then there exists an integer c such that the equation $A^2 - mB^2 = c$ has infinitely many solutions $(A, B) \in \mathbb{Z} \times \mathbb{Z}$.*

Proof By the preceding lemma, there exist numbers $A, B \in \mathbb{Z}$, not both 0, that satisfy the inequalities

$$|A - B\sqrt{m}\,| \leq \frac{1}{N}(1 + \sqrt{m}\,), \; |A| \leq N, \; |B| \leq N. \tag{7.3}$$

The triangle inequality shows that

$$|A + B\sqrt{m}\,| \leq |A| + |B\sqrt{m}\,| \leq (1 + \sqrt{m}\,) \cdot N, \tag{7.4}$$

and multiplying (7.3) and (7.4) yields

$$|A^2 - mB^2| \leq (1 + \sqrt{m}\,)^2. \tag{7.5}$$

Now let $N \to \infty$; then infinitely many distinct pairs (A, B) must occur, since if we had only finitely many, then the set $\{|A - B\sqrt{m}\,| : A, B \in \mathbb{Z}\}$ would possess a minimum, which is impossible because of (7.3).

Since $|A^2 - mB^2|$ is bounded from above by (7.3), there must exist an integer c with $|c| \leq (1 + \sqrt{m}\,)^2$ for which $A^2 - mB^2 = c$ has infinitely many solutions in integers. □

Now we can prove Theorem 7.2. According to Corollary 7.4, there exists an integer $c \neq 0$ such that there are infinitely many pairs (A, B) with $A^2 - mB^2 = c$; here we may clearly assume that $A > 0$. Among these infinitely many solutions, we choose $(c+1)^2$ solutions and consider the residue classes of A and B modulo c; by Dirichlet's pigeonhole principle, there must exist pairs $(A_1, B_1) \neq (A_2, B_2)$ with $A_1 \equiv A_2 \bmod c$ and $B_1 \equiv B_2 \bmod c$. The elements $\eta_j = A_j + B_j\sqrt{m}$ then have the same norms $N\eta_1 = N\eta_2 = c$ and satisfy the congruence $\eta_1 \equiv \eta_2 \bmod c$. It follows from $N(\eta_1/\eta_2) = 1$ that η_1/η_2 is a unit if we can show that this is an algebraic integer. To this end, observe that $\eta_1/\eta_2 = 1 + (\eta_1 - \eta_2)/\eta_2 = 1 + (\eta_1 - \eta_2)\eta_2'/c$. Since the difference $\eta_1 - \eta_2$ is divisible by c by construction, η_1/η_2 is indeed an algebraic integer and thus a unit.

It remains to show that $\eta_1/\eta_2 \neq \pm 1$ is a nontrivial unit. But $\eta_1/\eta_2 \neq 1$ follows from $\eta_1 \neq \eta_2$, and $\eta_1/\eta_2 \neq -1$ follows from the fact that A_1 and A_2 are both positive. This concludes the proof of Theorem 7.2.

We now know that there exist nontrivial units in each real quadratic number field. In fact, it is possible to determine the abstract structure of the unit group: For real quadratic number fields k, we have $\mathcal{O}_k^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$. As we will show in a moment, each unit $\eta \in \mathcal{O}_k^\times$ can be written in the form $\eta = (-1)^s \varepsilon^t$ for some "fundamental unit" ε, and then the map $\lambda : E_k \longrightarrow (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$ defined by $\lambda(\eta) = (s, t)$ provides us with an isomorphism of abelian groups. This is the content of our next theorem.

Theorem 7.5 *If k is a real quadratic number field, then there is a unit $\varepsilon \in \mathcal{O}_k^\times$ with the property that every unit $\eta \in \mathcal{O}_k^\times$ can be written uniquely in the form $\eta = \pm\varepsilon^t$ for some $t \in \mathbb{Z}$. In particular,*

$$\mathcal{O}_k^\times \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}.$$

We immediately see that if ε has the property in Theorem 7.5, then so do the units $\pm\varepsilon^{\pm 1}$. Among these four units, there are two that are positive, and among these exactly one is > 1. This unit $\varepsilon > 1$ will be called the fundamental unit of k.

Proof We identify the numbers $a + b\sqrt{m}$ with those real numbers that correspond to the positive square root of m. The only units $\eta \in \mathcal{O}_k^\times$ with $|\eta| = 1$ then are $\eta = \pm 1$, which follows from irrationality of $\sqrt{m}$.

We claim that among the units with $|\eta| > 1$, there is one with minimal absolute value. Otherwise there would exist a unit (in fact, infinitely many) with $1 < |\eta| < \frac{5}{4}$ (just pick two units that are sufficiently close to the infimum of the absolute values and consider their quotient). Since $|\eta\eta'| = 1$, this implies $\frac{4}{5} < |\eta'| < 1$. If we write $\eta = a + b\sqrt{m}$ (where $2a, 2b \in \mathbb{Z}$), then $2|a| = |\eta + \eta'| \le |\eta| + |\eta'| < \frac{9}{4}$, and hence $|a| \le 1$. Since $a = 0$ is not possible, we must have $a = \pm 1$. Then it follows immediately from $1 < |\eta| < \frac{5}{4}$ that $b = 0$, and hence $\eta = 1$ in contradiction to our assumption.

Let ε be a unit with minimal absolute value > 1. We claim that ε has the properties listed in Theorem 7.5. Otherwise there would exist a unit η with $\varepsilon^n < |\eta| < \varepsilon^{n+1}$ for some $n \in \mathbb{N}$ (the proof is similar to that of Theorem 2.6). But then $\eta\varepsilon^{-n}$ is a unit whose absolute value lies strictly between 1 and $|\varepsilon|$, and this contradicts the choice of ε.

Uniqueness is clear: $\pm\varepsilon^t = \pm\varepsilon^u$ implies $|\varepsilon^{t-u}| = 1$, which in turn implies $t = u$ since ε is irrational. But then the signs must also coincide. $\square$

Remark The proof of the solvability of the Pell equation $t^2 - mu^2 = 1$ given here does not provide us with a method of computing the fundamental unit, except for very small values of m. For example, $\varepsilon = 48842 + 5967\sqrt{67}$ is the fundamental unit of $\mathbb{Q}(\sqrt{67})$, and this solution is hard to find by solving the Pell equation by brute force (i.e., looking for an integer $m = 1, 2, 3, \ldots$ such that $mu^2 + 1 = t^2$ is a square). A much better way of computing the fundamental unit of quadratic number fields with modest discriminants is based on the theory of continued fractions. For number fields of higher degree, the computation of the unit group becomes time consuming with growing degree and discriminant even when using the best algorithms that are known today.[7]

[7] Good sources for the state of the art are [20, 91], and, in particular, [66].

7.1.1 The Negative Pell Equation

The equation $t^2 - mu^2 = -1$ is called the *negative Pell equation* or sometimes the anti-Pell equation. In this section we will show how to derive solvability conditions for the negative Pell equation from the solvability of the usual Pell equation.

We begin by considering the equation $t^2 - pu^2 = 1$ for prime values of p. We can write this equation in the form

$$pu^2 = t^2 - 1 = (t-1)(t+1).$$

The greatest common divisor of $t+1$ and $t-1$ divides their difference 2, and hence one of the following four possibilities must occur:

$$\begin{aligned} t+1 &= a^2, & t-1 &= pb^2, \\ t+1 &= pb^2, & t-1 &= a^2, \\ t+1 &= 2a^2, & t-1 &= 2pb^2, \\ t+1 &= 2pb^2, & t-1 &= 2a^2. \end{aligned}$$

We choose the integers a and b positive. Subtracting the right equation from the left, we find that at least one of the following four equations must be solvable in integers:

$$a^2 - pb^2 = 2; \quad a^2 - pb^2 = -2; \quad a^2 - pb^2 = 1; \quad a^2 - pb^2 = -1.$$

If we assume that (t, u) is the smallest positive solution of the Pell equation, then we can exclude the equation $a^2 - pb^2 = 1$ since $t + 1 = 2a^2$ implies that $a < t$.

A necessary condition for the equation $a^2 - pb^2 = 2$ to be solvable is that $p \equiv \pm 1 \bmod 8$. Similar considerations yield the following table:

	$p \equiv 3 \bmod 8$	$p \equiv 5 \bmod 8$	$p \equiv 7 \bmod 8$
$a^2 - pb^2 = +2$	x	x	
$a^2 - pb^2 = -2$		x	x
$a^2 - pb^2 = -1$	x		x

Here “x” represents the unsolvability of the corresponding equation.

