Scudra, Winkler, Pérez-Díaz
Rational Algebraic Curves
Springer (2008)

5.2 Rational Points on Conics

In the previous section we have analyzed optimal fields of parametrization of a curve $\mathcal{C}$ over K with ground field $\mathbb{K}$. The corollary to the theorem of Hilbert-Hurwitz tells us that if the degree of $\mathcal{C}$ is odd then the optimal field of parametrization is $\mathbb{K}$, otherwise it is a field extension of $\mathbb{K}$ of degree at most 2. Furthermore, the algorithm HILBERT-HURWITZ shows how the problem of checking the precise degree of this field extension can be reduced to the case of conics.

In this section, we focus on the case of conics. For certain fields we can decide the existence of rational points and, in the positive case, actually compute such points. Therefore, over such fields, we can derive an optimal parametrization algorithm. We present here the classical approach, based on the Legendre theory, for the case $\mathbb{K} = \mathbb{Q}$. For a description of the Legendre theory we refer to [CrR03], [IrR82], [Krä81], [LiN94] or [Ros88]. The relation of rational points and optimal parametrization has been investigated in [HiW98].

Throughout this section, $\mathcal{C}$ is a projective conic with ground field $\mathbb{Q}$, defined by

$$F(x, y, z) = a_1x^2 + a_2xy + a_3y^2 + a_4xz + a_5yz + a_6z^2,$$

where $a_i \in \mathbb{Q}$.

Our goal is to decide whether there is a rational point on $\mathcal{C}$, and if so, to compute one. By Theorem 5.6 we know that $\mathcal{C}$ has a rational point if and only if $\mathbb{Q}$ is an optimal field of parametrization; hence, if and only if, $\mathcal{C}$ has infinitely many rational points. In the following study, we distinguish between parabolas, ellipses (including circles), and hyperbolas. The case of parabolas is the easy one, and one may always, in fact, give an explicit formula for a rational point on it. However, the case of ellipses and hyperbolas is not so straight-forward. We need to manipulate the equation to reach a Legendre equation. The Legendre equation lets us decide the existence of rational points, and actually allows to compute such a point if it exists. In the sequel we denote by $\mathbb{Z}^\star$ the set of nonzero integers, and by $\mathbb{Z}^+$ the set of positive integers.

The Parabolic Case

We start by observing that $\mathcal{C}$ is a parabola if and only if the coefficients of $F(x, y, z)$ satisfy one of the following relations (see Exercise 2.3):

$$a_2^2 = 4a_1a_3 \quad \text{or} \quad a_4^2 = 4a_1a_6 \quad \text{or} \quad a_5^2 = 4a_3a_6.$$

Let us assume w.l.o.g that $a_2^2 = 4a_1a_3$, i.e. we consider a parabola with respect to x and y, where z is the homogenizing variable. Furthermore, let us assume that $a_3 \neq 0$ (otherwise, we may reason similarly by interchanging x and y). Then we have the relation

$$4a_3F(x,y,z) = (a_2x + 2a_3y + a_5z)^2 + (4a_3a_4 - 2a_2a_5)xz + (4a_3a_6 - a_5^2)z^2.$$

Since $\mathcal{C}$ is irreducible, this implies $4a_3a_4 - 2a_2a_5 \neq 0$. Thus,

$$\left(-2a_3(4a_3a_6 - a_5^2),\ -4a_5a_3a_4 + a_2a_5^2 + 4a_2a_3a_6,\ 4a_3(2a_3a_4 - a_2a_5)\right)$$

is a rational point on $\mathcal{C}$.

Example 5.10. Consider the affine parabola defined by

$$f(x,y) = x^2 + 2xy + y^2 + x + 2y - 2.$$

Since $a_3 \neq 0$, we can use the formula, and we get the rational point $(-3,2)$ on the parabola.

The Hyperbolic and the Elliptic Case

The hyperbolic/elliptic case is characterized by the conditions

$$a_2^2 \neq 4a_1a_3 \quad \text{and} \quad a_4^2 \neq 4a_1a_6 \quad \text{and} \quad a_5^2 \neq 4a_3a_6$$

on the coefficients of $F(x,y,z)$. By well-known techniques in linear algebra (see [Krä81]) we can find a linear change of coordinates over $\mathbb{Q}$ transforming the conic $\mathcal{C}$ onto a conic of the form

$$x^2 + ky^2 = \ell z^2 \tag{5.1}$$

where $k,\ \ell \in \mathbb{Q}$, and where either $k < 0$ or $\ell > 0$. This implies the existence of real points. Now, expressing k and ℓ as $k = \dfrac{k_1}{k_2},\quad \ell = \dfrac{\ell_1}{\ell_2}$ with $k_i,\ \ell_j \in \mathbb{Z}^*$, and cleaning up denominators in (5.1) we get the following equation over $\mathbb{Z}$

$$a'x^2 + b'y^2 + c'z^2 = 0 \tag{5.2}$$

where $a' = \operatorname{lcm}(k_2,\ \ell_2)$, $b' = \dfrac{k_1\,\ell_2}{\gcd(k_2,\ \ell_2)}$, and $c' = -\dfrac{\ell_1\,k_2}{\gcd(k_2,\ \ell_2)}$.

Clearly, a', b', c' are nonzero and do not all have the same sign. Now, we want to reduce (5.2) to an equation of similar form whose coefficients are squarefree and pairwise relatively prime.

First, we express a', b', c' as

$$a' = a_1'r_1^2,\quad b' = b_1'r_2^2,\quad c' = c_1'r_3^2,$$

where $a_1^{'}, b_1^{'}, c_1^{'}$ are squarefree (see Exercise 5.5). We get the equation

$$a_1'x^2 + b_1'y^2 + c_1'z^2 = 0 \tag{5.3}$$

Note that (5.3) has an integral solution if and only if (5.2) has one.
Next, we divide (5.3) by $\gcd(a_1', b_1', c_1')$, getting

$$a''x^2 + b''y^2 + c''z^2 = 0 \tag{5.4}$$

Now, we make the coefficients pairwise relatively prime. For this purpose, let $g_1 = \gcd(a'', b'')$, $a''' = a''/g_1$, $b''' = b''/g_1$, and let $(\overline{x}, \overline{y}, \overline{z})$ be an integral solution of (5.4). Then $g_1 \mid c''\overline{z}^2$, and hence, since $\gcd(a'', b'', c'') = 1$, we have $g_1 \mid \overline{z}^2$. Furthermore, since g_1 is squarefree (since a'', b'' are), we have $g_1 \mid \overline{z}$. So, letting $\overline{z} = g_1 z'$ and dividing (5.4) by g_1, we arrive at the equation

$$a'''\overline{x}^2 + b'''\overline{y}^2 + \underbrace{c''g_1}_{c'''}(z')^2 = 0.$$

At this point $\gcd(a''', b''') = 1$ and c''' is squarefree since g_1 and c'' are relatively prime. Repeating this process with $g_2 = \gcd(a''', c''')$ and $g_3 = \gcd(b'''', c'''')$ we finally arrive at an equation

$$a(x')^2 + b(y')^2 + c(z')^2 = 0 \ ,$$

where a, b, c satisfy the requirements in the following definition.

Definition 5.11. *Let $a, b, c \in \mathbb{Z}$ be such that $abc \neq 0$, and they satisfy the following conditions:*

$$\begin{aligned} &(i)\ \ a > 0,\ b < 0,\ \ \text{and}\ c < 0 \\ &(ii)\ \ a,\ \ b,\ \ \text{and}\ c\ \ \text{are squarefree} \\ &(iii)\ \ \gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1. \end{aligned} \tag{5.5}$$

Then, the equation

$$ax^2 + by^2 + cz^2 = 0 \tag{5.6}$$

is called a Legendre Equation.

Solving the Legendre Equation

The problem of finding a rational point on an ellipse or hyperbola reduces to the problem of finding a nontrivial integral solution of the so called Legendre Equation. Let us investigate necessary and sufficient conditions for the Legendre equation to have nontrivial integral solutions. By a nontrivial integral solution we mean a solution $(\overline{x}, \overline{y}, \overline{z}) \in \mathbb{Z}^3$ with $(\overline{x}, \overline{y}, \overline{z}) \neq$

$(0,0,0)$ and $\gcd(\overline{x},\overline{y},\overline{z})=1$. Such conditions are given by Legendre's Theorem (Theorem 5.17). Based on the description in [IrR82] we develop here a constructive proof from which we can extract an algorithm to compute integral solutions. For the formulation of Legendre's Theorem we need to introduce the notion of quadratic residues.

Definition 5.12. *Let $m, n \in \mathbb{Z}^\star$. Then we say that m is a* quadratic residue *modulo n, and we denote this by $m\,\mathcal{R}\,n$, if there exists $x \in \mathbb{Z}$ such that $x^2 \equiv_n m$.*

The problem of deciding whether $m\,\mathcal{R}\,n$ can be solved directly by checking all the elements in $\mathbb{Z}_n$. Alternatively, one may approach the problem by using Legendre's symbol (see [Coh00] or [IrR82] for the notion of Legendre's symbol). We outline here a method based on the notion of quadratic reciprocity to solve this question. If $n=1$ or $n=2$ the problem is trivial, and we may always assume w.l.o.g that $n>0$ (see Exercise 5.7). In this situation, if n is an odd prime number one can prove from the Law of quadratic reprocity (see Section 18.5 in [vGG99]) that $m\,\mathcal{R}\,n$ if and only if

$$m^{\frac{n-1}{2}} \equiv_n 1.$$

So we will have to deal with the case where $n>2$ and n is not a prime number.

Lemma 5.13. *Let $n, m \in \mathbb{Z}^\star$ such that $\gcd(m,n)=1$. If $a \in \mathbb{Z}^\star$ satisfies $a\,\mathcal{R}\,n$ and $a\,\mathcal{R}\,m$, then a also satisfies $a\,\mathcal{R}\,nm$.*

Proof: Since $a\,\mathcal{R}\,n$ and $a\,\mathcal{R}\,m$, there exist x_1, $x_2 \in \mathbb{Z}$ such that

$$x_1^2 \equiv_n a,\ x_2^2 \equiv_m a.$$

In addition, $\gcd(n,m)=1$ implies that there exist ℓ_1', $\ell_2' \in \mathbb{Z}$ such that $\ell_1' n - \ell_2' m = 1$. Thus, there exist ℓ_1, $\ell_2 \in \mathbb{Z}$, namely $\ell_i = \ell_i'(x_2 - x_1)$, $\ i=1,2$, such that

$$x_1 + \ell_1 n = x_2 + \ell_2 m\ .$$

In this situation we prove that for $x_3 = x_1 + \ell_1 n$ we get $x_3^2 \equiv_{nm} a$, from where we deduce that $a\,\mathcal{R}\,nm$. Indeed,

$$x_3^2 = (x_1+\ell_1 n)^2 \equiv_n x_1^2 \equiv_n a, \quad x_3^2 = (x_2+\ell_2 m)^2 \equiv_m x_2^2 \equiv_m a\ .$$

Thus, there exist $k_1, k_2 \in \mathbb{Z}$ such that

$$x_3^2 = a + k_1 n = a + k_2 m\ .$$

This implies that $k_1 n = k_2 m$. But $\gcd(n,m)=1$, and therefore n divides k_2. Hence, there exists $k_3 \in \mathbb{Z}$ such that $k_2 = k_3 n$, and then

$$x_3^2 = a + k_3 nm \equiv_{nm} a\ . \qquad \square$$

Now let us return to consider the case where $n > 2$ and n is not a prime number. Let

$$n = \prod_{i=1}^{r} n_i^{e_i}$$

be the irreducible factorization of n. Then, $m \mathcal{R} n$ implies that $m \mathcal{R} n_i$ for $i = 1, \ldots, r$ (see Exercise 5.7). Now, we distinguish two cases depending on whether n is squarefree or not.

Suppose n is squarefree. Then, $m \mathcal{R} n$ if and only if $m \mathcal{R} n_i$ for $i = 1, \ldots, r$ (note that the left-right implication always holds and for the right-left implication see Lemma 5.13). Thus, in this case, one may check whether $m \mathcal{R} n$ by checking whether $m \mathcal{R} n_i$, $\forall\, i = 1, \ldots, r$. We have seen above how this can be done for any prime number.