If $p \equiv 1 \bmod 8$, it follows from $t^2 - pu^2 = 1$ that t must be odd and thus $\gcd(t-1, t+1) = 2$. Therefore the first three cases are impossible, and we end up with the equation $a^2 - pb^2 = -1$.

Since, as we have seen, one of the three equations must be solvable, we obtain the following:

Proposition 7.6 *The solvability of $t^2 - pu^2 = 1$ for odd prime numbers p implies the solvability of*

$$\begin{aligned} a^2 - pb^2 &= -1 && \textit{for } p \equiv 1 \bmod 4, \\ a^2 - pb^2 &= -2 && \textit{for } p \equiv 3 \bmod 8, \\ a^2 - pb^2 &= +2 && \textit{for } p \equiv 7 \bmod 8. \end{aligned}$$

Even if the equation $a^2 - pb^2 = \pm 2$ for some prime $p \equiv 1 \bmod 8$ is not solvable in integers, the ring of integers in $k = \mathbb{Q}(\sqrt{p})$ might contain elements of norm ± 2, as the example $N(\frac{5+\sqrt{17}}{2}) = 2$ shows.

7.2 Which Numbers Are Norms?

The only method we know so far for showing the unsolvability of the norm equation $x^2 - my^2 = c$ for given values of $m \in \mathbb{N}$ and $c \in \mathbb{Z}$ is reducing the equation modulo n for some choice of n, where n in general is a divisor of m or c, and showing that the congruence does not have a solution. For example, $x^2 - 10y^2 = \pm 2$ is not solvable in integers since the congruence $x^2 \equiv \pm 2 \bmod 5$ does not have solutions. This method does not work in the case of the equation $x^2 - 79y^2 = \pm 3$, the reason being that $x^2 - 79y^2 = -3$ has the rational solution $x = \frac{2}{5}$, $y = \frac{1}{5}$; in particular, this equation is solvable module each modulus coprime to 5. Similarly, the solutions $x = \frac{13}{7}$ and $y = \frac{2}{7}$ show that the congruence is solvable for each modulus coprime to 7. This implies by the Chinese remainder theorem that $x^2 - 79y^2 \equiv -3 \bmod m$ is solvable for each nonzero modulus $m \in \mathbb{Z}$.

Remark Hasse's Local–Global Principle for quadratic forms implies that equations such as $x^2 - my^2 = c$ have rational solutions if and only if the congruence $x^2 - my^2 \equiv c \bmod N$ is solvable for each modulus N. The example above implies that there is no similar Local–Global Principle for integral solutions of such equations. For cubic equations such as $y^2 = x^3 - m$ even the Local–Global Principle for rational solutions does not hold. In the case of integral solutions of $x^2 - my^2 = c$, the class group $\mathrm{Cl}(k)$ of $k = \mathbb{Q}(\sqrt{m})$ is a measure for the obstruction to the Local–Global Principle in the sense that if the class group of k is trivial, the equation $x^2 - my^2 = c$ is solvable in integers if and only if the congruence $x^2 - my^2 \equiv c \bmod N$ is solvable for each modulus N. In the case of elliptic curves, there is a similar group called the Tate–Shafarevich group. Understanding the failure of Local–Global principles is a central area of research in modern number theory.

In order to show that $x^2 - 79y^2 = -3$ does not have integral solutions, we have to employ a different technique. Let us consider an arbitrary real quadratic number field $k = \mathbb{Q}(\sqrt{m})$, and let $\varepsilon = t + u\sqrt{m} > 1$ be the fundamental unit (we allow t and u to be half-integers). Assume moreover that $\alpha \in \mathcal{O}_k$ is a solution of the equation

$|N\alpha| = c$. The basic idea is to choose the exponent n in $\beta = \alpha\varepsilon^n$ in such a way that the coefficients of β with respect to the basis $\{1, \sqrt{m}\}$ become as small as possible. It is clear from geometric considerations that there exists an exponent $n \in \mathbb{Z}$ such that

$$1 \le |\varepsilon^n \alpha| < \varepsilon.$$

If we set $\beta = \varepsilon^n\alpha$ and write $\beta = a + b\sqrt{m}$ (again a and b are allowed to be half-integers), then

$$|\beta'| = \frac{|\beta\beta'|}{|\beta|} = \frac{c}{|\beta|},$$

and we obtain the bounds

$$\frac{c}{\varepsilon} < |\beta'| \le c.$$

The triangle inequality now yields

$$\begin{aligned} |2a| &= |\beta + \beta'| \le |\beta| + |\beta'| < \varepsilon + c, \\ |2b|\sqrt{m} &= |\beta - \beta'| \le |\beta| + |\beta'| < \varepsilon + c. \end{aligned} \tag{7.6}$$

This immediately yields bounds for a and b, and now the problem can be solved in finitely many steps by simply checking the possible values of a and b one by one. Before we do this in our example, we will improve the bounds on a and b.

To this end, we set $\beta = \varepsilon^n\alpha$ and choose the exponent $n \in \mathbb{Z}$ in such a way that

$$\frac{\sqrt{c}}{\sqrt{\varepsilon}} \le |\beta| < \sqrt{c\varepsilon}\,.$$

As above, this implies the bounds

$$|\beta| < \sqrt{c\varepsilon} \quad \text{and} \quad |\beta'| \le \sqrt{c\varepsilon}\,,$$

and now we obtain $|2a| < 2\sqrt{c\varepsilon}$, which is a lot better than $|2a| < \varepsilon + c$.

As a matter of fact these bounds may be improved again by using the following lemma:

Lemma 7.7 *If $x, y \in \mathbb{R}$ satisfy the inequalities $0 < x \le r$, $0 < y \le r$, and $0 < xy \le s$, then $x + y \le r + \frac{s}{r}$.*

This claim follows from the observation $0 < (r-x)(r-y) = r^2 - r(x+y) + xy \le r^2 + s - r(x+y)$.

In our case, we have $r = \sqrt{c\varepsilon}$ and $s = c$; thus $|\beta + \beta'| \le \sqrt{c}\,\big(\sqrt{\varepsilon} + \frac{1}{\sqrt{\varepsilon}}\big)$. Since $\frac{1}{\sqrt{\varepsilon}} < 1$, this bound improves the previous one by a factor of about 2. We have proved the following:

Theorem 7.8 *Let k be a quadratic number field with a unit $\varepsilon > 1$; then for each $\alpha \in \mathcal{O}_k$ with norm $|N\alpha| = c$, there exists an associate $\beta = a + b\sqrt{m}$ (with integers or half-integers a, b) such that*

$$|a| \le \frac{1}{2}\sqrt{c}\Big(\sqrt{\varepsilon} + \frac{1}{\sqrt{\varepsilon}}\Big) \quad \textit{and} \quad |b| \le \frac{1}{2\sqrt{m}}\sqrt{c}\Big(\sqrt{\varepsilon} + \frac{1}{\sqrt{\varepsilon}}\Big). \tag{7.7}$$

If there is an element $\alpha \in \mathbb{Z}[\sqrt{79}\,]$ with norm ± 3, then (set $m = 79$, $\varepsilon = 80 + 9\sqrt{79}$, and $c = 3$) there is an element $a + b\sqrt{79}$ with norm ± 3 such that $|b| < 1.25$. Thus it is sufficient to consider $b = 1$, but the equation $a^2 - 79 \cdot 1^2 = \pm 3$ is not solvable in integers since 79 ± 3 is not a square. Thus $\mathbb{Z}[\sqrt{79}\,]$ does not contain an element with norm ± 3, and hence 3 is irreducible, but not prime since $3 \mid (2 - \sqrt{79}\,)(2 + \sqrt{79})$.

Remark Theorem 7.8 goes back to Pafnuty Chebyshev [18]; the corresponding result in general number fields but with weaker bounds had been obtained before by Dirichlet [30]. Chebyshev is best known for his contributions to the proof of the prime number theorem. This theorem states that the number $\pi(x)$ of all prime numbers $\le x$ is asymptotically equal to $\pi(x) \sim \frac{x}{\log x}$ in the sense that the quotient of these functions has limit 1 as $x \to \infty$; here $\log x$ denotes the natural logarithm. Chebyshev proved that if the limit of $\frac{\pi(x)}{x/\log x}$ for $x \to \infty$ exists, then it must be equal to 1. The existence of this limit and thus the prime number theorem was established independently in 1896 by Jacques Hadamard and Charles-Jean de la Vallée-Poussin.

7.2.1 Davenport's Lemma

Using Theorem 7.8, it is easy to prove a result going back to Harold Davenport:

Proposition 7.9 *Let m, n, and t be natural numbers with $m = t^2 + 1$; if the Diophantine equation $x^2 - my^2 = \pm n$ has integral solutions with $n < 2t$, then $x + y\sqrt{m}$ is associated with a rational integer a and $n = a^2$ is a perfect square.*

This result tells us that the only norms less than $2t$ in absolute value are the obvious ones, namely elements associated with rational integers a, which have norms $\pm a^2$. The norms of all other elements have absolute value $\ge 2t$.

For a proof, set $\xi = x + y\sqrt{m}$; we will show that if $|N\xi| = n$ is not a square, then $n \ge 2t$. Assume therefore that $n < 2t$; since $\varepsilon = t + \sqrt{m} > 1$ is a unit in $\mathbb{Z}[\sqrt{m}\,]$, we can find a power η of ε for which $\xi\eta = a + b\sqrt{m}$ has coefficients a and b that satisfy the bounds from Theorem 7.8. Because of $2t < \varepsilon < 2\sqrt{m}$, we find

$$|b| \le \frac{\sqrt{n}}{2\sqrt{m}}\left(\sqrt{\varepsilon} + \frac{1}{\sqrt{\varepsilon}}\right) < 1 + \frac{1}{t}.$$

Since the claim is trivial for $t = 1$, we may assume that $t \ge 2$, and then the last inequality gives $|b| \le 1$. If $b = 0$, then $(x + y\sqrt{m}\,)\eta = a$ is associated with a rational integer, and $|N\xi| = a^2$ is a square. If $b = \pm 1$, then $\alpha = \xi\eta = a \pm \sqrt{m}$. Now $|N\xi| = |N\alpha| = |a^2 - m|$ is minimal for values of a close to $\sqrt{m}$, and we find

$$n = |a^2 - m| = \begin{cases} 2t & \text{if } a = t \pm 1; \\ 1 & \text{if } a = t. \end{cases}$$

Thus either $n = 1$ (which we have excluded) or $n \ge 2t$. This proves our claims.

Proposition 7.9 was used by Ankeny, Chowla, and Hasse [2] for constructing quadratic number fields with nontrivial class groups.

Proposition 7.10 *The quadratic number field $k = \mathbb{Q}(\sqrt{m})$ with $m = t^2 + 1$ and $t = 2lq$, where q is prime and $l > 1$, has class number > 1.*

Since $m \equiv 1 \bmod q$, the prime q splits in k, and we have $(q) = \mathfrak{q}\mathfrak{q}'$. If $\mathfrak{q}$ is principal, then the equation $x^2 - my^2 = \pm 4q$ has integral solutions. But since $4q < 2t = 4lq$ is not a square, this contradicts Proposition 7.9.

Examples In the following examples, $m = t^2 + 1$ is prime. The ambiguous class number formula (see Chap. 9) will explain why the class number h is odd in this case.

q	l	t^2+1	h
3	4	577	7
	6	1297	11
	9	2917	3
	11	4357	5
	14	7057	21

q	l	t^2+1	h
5	2	401	5
	4	1601	7
	9	8101	13
	11	12101	5
	12	14401	43

The following result[8] shows that even a simple result such as Proposition 7.9 allows us to deduce astonishingly simple lower bounds for class numbers of fields of Richaud–Degert type.

[8]This theorem is due to Halter-Koch [48] and the proof presented here to Mollin [95].

Theorem 7.11 *Let t be an odd integer with prime factorization $t = p_1^{e_1} \cdots p_s^{e_s}$ and set $m = t^2 + 1$, and assume that $m = t^2 + 1$ is squarefree. Then the class number h of $\mathbb{Z}[\sqrt{m}\,]$ satisfies $h \ge S = 2\tau(n) - 2$, where*

$$\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_s + 1)$$

denotes the sum of all divisors of n.

If $t = q^e$ is a prime power, then the class number is divisible by S.

Proof For each prime $p_1 \mid m$, we have $(m/p_j) = +1$, and hence p_j splits in $\mathbb{Z}[\sqrt{m}\,]$ as $(p_j) = \mathfrak{p}_j\mathfrak{p}_j'$, where $\mathfrak{p}_j = (p_j, 1 + \sqrt{m})$. Let $\mathfrak{p}_0 = (2, \sqrt{m})$ denote the prime ideal above 2 and set $e_1 = 1$. We now consider the ideals $\mathfrak{a} = \mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_s^{a_s}$ with $0 \le a_j \le e_j$; clearly there are $(e_0 + 1)(e_1 + 1) \cdots (e_s + 1)$ such ideals; since $(e_0 + 1)(e_1 + 1) \cdots (e_s + 1) = \tau(n)$ is the number of divisors of n and since $e_0 + 1 = 2$, the number of ideals is $2\tau(n)$.

The class number bound will follow if we can show that only two among these ideals $\mathfrak{a}$ can be principal:

- the unit ideal $\mathfrak{a} = \mathfrak{p}_0^0\mathfrak{p}_1^0 \cdots \mathfrak{p}_s^0 = (1)$;
- the ideal $\mathfrak{a} = \mathfrak{p}_0\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$ with norm $2t$.

In fact, if $\mathfrak{a} = \mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_s^{a_s} = (x + y\sqrt{m})$ is principal, then $|x^2 - my^2| = N\mathfrak{a} \le N(\mathfrak{p}_0\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}) = 2t$. If $\mathfrak{a}$ is not one of the two ideals with norm 1 or $2t$, then $1 < |x^2 - my^2| < 2t$; but then $y = 0$ and $\mathfrak{a} = (x)$ for some rational integer x. Now $\mathfrak{a} = \mathfrak{a}^\sigma$ for the the nontrivial automorphism of $k/\mathbb{Q}$ implies $a_1 = \ldots = a_s = 0$, and hence $\mathfrak{a} = \mathfrak{p}_0$; but the prime ideal above 2 is not principal.

For proving the last claim, assume that $t = q^e$ for an odd prime number q. The relation $\mathfrak{p}_0\mathfrak{q}^e = (t + 1 + \sqrt{m})$, together with the fact that no ideal of the form $\mathfrak{z}\mathfrak{q}^j$ with $0 \le j < e$ is principal, implies that the ideal class of $\mathfrak{q}$ has order $2e$; thus we obtain the lower bound $2e \mid h$, where $2e = 2\tau(t) - 2$. □

The following table compares the lower bound S in Theorem 7.11 with the class number h for a few small values of m:

t	m	S	h
3	10	2	2
5	26	2	2
9	82	4	4
11	122	2	2
13	170	2	4
15	226	6	8
17	290	2	4
19	362	2	2

t	m	S	h
21	442	6	8
23	530	2	4
25	626	4	4
27	730	6	12
29	842	2	6
31	962	2	4
33	1090	6	12
35	1226	6	10

t	m	S	h
37	1370	2	4
39	1522	6	12
45	2026	10	14
47	2210	2	8
49	2402	4	8
51	2602	6	10
53	2810	2	8
55	3026	6	16

7.3 Computing the Solution of the Pell Equation

The computation of the units in a real quadratic number field $\mathbb{Q}(\sqrt{m})$, that is, solving the corresponding Pell equation $x^2 - my^2 = \pm 1$, is usually a quite difficult problem.

The basic idea behind the computation of the fundamental unit of a quadratic number field that we will present here is, as in the proof of the solvability of the Pell equation, the construction of sufficiently many elements of small norm. If we have many such elements, then we will look for elements α and β that not only have the same norm but also generate the same principal ideal. In this case, the quotient $\frac{\alpha}{\beta}$ will be a (possibly trivial) unit.

In order to convey the main idea, we consider the ring $\mathbb{Z}[\sqrt{11}\,]$. We look for solutions of the equation $x^2 - 11y^2 = n$ for small values of n. If we pick $y = 1$, the expression $x^2 - 11y^2$ will be small if $x \approx \sqrt{11}$, that is, for $x = 3$ and $x = 4$. Thus

$$\begin{aligned} 3^2 - 11 &= -2, \\ 4^2 - 11 &= +5. \end{aligned}$$

For $y = 2$, we choose $x \approx 2\sqrt{11}$, and we find

$$\begin{aligned} 6^2 - 11 \cdot 2^2 &= -8, \\ 7^2 - 11 \cdot 2^2 &= +5. \end{aligned}$$

Thus we already have found elements $4 \pm \sqrt{11}$ and $7 \pm 2\sqrt{11}$ with the same norm 5. Which of these generate the same ideal? One possibility of finding the right choice of signs is simply computing the quotients:

$$\frac{7 + 2\sqrt{11}}{4 + \sqrt{11}} = \frac{(7 + 2\sqrt{11})(4 - \sqrt{11})}{(4 + \sqrt{11})(4 - \sqrt{11})} = \frac{6 + \sqrt{11}}{5},$$

which is not an algebraic integer; thus $7 + 2\sqrt{11}$ and $4 + \sqrt{11}$ generate distinct prime ideals above 5. On the other hand,

$$\frac{7 + 2\sqrt{11}}{4 - \sqrt{11}} = \frac{(7 + 2\sqrt{11})(4 + \sqrt{11})}{(4 + \sqrt{11})(4 - \sqrt{11})} = \frac{50 + 15\sqrt{11}}{5} = 10 + 3\sqrt{11},$$

and we have found the nontrivial unit $\varepsilon = 10 + 3\sqrt{11}$.