Now assume that n is not squarefree. Let $m \mathcal{R} n$, and let $x \in \mathbb{Z}$ be such that $x^2 \equiv_n m$. Then, we know that $x^2 \equiv_{n_i} m$ for $i = 1, \ldots, r$. Thus, one may check the existence of x as follows: if for some $i \in \{1, \ldots, r\}$ we have that $m \not\mathcal{R} n_i$, then $m \not\mathcal{R} n$. On the other hand, assume that for every $i \in \{1, \ldots, r\}$ we have $m \mathcal{R} n_i$ and $x_i \in \mathbb{Z}$ is such that $x_i^2 \equiv_{n_i} m$ (these x_i are usually not unique). For the possible $x \in \mathbb{Z}$ such that $x^2 \equiv_n m$ we must have that $x \equiv_{n_i} x_i$ for some candidates x_i. Thus, applying the Chinese Remainder Algorithm to these congruences one determines the possible candidates for x (observe that these candidates are $x + k \prod_{i=1}^{r} n_i$, for some k). Finally the problem is solved by checking whether any of these candidates satisfies $x^2 \equiv_n m$.

So now let us return to our original problem of solving the Legendre equation. First, we state some preliminary technical lemmas.

Lemma 5.14. *Let $n \in \mathbb{Z}^+$, and let α, β, and γ be positive non-integral real numbers such that $\alpha\beta\gamma = n$. Then, for every triple $(a_1, a_2, a_3) \in \mathbb{Z}^3 \backslash \{(0,0,0)\}$, the congruence*

$$a_1 x + a_2 y + a_3 z \equiv_n 0$$

has a solution $(\overline{x}, \overline{y}, \overline{z}) \neq (0,0,0)$ such that

$$|\overline{x}| < \alpha \ , |\overline{y}| < \beta, \text{ and } |\overline{z}| < \gamma.$$

Proof: Consider the set

$$S = \{(x, y, z) \in \mathbb{N}^3 \mid x \leq \lfloor \alpha \rfloor \text{ and } y \leq \lfloor \beta \rfloor \text{ and } z \leq \lfloor \gamma \rfloor\} \ .$$

Note that $\operatorname{card}(S) = (1 + \lfloor \alpha \rfloor)(1 + \lfloor \beta \rfloor)\,(1 + \lfloor \gamma \rfloor) > \alpha\beta\gamma = n$. Now we consider the set $\mathcal{A} = \{a_1 x + a_2 y + a_3 z \mid (x, y, z) \in S\}$. If $\operatorname{card}(\mathcal{A}) < \operatorname{card}(S)$, this means that there exist at least two distinct elements (x_1, y_1, z_1), $(x_2, y_2, z_2) \in S$ such that

$$a_1 x_1 + a_2 y_1 + a_3 z_1 = a_1 x_2 + a_2 y_2 + a_3 z_2 \ .$$

Now, let us assume that $\operatorname{card}(\mathcal{A}) = \operatorname{card}(S)$. Then, since $\operatorname{card}(S) > n$ and there are n residue classes modulo n, one deduces that there exist at least two distinct elements (x_1, y_1, z_1), $(x_2, y_2, z_2) \in S$ such that

$$a_1x_1 + a_2y_1 + a_3z_1 \equiv_n a_1x_2 + a_2y_2 + a_3z_2 \ .$$

In any case, $(\overline{x}, \overline{y}, \overline{z}) = (x_1 - x_2, y_1 - y_2, z_1 - z_2) \neq (0,0,0)$ is a solution of the congruence

$$a_1x + a_2y + a_3z \equiv_n 0 \ .$$

In addition, since α, β, and γ are positive non-integral real numbers, and $x_i, y_i, z_i \in \mathbb{N}$, we know that $0 \leq x_i < \alpha$, $0 \leq y_i < \beta$, $0 \leq z_i < \gamma$, for $i = 1, 2$. Thus,

$$|\overline{x}| = |x_1 - x_2| \leq \max\{x_1, x_2\} < \alpha \ ,$$

and similarly

$$|\overline{y}| < \beta, \quad \text{and} \quad |\overline{z}| < \gamma \ . \qquad \square$$

Lemma 5.15. *Let $m, n \in \mathbb{N}$ such that* $\gcd(m, n) = 1$, *and let $ax^2 + by^2 + cz^2$, with $a, b, c \in \mathbb{Z}$, be a form that factors modulo m and modulo n. Then, $ax^2 + by^2 + cz^2$ also factors modulo mn.*

Proof: See Exercise 5.6. □

Lemma 5.16. *Let $r \in \mathbb{Z}^+$ such that $-1 \, \mathcal{R} \, r$. Then, the equation*

$$x^2 + y^2 = r$$

has an integral solution.

Proof: First, since $-1 \, \mathcal{R} \, r$, there exists $x_0 \in \mathbb{Z}$ and $k \in \mathbb{Z}$ such that

$$x_0^2 + 1 = kr \ .$$

Moreover, $k \in \mathbb{N}^\star$ because $r > 0$. Let us assume that $k = 1$. Then, $(x_0, 1)$ is a nontrivial integral solution of the equation $x^2 + y^2 = r$; hence the statement holds. Now, let $k > 1$. Then, taking $y_0 = 1$, one has that (x_0, y_0) is a nontrivial integral solution of the equation $x^2 + y^2 = kr$. Then, let x_1, y_1 be integers of least absolute value such that $x_1 \equiv_k x_0$, and $y_1 \equiv_k y_0$. Note that there exist $c, d \in \mathbb{Z}$ such that $x_1 = x_0 + ck$, and $y_1 = y_0 + dk$. Thus,

$$x_1^2 + y_1^2 = (x_0 + ck)^2 + (y_0 + dk)^2 \equiv_k x_0^2 + y_0^2 \equiv_k 0 \ .$$

Therefore, there exists k' such that $x_1^2 + y_1^2 = k'k$. Moreover, because of $|x_1|, |y_1| \leq k/2$, we get

$$x_1^2 + y_1^2 \le \left(\frac{k}{2}\right)^2 + \left(\frac{k}{2}\right)^2 = \frac{1}{2}k^2 ,$$

and hence $0 < k' \le \frac{k}{2}$. Additionally

$$k'k^2r = (k'k)(kr) = (x_1^2 + y_1^2)(x_0^2 + y_0^2) = (x_0x_1 + y_0y_1)^2 + (x_0y_1 - x_1y_0)^2 ,$$

and therefore

$$k'r = \left(\frac{x_0x_1 + y_0y_1}{k}\right)^2 + \left(\frac{x_0y_1 - x_1y_0}{k}\right)^2 .$$

Now, let $x_2 = (x_0x_1 + y_0y_1)/k$, and $y_2 = (x_0y_1 - x_1y_0)/k$. We observe that

$$x_0x_1 + y_0y_1 = x_0(x_0 + ck) + y_0(y_0 + dk) \equiv_k x_0^2 + y_0^2 \equiv_k 0 ,$$

and

$$x_0y_1 - x_1y_0 = x_0(y_0 + dk) - y_0(x_0 + ck) \equiv_k 0 .$$

Thus, $x_2, y_2 \in \mathbb{Z}$, and (x_2, y_2) is a nontrivial integral solution of $x^2 + y^2 = k'r$. In this situation, since $k' \le k$, we either have a solution of $x^2 + y^2 = r$ (i.e. if $k' = 1$) or we may apply the previous reasoning again. Proceeding inductively we finally finish the proof. □

Remark. The proof of Lemma 5.16 is constructive. In the following we outline the corresponding algorithmic process. For this purpose, we will denote by "qr" an algorithmic procedure that decides whether $m\mathcal{R}n$, and that in the affirmative case outputs $x \in \mathbb{Z}$ such that $x^2 \equiv_n m$. Then, given $r \in \mathbb{Z}^+$ such that $-1\,\mathcal{R}\,r$, the computation of $\alpha, \beta \in \mathbb{Z}$ such that $r = \alpha^2 + \beta^2$, can be performed as follows.

1. Determine
$$\alpha := \mathrm{qr}(-1, r), \quad \beta := 1, \quad k := \frac{\alpha^2 + \beta^2}{r}.$$
2. While $k > 1$ do
$$\alpha_1 := \alpha \bmod k, \quad \beta_1 := \beta \bmod k, \quad \alpha_2 := \frac{\alpha_1\alpha + \beta_1\beta}{k},$$
$$\beta_2 := \frac{\alpha\beta_1 - \alpha_1\beta}{k}, \quad \alpha := \alpha_2, \quad \beta := \beta_2, \quad k := \frac{\alpha^2 + \beta^2}{r}.$$
3. Return (α, β). □

Now we are ready for stating Legendre's Theorem.

Theorem 5.17. (Legendre's Theorem) *The Legendre equation $ax^2 + by^2 + cz^2 = 0$ has a nontrivial integral solution if and only if $(-ab)\,\mathcal{R}\,c$, $(-bc)\,\mathcal{R}\,a$, and $(-ac)\,\mathcal{R}\,b$.*

Proof: Let $(\overline{x}, \overline{y}, \overline{z})$ be a nontrivial integral solution of $ax^2 + by^2 + cz^2 = 0$. Note that we can assume w.l.o.g that $\gcd(\overline{x}, \overline{y}, \overline{z}) = 1$. First we prove that $\gcd(c, \overline{x}) = 1$. Indeed, if any prime p divides $\gcd(c, \overline{x})$, then p divides $b\overline{y}^2$. Because of (5.5), $\gcd(b, c) = 1$, so p does not divide b. Thus, p divides $\overline{y}$. Consequently, p^2 divides $a\overline{x}^2 + b\overline{y}^2$, and hence p^2 divides $c\overline{z}^2$. Because of (5.5) c is squarefree, which implies that p divides $\overline{z}$. Therefore, p divides $\gcd(\overline{x}, \overline{y}, \overline{z})$, which is impossible. So, we have proved that $\gcd(c, \overline{x}) = 1$.
Now, since $\gcd(c, \overline{x}) = 1$ there exist $\lambda, \mu \in \mathbb{Z}$ such that $\lambda c + \mu\overline{x} = 1$. This implies that $\mu\overline{x} \equiv_c 1$. Furthermore, from the equality $a\overline{x}^2 + b\overline{y}^2 + c\overline{z}^2 = 0$ we get that $a\overline{x}^2 \equiv_c -b\overline{y}^2$. Thus,

$$b^2\mu^2\overline{y}^2 \equiv_c -ab(\overline{x}\mu)^2 \equiv_c -ab \ ,$$

and consequently we have $(-ab)\,\mathcal{R}\,c$. The remaining conditions can be derived analogously.
In order to prove the reverse implication we first deal with three special cases.

1. Case $b = c = -1$. In this case, the hypothesis $(-bc)\,\mathcal{R}\,a$ implies that $-1\,\mathcal{R}\,a$. So, by Lemma 5.16 there exist r, $s \in \mathbb{Z}$ such that $r^2 + s^2 = a$. Hence, in this case, $(1, r, s)$ is a nontrivial integral solution of the Legendre equation.
2. Case $a = 1$, $b = -1$. In this case $(1, 1, 0)$ is a nontrivial integral solution of the Legendre equation.
3. Case $a = 1$, $c = -1$. In this case $(1, 0, 1)$ is a nontrivial integral solution of the Legendre equation.

Now, we treat the general case. Since $(-ab)\,\mathcal{R}\,c$, there exists $t \in \mathbb{Z}$ such that

$$t^2 \equiv_c -ab \ .$$

On the other hand, because of (5.5) we have $\gcd(a, c) = 1$. Thus, there exists $a^* \in \mathbb{Z}$ such that $aa^* \equiv_c 1$, and therefore

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv_c aa^*(ax^2 + by^2) \equiv_c a^*(a^2x^2 + aby^2) \\ &\equiv_c a^*(a^2x^2 - t^2y^2) = a^*(ax - ty)(ax + ty) \\ &\equiv_c (x - a^*ty)(ax + ty) \ . \end{aligned}$$