Here is a more elegant way of verifying that $7 + 2\sqrt{11}$ and $4 - \sqrt{11}$ generate the same ideal: We know that these elements have norm 5, and hence they generate prime ideals above 5. There are only two such ideals, namely $\mathfrak{p}_1 = (5, 1 + \sqrt{11})$

and $\mathfrak{5}_2 = (5, 1 - \sqrt{11})$. Thus $\sqrt{11} \equiv -1 \bmod \mathfrak{5}_1$ and $\sqrt{11} \equiv +1 \bmod \mathfrak{5}_2$, hence

$$7 + 2\sqrt{11} \equiv 0 \bmod \mathfrak{5}_1, \qquad 7 + 2\sqrt{11} \equiv 4 \bmod \mathfrak{5}_2,$$
$$4 + \sqrt{11} \equiv 3 \bmod \mathfrak{5}_1, \qquad 4 + \sqrt{11} \equiv 0 \bmod \mathfrak{5}_2,$$

and this shows that $(7 + 2\sqrt{11}\,) = (4 - \sqrt{11}) = \mathfrak{5}_1$.

Another possibility of finding a nontrivial unit is based on the observation that $(2) = \mathfrak{2}^2$ is ramified in K. Since $3+\sqrt{11}$ has norm -2, we must have $\mathfrak{2} = (3+\sqrt{11})$, and then $(2) = \mathfrak{2}^2 = (3+\sqrt{11}\,)^2 = (20+6\sqrt{11})$ shows that $\frac{20+6\sqrt{11}}{2} = 10+3\sqrt{11}$ is a unit.

Now let us see how this method works for larger values of m, say for $m = 3431$. Again we begin by collecting elements with small norms:

α	$\mathrm{N}\alpha$	α	$\mathrm{N}\alpha$
$55 + \sqrt{m}$	$-2 \cdot 7 \cdot 29$	$60 + \sqrt{m}$	13^2
$56 + \sqrt{m}$	$-5 \cdot 59$	$61 + \sqrt{m}$	$2 \cdot 5 \cdot 29$
$57 + \sqrt{m}$	$-2 \cdot 7 \cdot 13$	$62 + \sqrt{m}$	$7 \cdot 59$
$58 + \sqrt{m}$	-67	$63 + \sqrt{m}$	$2 \cdot 269$
$59 + \sqrt{m}$	$2 \cdot 5^2$	$64 + \sqrt{m}$	$5 \cdot 7 \cdot 19$

We remark in passing that $60^2 - m = 13^2$ is a square; this implies that $m = 60^2 - 13^2 = (60 - 13)(60 + 13) = 47 \cdot 73$. Fermat's method of factorization is based on this idea.

The fact that 3 does not occur among these prime factors is explained by the observation that there is not even an ideal with norm 3 in $\mathbb{Q}(\sqrt{m})$ since $(\frac{m}{3}) = -1$. For the same reason, the primes 11 and 17 do not show up as factors. Instead of waiting until elements with the same norm occur, we will use an idea that was already used by Fermat and his contemporaries in their search for numbers whose sums of divisors are squares or cubes. We factor the elements with small norm into primes. It is easy to write down a list of prime ideals with small norms; in our case, these are $\mathfrak{2} = (2, 1+\sqrt{m})$, $\mathfrak{5}_1 = (5, 1+\sqrt{m})$, $\mathfrak{5}_2 = (5, 1-\sqrt{m})$, $\mathfrak{7} = (7, 1+\sqrt{m})$, and $\mathfrak{7}_2 = (7, 1 - \sqrt{m})$. Now we factor all elements with small norm that are only divisible by 2, 5, and 7:

α	$\mathfrak{2}$	$\mathfrak{5}_1$	$\mathfrak{5}_2$	$\mathfrak{7}_1$	$\mathfrak{7}_2$
$1 + \sqrt{m}$	1	1	0	3	0
$1 - \sqrt{m}$	1	0	1	0	3
$41 + \sqrt{m}$	1	3	0	0	1
$41 - \sqrt{m}$	1	0	3	1	0
$59 + \sqrt{m}$	1	0	2	0	0
$59 - \sqrt{m}$	1	2	0	0	0

The first line in this table records the prime ideal decomposition

$$(1+\sqrt{m}\,) = \mathfrak{2}^1 \cdot \mathfrak{5}_1^1 \cdot \mathfrak{7}_1^3.$$

If we look carefully at this table, then we can see that

$$(1+\sqrt{m}\,)(41+\sqrt{m}\,)^3 = \mathfrak{2}^4\mathfrak{5}_1^{10}\mathfrak{7}_1^3\mathfrak{7}_2^3.$$

Since $\mathfrak{2}^2 = (2)$ und $\mathfrak{7}_1\mathfrak{7}_2 = (7)$, the element

$$\frac{(1+\sqrt{m}\,)(41+\sqrt{m}\,)^3}{2^2\cdot 7^3} = 21549 + 364\sqrt{m}$$

has the prime ideal factorization $\mathfrak{5}_1^{10}$. But then $(59-\sqrt{m}\,)^5 = \mathfrak{2}^5\mathfrak{5}^{10}$ shows that

$$\alpha = \frac{(59-\sqrt{m}\,)^5}{21549+364\sqrt{m}} = 49316884 - 841948\sqrt{m}$$

is an algebraic integer with the factorization $\mathfrak{2}^5$. Since the ideal $\mathfrak{2}$ is ramified, the element $\varepsilon = 2^5/\alpha^2$ must be a unit, and we have

$$\varepsilon = 152009690466840 + 2595140740627\sqrt{m}.$$

Observe that this method gives us not only a nontrivial unit but also something called a "compact representation" of this unit:

$$\varepsilon = \frac{2(1+\sqrt{m}\,)^2(41+\sqrt{m}\,)^6}{7^6(59-\sqrt{m}\,)^{10}}.$$

Also observe that the prime ideal factorization in quadratic number fields is an essential component of this method of solving the completely elementary equation $x^2 - my^2 = 1$.

After having found a nontrivial unit ε, the question remains how we can check that this unit is fundamental. So far we only know that $\varepsilon = \pm\eta^n$ for some integer n, where η is the fundamental unit. Since $\varepsilon > 1$, the positive sign must hold, and we have $n \geq 1$. Clearly, ε is not a square as we can read off from its compact representation. Thus we only have to check whether ε is an n-th power for the values $n = 3, 5, 7, \ldots$, and the first problem is bounding this exponent.

The following bound is simple and best possible:

Lemma 7.12 *Let $\eta > 1$ be the fundamental unit of a real quadratic number field with discriminant d. Then*

$$\log \eta > \begin{cases} \log \sqrt{d}, & \text{if } N\varepsilon = +1, \\ \log(\sqrt{d} - 1), & \text{if } N\varepsilon = -1. \end{cases}$$

Proof Let $K = \mathbb{Q}(\sqrt{m})$ with $m \equiv 2, 3 \bmod 4$ and $N\varepsilon = +1$. Then the smallest possible value of ε is $a + \sqrt{m}$ with $a \approx \sqrt{m}$. If $N\varepsilon = +1$, then $a > \sqrt{m}$, and this implies $\varepsilon > 2\sqrt{m} = \sqrt{d}$.

Observe that the family of quadratic number rings $\mathbb{Z}[\sqrt{m}\,]$ with $m = t^2 - 1$ has units $\varepsilon_m = t + \sqrt{m}$ for which $\varepsilon_m = \sqrt{m+1} + \sqrt{m} > 2\sqrt{m} = \sqrt{d}$ is best possible since $\varepsilon_m - \sqrt{d} = \sqrt{m+1} - \sqrt{m} = \frac{1}{\sqrt{m+1}+\sqrt{m}} < \frac{1}{2\sqrt{m}}$.