Using the remaining hypotheses (i.e. $(-bc)\,\mathcal{R}\,a$, and $(-ac)\,\mathcal{R}\,b$) and reasoning similarly as above we see that $ax^2 + by^2 + cz^2$ can also be expressed as a product of linear factors modulo b and modulo a. Then, taking into account Lemma 5.15 and (5.5), we deduce that there exist $a_1, \ldots, a_6 \in \mathbb{Z}$ such that

$$ax^2 + by^2 + cz^2 \equiv_{abc} (a_1x + a_2y + a_3z)(a_4x + a_5y + a_6z) \ .$$

Now, we consider the congruence

$$(a_1x + a_2y + a_3z) \equiv_{abc} 0 \ .$$

Since we are not in any of the special cases, and since a, b and c satisfy (5.5), we have that $\sqrt{bc}$, $\sqrt{-ac}$, and $\sqrt{-ab}$ are non-integral real numbers, and their product is abc. Applying Lemma 5.14 to the previous congruence, with $\alpha = \sqrt{bc}$, $\beta = \sqrt{-ac}$, and $\gamma = \sqrt{-ab}$, we deduce that there exists a nontrivial integral solution, say (x_1, y_1, z_1) of $a_1x + a_2y + a_3z \equiv_{abc} 0$, where

$$|x_1| < \sqrt{bc}, \quad |y_1| < \sqrt{-ac}, \quad \text{and} \quad |z_1| < \sqrt{-ab}\ .$$

Thus, taking into account that

$$ax^2 + by^2 + cz^2 \equiv_{abc} (a_1x + a_2y + a_3z)(a_4x + a_5y + a_6z)\ ,$$

we deduce that

$$ax_1^2 + by_1^2 + cz_1^2 \equiv_{abc} 0\ .$$

Furthermore, since b and c are negative and $|x_1| < \sqrt{bc}$, the above inequalities imply that

$$ax_1^2 + by_1^2 + cz_1^2 \leq ax_1^2 < abc\ .$$

Moreover, since $a > 0$, $|y_1| < \sqrt{-Ac}$, $|z_1| < \sqrt{-ab}$ and b, c are negative, we have

$$ax_1^2 + by_1^2 + cz_1^2 \geq by_1^2 + cz_1^2 > b(-ac) + c(-ab) = -2abc\ .$$

Thus, $ax_1^2 + by_1^2 + cz_1^2$ is a multiple of abc, and $-2abc < ax_1^2 + by_1^2 + cz_1^2 < abc$. Hence, we are in one of the following cases:

$$ax_1^2 + by_1^2 + cz_1^2 = 0, \qquad \text{or} \qquad ax_1^2 + by_1^2 + cz_1^2 = -abc\ .$$

If the first case the result follows immediately. So let us assume that $ax_1^2 + by_1^2 + cz_1^2 = -abc$. In this situation, we introduce the integers

$$x_2 = x_1z_1 - by_1, \quad y_2 = y_1z_1 + ax_1, \quad z_2 = z_1^2 + ab\ .$$

For these numbers we get the relation

$$\begin{aligned} ax_2^2 + by_2^2 + cz_2^2 &= a(x_1z_1 - by_1)^2 + b(y_1z_1 + ax_1)^2 + c(z_1^2 + ab)^2 = \\ &= (ax_1^2 + by_1^2 + cz_1^2)z_1^2 - 2abx_1y_1z_1 + 2abx_1y_1z_1 + \\ &\quad + ab(by_1^2 + ax_1^2 + cz_1^2) + abcz_1^2 + a^2b^2c \\ &= (-abc)z_1^2 + ab(-abc) + abcz_1^2 + a^2b^2c = 0\ . \end{aligned}$$

Thus, (x_2, y_2, z_2) is a solution. Furthermore, it is a nontrivial solution. Indeed, if $z_1^2 + ab = 0$, the coprimality and squarefreeness of a and b imply that $a = 1$ and $b = -1$. But this case has been treated above.

This completes the proof. Nontrivial solutions have been found in all cases. □

Theorem 5.17 characterizes the existence of nontrivial solutions of the Legendre equation by means of quadratic residues. However, from the proof it is not clear how to compute a solution if it exists. In the following, we see how to approach the problem algorithmically. For this purpose, we first introduce the following notion.

Definition 5.18. *Let $ax^2+by^2+cz^2=0$ be a Legendre equation. The equation*

$$-x^2+(-ba)y^2+(-ca)z^2=0$$

is called the associated equation *to the Legendre equation.*

Remark. Consider the equation of the form $-x^2+Ay^2+Bz^2=0$, where A, B are positive squarefree integers. This equation is associated to the Legendre equation $\gcd(A,B)x^2-\frac{A}{\gcd(A,B)}y^2-\frac{B}{\gcd(A,B)}z^2=0$. □

Theorem 5.19. *The Legendre equation has a nontrivial integral solution if and only if its associated equation has a nontrivial integral solution.*

Proof: Let (λ,μ,γ) be a nontrivial integral solution of the Legendre equation $ax^2+by^2+cz^2=0$, i.e.

$$a\lambda^2+b\mu^2+c\gamma^2=0\ .$$

Multiplying by $-a$, we get

$$-(a\lambda)^2+(-ab)\mu^2+(-ac)\gamma^2=0\ .$$

Thus, $(-a\lambda,\mu,\gamma)$ is a nontrivial integral solution of the associated equation to the Legendre equation (note that $a>0$).
Conversely, if (λ,μ,γ) is a nontrivial integral solution of the associated equation to the Legendre equation, then

$$-\lambda^2+(-ba)\mu^2+(-ca)\gamma^2=0\ .$$

Multiplying by $-a$, we get

$$a\lambda^2+b(a\mu)^2+c(a\gamma)^2=0\ ,$$

so $(\lambda,a\mu,a\gamma)$ is a nontrivial integral solution of the Legendre equation (note that $a>0$). □

Remark. The proof of Theorem 5.19 provides an explicit transformation of solutions of the Legendre equation and solutions of the associated equation. More precisely,

(i) if (λ,μ,γ) is a nontrivial integral solution of the Legendre equation, then $(-a\lambda,\mu,\gamma)$ is a non-trivial integral solution of the associated equation, and

(ii) if (λ, μ, γ) is a nontrivial integral solution of the associated equation, then $(\lambda, a\mu, a\gamma)$ is a nontrivial integral solution of the Legendre equation. □

Applying Legendre's Theorem (Theorem 5.17) and Theorem 5.19, we may also characterize the existence of solutions of the associated equation by means of quadratic residues of its coefficients. More precisely, we get the following theorem.

Theorem 5.20. *The associated equation to the Legendre equation has a nontrivial solution if and only if* $(-ab)\,\mathcal{R}\,(-ac)$, $(-ac)\,\mathcal{R}\,(-ab)$, *and* $(-bc)\,\mathcal{R}\,a$.

Proof: From Theorem 5.19 we know that the equation $-x^2 + (-ba)y^2 + (-ca)z^2 = 0$ has a nontrivial integral solution if and only if the Legendre equation $ax^2 + by^2 + cz^2 = 0$ has one. From Theorem 5.17 we know that $ax^2 + by^2 + cz^2 = 0$ has a nontrivial integral solution if and only if $(-bc)\,\mathcal{R}\,a$, $(-ac)\,\mathcal{R}\,b$, and $(-ab)\,\mathcal{R}\,c$. Observe that $(-ac)\,\mathcal{R}\,(-a)$ and $(-ab)\,\mathcal{R}\,(-a)$ always hold; we see this by taking $x = a$ for both cases in Definition 5.12. Thus, from $(-ac)\,\mathcal{R}\,b$ and $(-ac)\,\mathcal{R}\,(-a)$ and Lemma 5.13 (note that $\gcd(a, b) = 1$ because of (5.5)) we get that $(-ac)\,\mathcal{R}\,(-ab)$. Similarly, from $(-ab)\,\mathcal{R}\,c$, $(-ab)\,\mathcal{R}\,(-a)$ and Lemma 5.13 we get that $(-ab)\,\mathcal{R}\,(-ac)$.
Conversely, we assume that $(-ab)\,\mathcal{R}\,(-ac)$, $(-ac)\,\mathcal{R}\,(-ab)$, and $(-bc)\,\mathcal{R}\,a$. Then from Exercise 5.7 (iv) we deduce that $(-ab)\,\mathcal{R}\,c$, $(-ac)\,\mathcal{R}\,b$, and $(-bc)\,\mathcal{R}\,a$. Theorem 5.17 now implies that $ax^2 + by^2 + cz^2 = 0$ has a nontrivial integral solution. Because of Theorem 5.19 this means that the associated equation $-x^2 + (-ba)y^2 + (-ca)z^2 = 0$ also has a nontrivial integral solution. □

Remark. Note that the conditions in Theorems 5.17 and 5.20 are equivalent. □

In the previous theorems we have seen how to reduce the study of the Legendre equation to its associated equation. In the next theorem we prove that if the associated Legendre equation has a nontrivial integral solution, then this solution can be determined algorithmically.

Theorem 5.21. *If the associated equation to the Legendre equation has a nontrivial integral solution, then it can be determined algorithmically.*

Proof: Let us assume that $-x^2+(-ba)y^2+(-ca)z^2 = 0$, the associated equation to the Legendre equation, has a nontrivial integral solution. By Theorem 5.20 we deduce that $(-ab)\,\mathcal{R}\,(-ca)$, $(-ca)\,\mathcal{R}\,(-ab)$, and $(-cb)\,\mathcal{R}\,a$. Let us first deal with two special cases.

(1) If $-ca = 1$ (that is $a = 1$ and $c = -1$, see Definition 5.11), then $(1, 0, 1)$ is a nontrivial integral solution, and if $-ba = 1$ (that is $a = 1$ and $b = -1$, see Definition 5.11), then $(1, 1, 0)$ is a nontrivial integral solution.

(2) Now consider the case $-ca = -ba$ (that is $c = b = -1$, see Definition 5.11). $(-cb)\,\mathcal{R}\,a$ means $-1\,\mathcal{R}\,a$, so by the Remark to Lemma 5.16 we can determine algorithmically integers r and s, not both zero, such that $a = r^2 + s^2$. Then, $(r^2 + s^2, s, r)$ is a nontrivial solution of $-x^2 + (-ba)y^2 + (-ca)z^2 = 0$.

Now we treat the general case. W.l.o.g. we assume that $-ba < -ca$, i.e. $-b < -c$. Otherwise we only have to interchange the roles of z and y. The strategy will be the following: first, we find a squarefree integer A, with $0 < A < -ca$, and we consider the new equation $Az^2 + (-ba)Y^2 = X^2$, where

$$A\,\mathcal{R}\,(-ba), \quad (-ba)\,\mathcal{R}\,A, \quad \text{and} \quad \frac{-A(-ba)}{\gcd(A,-ba)^2}\,\mathcal{R}\,\gcd(A,-ba)\ .$$

Thus, we reduce the given associated Legendre equation $(-ca)z^2 + (-ba)y^2 = x^2$ to a new equation associated to some Legendre equation (see Remark to Definition 5.18) having a nontrivial solution (see Theorem 5.20). Moreover, we show that a solution of the old equation can be computed from a solution of the new equation. After a finite number of steps, interchanging A and $-ba$ in case A is less than $-ba$ (we are assuming that $-ba < -ca$), we arrive either at the case $A = 1$ or at $A = -ba$, each of which has been treated in (1) or (2). Since $(-ba)\,\mathcal{R}\,(-ca)$, we deduce that there exist α, $k \in \mathbb{Z}$ such that

$$\alpha^2 = -ba + k(-ca)\ .$$

Observe that we can always assume $|\alpha| \leq -ca/2$. We express $k = Am^2$, where $A, m \in \mathbb{Z}$, and A is squarefree; note that A and m can be determined algorithmically from the squarefree factorization of k (see Exercise 5.5). So we have

$$\alpha^2 = -ba + Am^2(-ca)\ .$$

First we show that $0 < A < -ca$. From our assumption $-ba < -ca$ we get

$$0 \leq \alpha^2 = -ba + Am^2(-ca) < -ca + Am^2(-ca) = -ca(1 + Am^2)\ .$$

Neither A nor m can be 0, because otherwise $\alpha^2 = -ba$, which is impossible ($\gcd(a,b) = 1$ and a, b are squarefree). Furthermore, $-ca > 0$ implies that $0 < 1 + Am^2$, so $A > 0$.
The relations $\alpha^2 = -ba + Am^2(-ca)$, $-ba > 0$, and $|\alpha| \leq -ca/2$ imply

$$Am^2(-ca) = \alpha^2 + ba < \alpha^2 \leq \frac{(-ca)^2}{4}\ .$$

This finishes the proof of $0 < A < -ca$.
Now we consider the new equation

$$AZ^2 + (-ba)Y^2 = X^2\ ,$$

and we prove that this equation satisfies the same hypothesis as the equation original equation $(-ca)z^2 + (-ba)y^2 = x^2$. First, note that A, $-ba \in \mathbb{Z}^+$, and they are squarefree. Now,we prove that

$$A\,\mathcal{R}\,(-ba), \quad (-ba)\,\mathcal{R}\,A, \quad \text{and} \quad \frac{-A(-ba)}{\gcd(A,-ba)^2}\,\mathcal{R}\,\gcd(A,-ba)\ , \qquad (5.7)$$

which implies that $AZ^2 + (-ba)Y^2 = X^2$ is associated to some Legendre equation (see Remark to Definition 5.18). Observe that, by Theorem 5.20, we deduce that the new equation has a nontrivial solution.