The other cases are discussed similarly. □

In our case we have $m = 3431 = 47 \cdot 73$; since m is divisible by the prime number $47 \equiv 3 \bmod 4$, we must have $N\varepsilon = +1$ and thus $\log \varepsilon \geq 4.763\ldots$, and hence $n = \log \varepsilon / \log \eta \leq 33.3/4.763 = 6.991\ldots$. Therefore $n \leq 6$, and since we already know that ε is not a square, we must have $m \leq 5$.

Thus it remains to show that ε is not a cube or a fifth power. Perhaps the easiest way of doing this is finding a prime ideal $\mathfrak{p}$ modulo which ε is not a cube or a fifth power.

- Since $\varepsilon \equiv 0 - 3\sqrt{m} \equiv 3 \bmod \mathfrak{5}_1$, the unit ε is not a square; in fact, $(\frac{3}{5}) = -1$ implies that 3 is not a square modulo $\mathfrak{5}_1$.
- For showing that ε is not a cube, we need to find a prime ideal $\mathfrak{p}$ with norm $N\mathfrak{p} \equiv 1 \bmod 3$. Now $\varepsilon \equiv 3 + \sqrt{m} \equiv 2 \bmod \mathfrak{7}_1$, and since 2 is not a cubic residue modulo 7 and $\mathcal{O}_K/\mathfrak{7}_1 \simeq \mathbb{Z}/7\mathbb{Z}$, the unit ε is not a cubic residue modulo $\mathfrak{7}_1$. In particular, ε is not a cube.
- Let $\mathfrak{q} = (61, 25+\sqrt{m})$; then $\mathfrak{p}$ has norm $N\mathfrak{p} = 61$, and we have $\varepsilon \equiv 40-3\sqrt{m} \equiv 54 \bmod \mathfrak{q}$. Since 54 is not a fifth power modulo 61, the unit ε cannot be a fifth power.

Instead of working with residue classes, we can compute with real numbers. To this end, we determine the real approximations

$$\begin{aligned} \varepsilon &\approx 304\,019\,380\,933\,679.999\,999\,999\,999\,996\,711 \\ 1/\varepsilon &\approx 0.000\,000\,000\,000\,003\,289. \end{aligned}$$

Now $\varepsilon + 1/\varepsilon$ is an integer; in fact, if we write $\varepsilon = a + b\sqrt{m}$, then $1/\varepsilon = a - b\sqrt{m} = \varepsilon'$ and thus $\varepsilon + \frac{1}{\varepsilon} = 2a$. If $\varepsilon = \eta^5$ were a fifth power, then $\eta + 1/\eta = \eta + \eta'$ would be an integer. Since $\eta \approx 788.098052\ldots$ and $1/\eta \approx 0.001268877\ldots$, we have $\eta + 1/\eta \approx 788.0993\ldots$. Thus ε is not a fifth power, and the cases $n = 2$ and $n = 3$ can be treated similarly.

7.4 Parametrized Units

It is rather easy to construct families of quadratic number fields in which the fundamental unit can be written down explicitly. The simplest way of finding such a family is looking at the unit equation $t^2 - mu^2 = \pm 1$ and setting $u = 1$; then $m = t^2 \mp 1$ (with $t \geq 2$), and in fact $\varepsilon_t = t + \sqrt{t^2 \mp 1}$ is a unit in $\mathbb{Z}[\sqrt{m}\,]$.

Proposition 7.13 *If $m = t^2 - 1$ is squarefree for $t \geq 2$, then $\varepsilon_m = t + \sqrt{m}$ is the fundamental unit of $\mathbb{Z}[\sqrt{m}\,]$.*

This result also holds if m is not squarefree, but then $\mathbb{Z}[\sqrt{m}\,]$ is not the ring of integers of $\mathbb{Q}(\sqrt{m})$.

Since we have already shown that ε_m is a unit, it only remains to show that ε_m is fundamental. But since $\varepsilon_m > 1$, this unit can only be not fundamental if $\varepsilon_m = (r + s\sqrt{m}\,)^k$ for some exponent $k \geq 2$, and in that case the coefficient of $\sqrt{m}$ in ε would have to be strictly greater than 1; for example, we have $(r + s\sqrt{m}\,)^2 = r^2 + ms^2 + 2rs\sqrt{m}$.

The case $m = t^2 + 1$ is slightly more complicated.

Proposition 7.14 *Assume that $m = t^2 + 1$ is squarefree for $t \geq 1$. If t is odd, then $\varepsilon_m = t + \sqrt{m}$ is the fundamental unit of $\mathbb{Z}[\sqrt{m}\,]$. If t is even, then ε_m is the fundamental unit of $\mathbb{Z}[\frac{1+\sqrt{m}}{2}\,]$ except for $t = 2$, when $\varepsilon_5 = 2 + \sqrt{5} = (\frac{1+\sqrt{5}}{2})^3$.*

The proof that ε_m is fundamental if t is odd (and thus if $m \equiv 2 \bmod 4$) is exactly as above. Assume therefore that t is even and $m = t^2 + 1 \equiv 1 \bmod 4$. If ε_m is not fundamental, then $\varepsilon_m = \big(\frac{r+s\sqrt{m}}{2}\big)^k$ for some exponent $k \geq 2$. If r and s are even, the proof above works. Assume therefore that r and s are odd. Then the smallest power of $\frac{r+s\sqrt{m}}{2}$ that lies in $\mathbb{Z}[\sqrt{m}\,]$ is 3, and in fact k must be a multiple of 3. The case $k \geq 6$ cannot occur (the same proof as above), and if $k = 3$, then

$$\Big(\frac{r + s\sqrt{m}}{2}\Big)^3 = \frac{r^3 + 3rms^2 + (3r^2 s + ms^3)\sqrt{m}}{8}$$

shows that we must have $3r^2 s + ms^3 = 8$. Since s is odd, this implies $s = 1$, and then $3r^2 + m = 8$ yields $m = 5$ and $r = 1$ as the only integral solution.

We obtain a slightly less trivial family by writing the Pell equation $t^2 - mu^2 = 1$ in the form $mu^2 = t^2 - 1 = (t-1)(t+1)$. Setting $t - 1 = u^2$ and $t + 1 = m$, we find $m = u^2 + 2$ and $t = u^2 + 1$. In this way we obtain the following proposition.

Proposition 7.15 *Assume that $m = t^2 + 2$ is squarefree. Then $\varepsilon_m = t^2 + 1 + t\sqrt{m}$ is the fundamental unit of $\mathbb{Z}[\sqrt{m}\,]$.*

Here $\varepsilon_m = (r + s\sqrt{m}\,)^k$ is impossible for $k \geq 2$ because already the coefficient of $\sqrt{m}$ in $(r + s\sqrt{m}\,)^2 = r^2 + ms^2 + 2rs\sqrt{m}$ is too large: We must have $r^2 + ms^2 > t^2 + 1$ since otherwise $rs = 0$, which is impossible.

In the examples above, the units are rather small. For finding fields with larger fundamental units,[9] we construct elements α and β with $N\alpha = \pm a^n$ and $N\beta = a$; using some additional conditions, we can make sure that the quotient $\varepsilon = \alpha/\beta^n$ is integral and therefore a unit.

For finding fields $K = \mathbb{Q}(\sqrt{m})$ containing elements with norm $\pm a^n$, we can simply write $m = r^2 + a^n$; then $\alpha = r + \sqrt{m}$ has norm $N\alpha = -a^n$. For finding elements with norm $\pm a$ in $\mathbb{Z}[\sqrt{m}\,]$, we observe that if $Q(x, y) = Ax^2 + Bxy + Cy^2$ (below, we will often abbreviate this form by $Q = (A, B, C)$) is a binary quadratic form with discriminant $\Delta = B^2 - 4AC = 4m$, and if $Q(s, t) = 1$, then

$$As^2 + Bst + Ct^2 = 1 \quad \text{implies} \quad 4A = (2As + Bt)^2 - \Delta t^2,$$

and hence $As + \frac{1}{2}Bt + t\sqrt{m}$ has norm A. Clearly, the quadratic form $Q = (a, 2r, a^{n-1})$ has discriminant $4m$, so all we need is a solution of the equation $1 = Q(s, t) = as^2 + 2rst + a^{n-1}t^2$ in integers. Before we construct such solutions, we prove that we do in fact obtain units in this way:

Proposition 7.16 *Assume that $m = r^2 + a^n \equiv 2, 3 \bmod 4$ for coprime integers $a > 1$ and $n \geq 2$. Assume moreover that $Q(s, t) = 1$, where s and t are nonzero integers and where $Q = (-a, 2r, a^{n-1})$. Set $\alpha = r + \sqrt{m}$ and $\gamma = as - rt - t\sqrt{m}$; then $N\alpha = -a^n$, $N\gamma = -a$, and the element*

$$\varepsilon = \frac{\gamma^n}{\alpha}$$

is a nontrivial unit in $\mathbb{Z}[\sqrt{m}\,]$.