Let us prove that each of these relations hold.

(i) First we prove that $A\mathcal{R}(-ba)$. For this purpose, we show that $A\mathcal{R}(-a)$ and $A\mathcal{R}b$ which implies, by Lemma 5.13, that $A\,\mathcal{R}\,(-ba)$. From $\alpha^2 = -ba + Am^2(-ca)$ and the squarefreeness of a we deduce that a divides α. So if we set $\alpha_1 = -\alpha/a$, then $\alpha_1 \in \mathbb{Z}$ and

$$-a\alpha_1^2 = b + Am^2c\ .$$

Hence,

$$Am^2c^2 \equiv_{-a} -cb\ .$$

Moreover, from $-a\alpha_1^2 = b + Am^2c$ and $\gcd(a,b) = 1$ we get $\gcd(m,a) = 1$. Because of $(-cb)\,\mathcal{R}\,(-a)$ there exists $y_1 \in \mathbb{Z}$ such that $y_1^2 \equiv_{-a} -cb$. Thus,

$$A \equiv_{-a} (m^\star)^2(c^\star)^2y_1^2\ ,$$

where $m^\star$ and $c^\star$ are the inverses of m and c modulo $-a$, respectively. m and a are relatively prime, so are c and a. Therefore, $A\,\mathcal{R}\,(-a)$.
Now we show that $A\,\mathcal{R}\,b$. Because of $(-ca)\,\mathcal{R}\,(ab)$ there exists $\beta \in \mathbb{Z}$ such that $\beta^2 \equiv_b (-ca)$. So from $\alpha^2 = -ab + Am^2(-ca)$ we get

$$\alpha^2 \equiv_b Am^2(-ca) \equiv_b Am^2\beta^2\ .$$

Observe that $\gcd(\beta,b) = 1$. Indeed, assume $1 \neq d = \gcd(\beta,b)$. Because of $\beta^2 \equiv_b (-ca)$ there exists $\lambda \in \mathbb{Z}$ such that $\beta^2 = (-ca) + \lambda b$. Therefore, d divides ca, which is impossible because of $\gcd(a,b) = \gcd(c,b) = 1$. Furthermore, note that by hypothesis a, b, c are pairwise relatively prime, so also $\gcd(ca,b) = \gcd(m,b) = 1$ (see Exercise 5.8). Putting all this together, we get

$$\alpha^2(m^*)^2(u^*)^2 \equiv_b A\ ,$$

where u^*, and m^* are the inverses of β, and m modulo b, respectively. Therefore, $A\,\mathcal{R}\,b$.

(ii) The condition $(-ba)\,\mathcal{R}\,A$ follows from $\alpha^2 = -ba + Am^2(-ca)$.

(iii) Finally, we show that $\frac{-A(-ba)}{\gcd(A,-ba)^2} \mathcal{R} \gcd(A,-ba)$ holds. Let $r = \gcd(A,-ba)$, $A_1 = A/r$ and $b_1 = -ba/r$. Then, we have to show that $(-A_1 b_1) \mathcal{R}\, r$. From $\alpha^2 = -ba + Am^2(-ca)$ we deduce that

$$\alpha^2 = b_1 r + A_1 r m^2(-ca) .$$

A is squarefree, so also r is squarefree, and hence that r divides α. So

$$A_1 m^2(-ca) \equiv_r -b_1 ,$$

which implies that

$$-A_1 b_1 m^2(-ca) \equiv_r b_1^2 .$$

Note that by hypothesis a, b, c are pairwise relatively prime, so by the same reasoning as above $\gcd(ca, r) = \gcd(m, r) = 1$. From $(-ca) \mathcal{R} (-ba)$ and $b_1 r = -ab$ we obtain $(-ca) \mathcal{R}\, r$. Thus, there exists $w \in \mathbb{Z}$ such that $w^2 \equiv_r (-ca)$. Observe that $\gcd(w, r) = 1$. Indeed, assume $1 \neq d = \gcd(w, r)$. Because of $w^2 \equiv_r (-ca)$ there exists $\lambda \in \mathbb{Z}$ such that $w^2 = (-ca) + \lambda r$. Therefore, d divides to ca, which is impossible because of $\gcd(ac, r) = 1$. Putting all this together, we get

$$-A_1 b_1 \equiv_r b_1^2 (m^*)^2 v^* \equiv_r b_1^2 (m^*)^2 (w^*)^2 ,$$

where v^*, m^* and w^* are the inverses of $-ca$ and m and w modulo r, respectively. Therefore, $(-A_1 b_1) \mathcal{R}\, r$.

So all the relations in (5.7) hold.
Finally, we show that if we have a nontrivial solution $(\overline{X}, \overline{Y}, \overline{Z})$ of $AZ^2 + (-ba)Y^2 = X^2$, we can algorithmically determine a nontrivial solution $(\overline{x}, \overline{y}, \overline{z})$ of $(-ca)z^2 + (-ba)y^2 = x^2$. So assume

$$A\overline{Z}^2 = \overline{X}^2 - (-ba)\overline{Y}^2 .$$

Then, taking into account that $Am^2(-ca) = \alpha^2 - (-ba)$, we get

$$(-ca)(A\overline{Z}m)^2 = (\overline{X}^2 - (-ba)\overline{Y}^2)(\alpha^2 - (-ba)) =$$
$$(\overline{X}\alpha + (-ba)\overline{Y})^2 - (-ba)(\alpha\overline{Y} + \overline{X})^2 .$$