There is, of course, a similar result for $m \equiv 1 \bmod 4$. If r is odd, then one has to consider elements of the form $\alpha = \frac{r+\sqrt{m}}{2}$.

Proof Set $\mathfrak{a} = (a, r + \sqrt{m})$. Clearly,

$$\gamma = as - rt - t\sqrt{m} = as - t(r + \sqrt{m}\,) \in \mathfrak{a},$$

hence $\mathfrak{a} \mid (\gamma)$. Moreover,

$$\mathfrak{a}^n = (a^n, a^{n-1}\alpha, \ldots, a\alpha^{n-1}, \alpha^n) = (\alpha)(r - \sqrt{m}, a^{n-1}, \ldots, \alpha^{n-1}) = (\alpha)$$

since $(\alpha', \alpha^{n-1}) \supseteq (\alpha', \alpha) = (1)$. In fact, if $\mathfrak{p}$ is a prime ideal dividing (α', α), then either $\mathfrak{p}$ is ramified, or $m \equiv 1 \bmod 4$ and $\mathfrak{p} \mid (2)$. Since we have excluded the last

[9]The class number formula roughly implies that fields with large fundamental units tend to have small class numbers; constructing families of fields with large fundamental units is therefore important with respect to Gauss's conjecture that there are infinitely many real quadratic number fields with class number 1.

case, $\mathfrak{p}$ is ramified. Since $\mathfrak{p} \mid N\alpha = a^n$, this implies $\mathfrak{p} \mid (a)$. But then $\mathfrak{p} \mid (m)$ implies $\mathfrak{p} \mid (r)$ contradicting the assumption that r and a are coprime.

Now $\gamma \in \mathfrak{a}$ and $|N\gamma| = N\mathfrak{a}$ implies $\mathfrak{a} = (\gamma)$. This shows that $(\alpha) = (\gamma)^n$, and hence ε is a unit as claimed.

It remains to show that the unit ε is nontrivial, i.e., that $\varepsilon \neq \pm 1$. But $\varepsilon = \pm 1$ is equivalent to $\pm\gamma^n = \alpha = r + \sqrt{m}$, and this is impossible for $n \geq 2$ as soon as $a > 1$. Clearly, $\pm(t + u\sqrt{m}\,)^2 = r + \sqrt{m}$ is impossible; similarly, $\pm(\frac{t+u\sqrt{m}}{2}\,)^3 = r + \sqrt{m}$ implies $t = u = 1$ and $m = 5$, which in turn is only possible if $r = 2$ and $a = 1$. $\square$

Now let $m = r^2 + a^3$ and $Q = (-a, 2r, a^2)$. Setting $Q(x, 1) = 1$ and solving for r, we obtain

$$r = \frac{1 - a^2 + ax^2}{2x}.$$

This value of r is an integer, e.g., when $x = a - 1$ is even. Then $r = \frac{a^2-2a-1}{2}$, and we have $Q(a - 1, 1) = 1$ for the quadratic form $Q = (-a, a^2 - 2a - 1, a^2)$, and hence

$$\gamma = a(a-1) - \frac{a^2 - 2a - 1}{2} - \sqrt{m} = \frac{a^2 + 1 - 2\sqrt{m}}{2}$$

has norm $-a$.

An explicit calculation yields the unit

$$\varepsilon = \frac{a^5 - a^4 + 3a^3 + a^2 + 2}{2} + (a^3 - a^2 + 2a)\sqrt{m}.$$

The first few examples are given in the following table:

a	r	m	γ	ε
5	7	174	$13 - \sqrt{m}$	$1451 + 110\sqrt{174}$
9	31	1690	$41 - \sqrt{m}$	$27379 + 666\sqrt{1690}$
13	71	7238	$85 - \sqrt{m}$	$174747 + 2054\sqrt{7238}$
17	127	21042	$145 - \sqrt{m}$	$675683 + 4658\sqrt{21042}$

There are many other choices of r, each of which yields a similar family of units.

Now let $\Delta = (2a + 1)^2 + 4 \cdot 2^n$ for some integer a. Then

$$(2a + 1)^2 - \Delta = -4 \cdot 2^n, \quad \text{or} \quad a^2 + a + \frac{1 - \Delta}{4} = -2^n.$$

This shows that $(a, 1)$ is an integral point on the conic $x^2 + xy + \frac{1-\Delta}{4} = -2^n$; equivalently, the element $\alpha = \frac{2a+1+\sqrt{\Delta}}{2}$ has norm $N\alpha = -2^n$.

Next we look at conics of the form $Q(x, y) = 1$ with $Q = (2, b, c)$ and

$$\operatorname{disc} Q = b^2 - 8c = (2a + 1)^2 + 4 \cdot 2^n$$

that have an integral point. The simplest possible form is $Q = (2, -2a-1, -2^{n-1})$, and the simplest possible integral points are those with $y = \pm 1$. A necessary condition for the existence of an integral solution of $Q(x, \pm 1) = 1$, that is, of

$$2x^2 \pm (2a + 1)x - 2^{n-1} = 1,$$

is that the discriminant of the quadratic equation in x is a square:

$$(2a + 1)^2 + 8 \cdot (2^{n-1} - 1) = 4a^2 + 4a + 4 \cdot 2^n + 9 = \Box.$$

Setting this expression equal to $(2a + 3)^2$ quickly yields $a = 2^{n-1}$. In this case, the quadratic equation

$$2x^2 - (2^n + 1)x - (2^{n-1} - 1) = 0$$

has the solutions

$$x_{1,2} = \frac{2^n + 1 \pm (2^n + 3)}{4}, \quad i.e., \quad x_1 = -\frac{1}{2}, \quad x_2 = 2^{n-1} + 1.$$

Thus we now have $\Delta = (2^n + 3)^2 - 8 = (2^n + 1)^2 + 4 \cdot 2^n$, and the conic $Q(x, y) = 1$ with $Q = (2, -2^n - 1, -2^{n-1})$ has the integral point $(2^{n-1} + 1, 1)$. Since

$$8Q(x, y) = (4x - (2^n + 1)y)^2 - \Delta y^2,$$

this provides us with the element

$$\gamma = \frac{2^n + 3 + \sqrt{\Delta}}{2}$$

with norm $N\gamma = -2$. Since $\alpha = \frac{1}{2}[(2^n + 1) - \sqrt{\Delta}\,]$ has norm -2^n, the solution of the Pell equation is given by

$$\varepsilon = -\frac{\gamma^n}{\alpha},$$

which is a unit with norm -1. This family is due to Michael Nyberg [100] and (independently) to Daniel Shanks [115].

n	Δ	ε
1	17	$4+\sqrt{\Delta}$
2	41	$32+5\sqrt{\Delta}$
3	113	$776+73\sqrt{\Delta}$
4	353	$71264+3793\sqrt{\Delta}$
5	1217	$27628256+791969\sqrt{\Delta}$
6	4481	$46496952832+694603585\sqrt{\Delta}$

In this case, the discriminant Δ is asymptotically equal to $\Delta \sim 2^{2n}$, and we have $\gamma \sim 2^n$. Moreover, $\frac{1}{\alpha} = \frac{\alpha'}{N\alpha} \sim -\frac{2^n}{2^n} = -1$ is bounded, and hence $\varepsilon \sim \gamma^n \sim (2^n)^n \sim \Delta^{n/2}$. Thus $\log \varepsilon / \log \Delta$ is not bounded.

7.5 Factorization Algorithms

The same idea that we have used for computing the fundamental unit of a real quadratic number field can be applied directly for factoring large integers. As a modest example, we choose $N = 4469$ and begin by factoring the integers $a^2 - N$ for $a \approx \sqrt{4469} \approx 67$. We keep only those factorizations that involve sufficiently small prime numbers:

a	-1	2	5
62	1	0	4
63	1	2	3
67	0	2	1

The first line in this table encodes the factorization $62^2 - N = -5^4$.

Already the Indian mathematician Narayana Pandit (ca. 1340–1400) and later Pierre Fermat had used a similar method for factoring integers that do not have small factors. They checked whether any of the numbers $a^2 - N$ for $N = 1, 2, 3, \ldots$ is a square number: If $a^2 - N = b^2$, then we obtain the factorization $N = a^2 - b^2 = (a-b)(a+b)$.

The essential idea behind the modern factorization methods based on this idea (see, e.g., [130]) is the observation that we do not need a solution of the equation $a^2 - N = b^2$ but only a solution of the congruence $a^2 \equiv b^2 \bmod N$. Once we have found such a pair of integers a and b, the numbers $\gcd(a+b, N)$ and $\gcd(a-b, N)$ are (possibly trivial) factors of N. Now observe that

$$(63^2 - N)(67^2 - N) = -2^4 \cdot 5^4$$

implies the congruence

$$63^2 \cdot 67^2 \equiv -2^4 \cdot 5^4 \bmod N.$$

Moreover we have $62^2 \equiv -5^4 \bmod N$, and hence $63^2 \cdot 67^2 \equiv 4^2 \cdot 62^2 \bmod N$, and we find only the trivial factor $\gcd(63 \cdot 67 - 4 \cdot 62, N) = 1$.

By enlarging our factor base, we obtain

a	-1	2	5	11	13
62	1	0	4	0	0
63	1	2	3	0	0
67	0	2	1	0	0
71	0	2	0	1	1
72	0	0	1	1	1
83	0	2	1	2	0

Now we see $67^2 \cdot 72^2 \equiv 71^2 \cdot 5^2 \bmod N$, but this solution gives us once again just the trivial factorization. We are more lucky with $67^2 \cdot 11^2 \equiv 83^2 \bmod N$ since now $\gcd(67 \cdot 11 - 83, N) = 109$, and in fact we have $N = 41 \cdot 109$.

Finding such relations is essentially linear algebra: We interpret the exponents in the factorizations as elements of an $\mathbb{F}_2$-vector space, and then finding squares boils down to finding linear dependent vectors. The factorization method based on this idea is called the quadratic sieve.

Factoring Integers with the Pell Equation The computation of the fundamental unit is, for many values of m, about as difficult as factoring m. Indeed it follows from $x^2 - my^2 = 1$ that $my^2 = x^2 - 1 = (x-1)(x+1)$, and $\gcd(m, x-1)$ is a (possibly trivial) factor of m. For $m = 91$, for example, the fundamental unit is $\varepsilon = 1574 + 165\sqrt{91}$, and we have $\gcd(91, 1573) = 13$. The Bohemian mathematician Franz von Schafgotsch [128] factored $a = 909\,191$ by solving the Pell equation for $m = 5a = 4\,545\,955$; he obtained

$$790482741705651738629349656268492900551186678587245833797608 74^2 =$$

$$m \cdot 370748861793367258280487230881607848045136342896607634986 55^2 + 1,$$

and used the Euclidean algorithm to find the greatest common divisor of

$$790482741705651738629349656268492900551186678587245833797608 74+1$$

and $m = 1315$, which gave him the factorization

$$909\,191 = 263 \cdot 3457.$$

7.6 Diophantine Equations

There is a large class of Diophantine equation whose solution depends crucially on the structure of the unit group of quadratic number fields. To give the readers an idea of a few elementary techniques in this area, we will prove a result due to J.H.E. Cohn (see, e.g., [21]).

Let $m \equiv 5 \bmod 8$ be a squarefree natural number, and assume that the fundamental unit $\varepsilon = \frac{a+b\sqrt{m}}{2}$ has norm -1 and satisfies $a \equiv b \equiv 1 \bmod 2$. We will consider the sequence of integers

$$V_n = \varepsilon^n + \varepsilon'^n,$$

where $\varepsilon' = \frac{a-b\sqrt{m}}{2} = -\frac{1}{\varepsilon}$. The first three elements of the sequence (V_n) are $V_0 = 2$, $V_1 = a$, and $V_2 = a^2 + 2$.

If $m = 5$ (and therefore $a = 1$), these are called *Lucas numbers* after Édouard Lucas (1842–1891):

n	0	1	2	3	4	5	6	7
V_n	2	1	3	4	7	11	18	29

One consequence of the theorem we are about to prove is that the only squares in this sequence are $V_1 = 1$ and $V_3 = 4$.

We will need the following observations:

Proposition 7.17 *For all $k, n \in \mathbb{Z}$, we have*

$$V_{n+2} = aV_{n+1} + V_n, \tag{7.8}$$

$$V_{2n} = V_n^2 - 2(-1)^n, \tag{7.9}$$

$$V_{n+2k} \equiv (-1)^{k+1} V_n \bmod V_k. \tag{7.10}$$

Equation (7.8) follows from

$$\begin{aligned}V_{n+2} &= \varepsilon^{n+2} + \varepsilon'^{n+2} = (\varepsilon + \varepsilon')(\varepsilon^{n+1} + \varepsilon'^{n+1}) - \varepsilon\varepsilon'^{n+1} - \varepsilon'\varepsilon^{n+1} \\ &= V_1 V_{n+1} - \varepsilon\varepsilon' V_n = V_1 V_{n+1} + V_n\end{aligned}$$

since $V_1 = a$ and $\varepsilon\varepsilon' = -1$. Next

$$V_{2n} = \varepsilon^{2n} + \varepsilon'^{2n} = (\varepsilon^n + \varepsilon'^n)^2 - 2(\varepsilon\varepsilon')^n = V_n^2 - 2(-1)^n.$$

Equation (7.9) immediately implies that the numbers V_{2n} cannot be squares.

Finally,

$$\begin{aligned}V_{n+2k} &= \varepsilon^{n+2k} + \varepsilon'^{n+2k} = (\varepsilon^k + \varepsilon'^k)(\varepsilon^{n+k} + \varepsilon'^{n+k}) - \varepsilon^k\varepsilon'^{n+k} - \varepsilon'^k\varepsilon^{n+k} \\ &= V_k V_{n+k} - (-1)^k V_n \equiv (-1)^{k+1} V_n \bmod V_k.\end{aligned}$$

Next we observe that V_n is even if and only if n is divisible by 3. This follows from the recursion

$$V_{n+2} = aV_{n+1} + V_n$$

by induction.

In the following, k will always denote an integer not divisible by 3. Thus

$$V_{2k} = V_k^2 - 2(-1)^k \equiv \begin{cases} 3 \bmod 8 & \text{if } k \text{ is odd,} \\ 7 \bmod 8 & \text{if } k \text{ is even.} \end{cases}$$

Theorem 7.18 *Let $m \equiv 5 \bmod 8$ be squarefree, and let $\varepsilon = \frac{a+b\sqrt{m}}{2}$ denote the fundamental unit of $\mathbb{Q}(\sqrt{m})$, where we assume that a and b are odd. The number $V_n = \varepsilon^n + \varepsilon'^n$ is a square only in the following cases:*

1. *$n = 1$ and a is a square;*
2. *$n = 3$ and $a(a^2 + 3)$ is a square.*

Using `sage`, it is possible to show that the elliptic curve $y^2 = a(a^2+3)$ has exactly four integral points, namely $(0, 0)$, $(1, 0)$, $(3, 6)$, and $(12, 42)$. A proof by hand leads to the Diophantine equation $x^4 - 3y^4 = -2$, which seems to be difficult to solve with the methods presented here.

For the proof of Theorem 7.18, we will distinguish several cases.

1. $a \equiv 5, 7 \bmod 8$ **and** $n \equiv 3 \bmod 4$ We write $n = 2 \cdot 3^r k - 1$ for an even integer k not divisible by 3. Then $V_k \equiv 3 \bmod 4$ and

$$V_n = V_{2\cdot 3^r k-1} \equiv -V_{-1} \equiv a \bmod V_k$$

by (7.10); hence,

$$\begin{aligned}
\Big(\frac{V_n}{V_k}\Big) &= \Big(\frac{a}{V_k}\Big) && \text{since } V_n \equiv a \bmod V_k, \\
&= \Big(\frac{-1}{a}\Big)\Big(\frac{V_k}{a}\Big) && \text{since } (\tfrac{a}{V_k}) = (\tfrac{-V_k}{a}) \\
&= \Big(\frac{-2}{a}\Big) && \text{since} V_k \equiv 2 \bmod a \text{ if } k \text{ is even.} \\
&= -1 && \text{since } a \equiv 5, 7 \bmod 8.
\end{aligned}$$

But this implies our claim that V_n is not a square in this case.