Thus,

$$\overline{x} = \overline{X}\alpha + (-ba)\overline{Y}, \quad \overline{y} = \alpha\overline{Y} + \overline{X}, \quad \overline{z} = A\overline{Z}m ,$$

is a solution of the equation $(-ca)z^2 + (-ba)y^2 = x^2$. Clearly, $(\overline{x}, \overline{y}, \overline{z}) \in \mathbb{Z}^3$, but we still have to prove that the solution is nontrivial. For this purpose, we write the above equalities in matrix notation as:

$$\begin{pmatrix} \overline{x} \\ \overline{y} \\ \overline{z} \end{pmatrix} = \begin{pmatrix} \alpha & -ba & 0 \\ 1 & \alpha & 0 \\ 0 & 0 & Am \end{pmatrix} \cdot \begin{pmatrix} \overline{X} \\ \overline{Y} \\ \overline{Z} \end{pmatrix} .$$

The determinant of the matrix is $Am(\alpha^2-(-ba))$. $A > 0$, $m \neq 0$ and $\alpha^2 \neq -ba$ because $\gcd(a, b) = 1$ and a, b are squarefree. So the determinant is non-zero. Since $(\overline{X}, \overline{Y}, \overline{Z})$ is nontrivial, $(\overline{x}, \overline{y}, \overline{z})$ is also nontrivial. □

In Theorems 5.19 and 5.20, we have seen how to decide whether the Legendre equation has nontrivial solutions (see also the algorithmic comments given after Definition 5.11), and the proof of Theorem 5.21 shows how to compute a nontrivial solution of the Legendre equation, if there exists one. In the following, assuming that the existence of nontrivial solutions has already been checked, we outline an algorithm (derived from the proof of Theorem 5.21) for determining a nontrivial solution of the Legendre equation. To be more precise, we assume that the equation is given in Legendre form (see (5.5) and (5.6)). As above, we assume an algorithm "qr", which for given inputs m, n decides whether $m\mathcal{R}n$, and in the affirmative case outputs $x \in \mathbb{Z}$ such that $x^2 \equiv_n m$. Furthermore, we represent by "oddf" an algorithmic procedure such that if $k \in \mathbb{Z}^*$, then oddf(k) is a squarefree integer A satisfying $k = Am^2$ with $m \in \mathbb{Z}$.

Algorithm ASSOCIATED LEGENDRE SOLVE

Given positive squarefree integers B, C such that the equation $-x^2+By^2+Cz^2 = 0$ has a nontrivial solution, the algorithm computes a nontrivial integral solution $(\overline{x}, \overline{y}, \overline{z})$ of the equation $-x^2 + By^2 + Cz^2 = 0$.

1. If $C = 1$, then set $(\overline{x}, \overline{y}, \overline{z}) = (1, 0, 1)$, and go to Step 6.
2. If $B = 1$, then set $(\overline{x}, \overline{y}, \overline{z}) = (1, 1, 0)$, and go to Step 6.
3. If $C = B$, then compute r, $s \in \mathbb{Z}^*$ such that $B = C = r^2 + s^2$ (see Lemma 5.16 and the following remark). Set $(\overline{x}, \overline{y}, \overline{z}) = (r^2 + s^2, s, r)$, and go to Step 6.
4. If $C < B$, then apply Algorithm ASSOCIATED LEGENDRE EQUATION to the inputs C, B. Let (x_1, y_1, z_1) be the solution obtained. Set $(\overline{x}, \overline{y}, \overline{z}) = (x_1, z_1, y_1)$, and go to Step 6.
5. If $B < C$, then compute
$$\alpha := \mathrm{qr}(B, C), \quad k := (\alpha^2 - B)/C, \quad A := \mathrm{oddf}(k), \quad m := \sqrt{k/A}\,.$$
Apply Algorithm ASSOCIATED LEGENDRE SOLVE to the inputs B, A. Let (x_1, y_1, z_1) be the solution obtained. Set $(\overline{x}, \overline{y}, \overline{z}) = (\alpha x_1 + By_1, \alpha y_1 + x_1, Amz_1)$, and go to Step 6.
6. Return the point $(\overline{x}, \overline{y}, \overline{z})$.

Algorithm LEGENDRE SOLVE
Given integers a, b, c defining the Legendre equation $ax^2 + by^2 + cz^2 = 0$, having nontrivial solutions (see Definition 5.11), the algorithm computes a nontrivial integral solution $(\overline{x}, \overline{y}, \overline{z})$ of the Legendre equation.

1. Compute the point (x_1, y_1, z_1) obtained by applying the Algorithm ASSOCIATED LEGENDRE SOLVE to the pair $(-ba, -ca)$.
2. Return the point $(\overline{x}, \overline{y}, \overline{z}) = (x_1, ay_1, az_1)$.

Example 5.22. Consider the Legendre Equation

$$\text{(i)} \qquad 7x^2 - y^2 - 3z^2 = 0.$$

We show how to solve this equation by the Algorithm LEGENDRE SOLVE.
LEGENDRE SOLVE $(7, -1, -3)$:

$$a = 7, \qquad b = -1, \qquad c = -3.$$

```
(STEP 1) ASSOCIATED LEGENDRE SOLVE $(7, 21)$:
    $B = 7, \quad C = 21$
    (ii)  $-x^2 + 7y^2 + 21z^2 = 0.$
    (STEP 5) $B < C$, so
        $\alpha = \mathrm{qr}(7, 21) = 14, \quad k = \frac{196-7}{21} = 9, \quad A = 1, \quad m = 3.$
        ASSOCIATED LEGENDRE SOLVE $(7, 1)$:
            $B = 7, \quad C = 1$
            (iii)  $-x^2 + 7y^2 + z^2 = 0.$
            (STEP 1) $C = 1$, so
            Return $(1, 0, 1)$   (Solution of (iii))
        $(\overline{x}, \overline{y}, \overline{z}) := (14 \cdot 1 + 7 \cdot 0, 14 \cdot 0 + 1, 1 \cdot 3 \cdot 1) = (14, 1, 3)$
    Return $(14, 1, 3)$   (Solution of (ii))
(STEP 2) $(\overline{x}, \overline{y}, \overline{z}) := (14, 7, 21)$
Return $(14, 7, 21)$   (Solution of (i))
```

5.3 Optimal Parametrization of Rational Curves

We have seen how the theorem of Hilbert-Hurwitz (Theorem 5.8) can be used to classify optimal fields of parametrization of a rational curve, and in addition we have outlined an algorithm derived from the constructive proof of its corollary. But the algorithm, although theoretically interesting, does not have very satisfactory performance in practice. The reason is that, in general, $\mathcal{O}(d)$ birational transformations are required in order to reach a conic or a line and to invert either the simple points or the parametrization. Furthermore