2. $a \equiv 5, 7 \bmod 8$ **and** $n \equiv 1 \bmod 4$ Here we write $n = -3 + 2 \cdot 3^r k$ for some even integer n not divisible by 3 and find $V_n \equiv -V_{-3} = V_3 \bmod V_k$. Now $V_3 = a(a^2 + 3) = a \cdot 4b$ for some odd integer b; hence,

$$\begin{aligned}
\Big(\frac{V_3}{V_k}\Big) &= \Big(\frac{a}{V_k}\Big)\Big(\frac{b}{V_k}\Big) && \text{since } (\tfrac{4}{V_k}) = 1 \\
&= \Big(\frac{a}{V_k}\Big)\Big(\frac{-V_k}{b}\Big) && \text{since } V_k \equiv 3 \bmod 4 \\
&= \Big(\frac{a}{V_k}\Big) && \text{since } V_k \equiv V_2 = a^2 + 2 \equiv -1 \bmod b. \\
&= -1 && \text{since } (\tfrac{a}{V_k}) = (\tfrac{-V_k}{a}) = (\tfrac{-2}{a}) = -1 \text{ as above.}
\end{aligned}$$

3. $a \equiv 1, 3 \bmod 8$ **and** $n \equiv 1 \bmod 4$ We write $n = 2 \cdot 3^r k + 1$ for an even integer k not divisible by 3; since $V_n \equiv -V_1 \equiv -a \bmod V_k$ if $n > 1$, we have

$$\Big(\frac{V_n}{V_k}\Big) = \Big(\frac{-a}{V_k}\Big) = -\Big(\frac{a}{V_k}\Big) = -\Big(\frac{-2}{a}\Big) = -1.$$

4. $a \equiv 1, 3 \bmod 8$ **and** $n \equiv 3 \bmod 4$ If $n \neq 3$, we can write $n = 3 + 2 \cdot 3^r k$, where k is even and not divisible by 3. Then $V_n \equiv -V_3 \equiv -a \bmod V_k$, and again we find

$$\Big(\frac{V_n}{V_k}\Big) = \Big(\frac{-V_3}{V_k}\Big) = -\Big(\frac{V_3}{V_k}\Big) = -\Big(\frac{-2}{a}\Big) = -1.$$

If $n = 3$, then $V_3 = a^3 + 3a$ must be a square.

7.6.1 Summary

In this chapter we have shown

- that the Pell equation $x^2 - my^2 = 1$ has nontrivial solutions in integers for each nonsquare natural number m, that the unit group E_K of a real quadratic number field K is isomorphic to $E_K \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$, and
- how to find the solutions of the Pell equation for modest values of m by studying elements of K with small norms.

For learning more about the Pell equation, see [8, 66, 91], and [46], as well as the series of articles [78].

7.7 Exercises

7.1. Let k be a real quadratic number field; assume that $\eta = \alpha^2$ and $N\alpha < 0$ for elements $\eta, \alpha \in k^\times$. Show that, as real numbers, $\operatorname{Tr}\alpha = \sqrt{\eta} - \sqrt{\eta'}$.

7.2. Show that if $m = n^2$ is a square, then the equation $x^2 - my^2 = 1$ has only the trivial solutions $x = \pm 1$ in integers.

7.3. Show using Dirichlet's pigeonhole principle that for each real number x, there exist infinitely many pairs $(p, q) \in \mathbb{Z} \times \mathbb{Z}$ such that $|x - \frac{p}{q}| < \frac{1}{q^2}$.
Hint: Consider the remainders modulo 1 of the numbers $0, x, 2x, \ldots, nx$; these $n + 1$ remainders lie in the n intervals $[0, \frac{1}{n}), [\frac{1}{n}, \frac{2}{n}), \ldots, [\frac{n-1}{n}, 1)$.

7.4. Find elements with small nontrivial norm in the family of quadratic number fields $\mathbb{Q}(\sqrt{m})$ with $m = t^2 - 1$ and $m = t^2 \pm 4$.
Use this result for finding examples of real quadratic number fields with large class number.

7.5. Prove the following lemma (Hasse [58]): If $m > 0$ is not a square and $\varepsilon = \frac{t+u\sqrt{m}}{2}$ the fundamental unit of $\mathbb{Q}(\sqrt{m})$, and if n is the smallest positive nonsquare for which $x^2 - my^2 = \pm 4n$ is solvable in nonzero integers, then

$$n \geq \begin{cases} \frac{t}{u^2}, & \text{if } N\varepsilon = -1, \\ \frac{t-2}{u^2}, & \text{if } N\varepsilon = +1. \end{cases}$$

7.6. Show: If $m = 2p$ for primes $p \equiv 5 \bmod 8$, then $N\varepsilon_m = -1$ for the fundamental unit ε_m of $\mathbb{Q}(\sqrt{m})$.

7.7. Show: If $m = 2p$ for primes $p \equiv 3 \bmod 4$, then either $x^2 - my^2 = 2$ or $x^2 - my^2 = -2$ is solvable in nonzero integers. Also show that, in this case, $2\varepsilon_m$ is a square in $K = \mathbb{Q}(\sqrt{m})$, where ε_m denotes the fundamental unit in K.

7.8. Compute the fundamental units of $\mathbb{Q}(\sqrt{m})$ for $m = 3, 19, 43, 67, 131, 159, 199$.

7.9. Show: If $\varepsilon = \frac{t+u\sqrt{m}}{2}$ is the fundamental unit of $\mathbb{Q}(\sqrt{m})$ for $m \equiv 1 \bmod 8$, then t and u are even.

7.10. Let $m = n^2 - 1$ for some natural number $n \geq 2$. Show that $\varepsilon = n + \sqrt{m}$ is a unit in $\mathbb{Z}[\sqrt{m}\,]$ and that it is the fundamental unit of $\mathbb{Q}(\sqrt{m})$ if m is squarefree.

More generally, find units for $m = n^2 \pm 1$ and $m = n^2 \pm 4$.

7.11. Compute the class number and the fundamental unit of $K = \mathbb{Q}(\sqrt{478})$.

Hint: Consider the prime ideal above (2) and the prime ideals above 3 and 7. Determine the prime ideal factorizations of $(a + \sqrt{478})$ for $a = 10, 17, 22$, 24, and 25, and conclude that K has class number 1.

7.12. The solvability of the Pell equation $x^2 - my^2 = 1$ for positive nonsquares m may be formulated as follows: The part of the Euclidean plane defined by the hyperbolas $x^2 - my^2 = 1$ and $x^2 - my^2 = -1$ that contains their asymptotes contains infinitely many lattice points. In this formulation, the claim even holds when m is a square; in this case, all integral points lie on the asymptotes.

Show that the region between the two hyperbolas $2x^2 - 5y^2 = 1$ and $2x^2 - 5y^2 = -1$ does not contain any lattice point except $(0, 0)$.

7.13. Show that the continued fraction expansion of $\sqrt{m}$ for $m = t^2 - 1$ is given by

$$\sqrt{m} = [t-1; 1, 2t-2, 1, 2t-2, 1, 2t-2, \ldots] = [t-1; \overline{1, 2t-2}].$$

For example,

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \ldots}}}}}}.$$

7.14. Show that the continued fraction expansion of $\sqrt{m}$ for $m = t^2 + 2$ is given by

$$\sqrt{m} = [t; \overline{t, 2t}].$$

7.15. Show that $x^2 = a^3 + 3a$ for odd integers a is equivalent to

$$\left(\frac{a-1}{2}\right)^3 + \left(\frac{a+1}{2}\right)^3 = y^2,$$

where $y = \frac{x}{2}$.

Show moreover that the equation $y^2 = x(x^2 + 3)$ has the only integral points $(0, 0)$, $(1, \pm 2)$, $(3, \pm 6)$, and $(12, \pm 42)$ assuming that the equation $r^3 - 3s^4 = -2$ has the only integral solution $r = s = s$.

7.16. Let $p \equiv 3 \bmod 4$ be a prime number, and let $\varepsilon = t + u\sqrt{p}$ denote the fundamental unit of $\mathbb{Q}(\sqrt{p})$. Show that t is even and that $t \equiv 1 - (\frac{2}{p}) \bmod 4$.

7.17. Show that the function f defined in (7.2) is injective.

7.18. Let $\varepsilon = 2 + \sqrt{3}$ be the fundamental unit of $\mathbb{Z}[\sqrt{3}\,]$. Define the numbers $V_n = \varepsilon^n + \varepsilon'^n$ for $n \geq 0$. Show that these numbers satisfy the recurrence relation

$$V_{n+1} = 4V_n - V_{n-1}.$$

Also show that $V_{2n} = V_n^2 - 2$ and that the subsequence V_{2^n} consists of the numbers occurring in the Lucas–Lehmer test.