Points on Algebraic Curves and the Parametrization Problem *

Erik Hillgarter and Franz Winkler
Institut für Mathematik and RISC-LINZ
Johannes Kepler Universität
A-4040 Linz, Austria

28.2.1997

Abstract

A plane algebraic curve is given as the zeros of a bivariate polynomial. However, this implicit representation is badly suited for many applications, for instance in computer aided geometric design. What we want in many of these applications is a rational parametrization of an algebraic curve. There are several approaches to deciding whether an algebraic curve is parametrizable and if so computing a parametrization. In all these approaches we ultimately need some simple points on the curve. The field in which we can find such points crucially influences the coefficients in the resulting parametrization. We show how to find such simple points over some practically interesting fields. Consequently, we are able to decide whether an algebraic curve defined over the rational numbers can be parametrized over the rationals or the reals. Some of these ideas also apply to parametrization of surfaces. If in the term geometric reasoning we do not only include the process of proving or disproving geometric statements, but also the analysis and manipulation of geometric objects, then algorithms for parametrization play an important role in this wider view of geometric reasoning.

I. The parametrization problem

An algebraic curve $\mathcal{C}$ in the affine plane $\mathbf{A}^2(\mathbf{K})$ over the algebraically closed field $\mathbf{K}$ is defined as

$$\mathcal{C} = \{(x, y) \in \mathbf{K}^2 | f(x, y) = 0\},$$

where $f(x, y)$ is a bivariate square–free polynomial with coefficients in $\mathbf{K}$, called the defining polynomial of $\mathcal{C}$. Observe that the defining polynomial of a plane algebraic curves is determined up to multiplication by non-zero constants in $\mathbf{K}$. The curve $\mathcal{C}$ is irreducible iff its defining polynomial is irreducible. The degree of $\mathcal{C}$, $\deg(\mathcal{C})$, is simply the degree of the defining polynomial f.

The singularity structure of an algebraic curve is not fully apparent in the affine plane, since the curve might have "singularities at infinity". So from time to time we will need to view an algebraic curve as an entity in the projective plane $\mathbf{P}^2(\mathbf{K})$. The affine plane is embedded into the projective plane by identifying an affine point (a, b) with the projective point $(a : b : 1)$. In addition to these affine points, the projective plane contains *points at infinity*, with projective coordinates $(a : b : 0)$, where $(a, b) \neq (0, 0)$. A projective curve agrees with the corresponding

*Partially supported by *Österr. Fonds zur Förderung der wissenschaftlichen Forschung*, Proj. HySaX, Nr. P11160-TEC.

affine curve, except that finitely many points at infinity are added. The points on the projective curve are the solutions of $F(x,y,z)=0$, where $F(x,y,z)$ is the homogenization of $f(x,y)$ w.r.t. the homogenizing variable z.

Some algebraic curves can also be represented parametrically, i.e. their points can be generated by rational functions

$$x(t)=\frac{p_1(t)}{q_1(t)}, \quad y(t)=\frac{p_2(t)}{q_2(t)},$$

for some $p_1(t), p_2(t), q_1(t), q_2(t) \in \mathbf{K}[t]$. More precisely, we have the following definition.

Definition I.1: If the irreducible affine plane curve $\mathcal{C}$ is defined by $f(x,y) \in \mathbf{K}[x,y]$, $\mathbf{K}$ an algebraically closed field of characteristic 0, then $x(t), y(t) \in \mathbf{K}(t)$, the field of rational functions over $\mathbf{K}$, constitute a *rational parametrization* of $\mathcal{C}$ iff, except for finitely many exceptions, every evaluation $(x(t_0), y(t_0))$ at $t_0 \in \mathbf{K}$ is a point on $\mathcal{C}$, and conversely almost every point on $\mathcal{C}$ is the result of evaluating the parametrization at some element of $\mathbf{K}$.

In this case $\mathcal{C}$ is called *parametrizable* or *rational.*

Equivalently, $\mathcal{P}(t)=(x(t),y(t))$ is a rational parametrization of $\mathcal{C}$ if $\mathcal{P}:\mathbf{K}\longrightarrow\mathcal{C}$ is rational and not both $x(t)$ and $y(t)$ are constant. Furthermore, if $\mathcal{P}$ is birational we say that $\mathcal{P}(t)$ is a *proper parametrization.* □

In computer aided geometric design (cagd) one usually requires that the algebraic curves are rational, see e.g. [3]. In fact, transformation methods between these two representations of algebraic curves of genus 0 are of great interest in cagd. This problem appears as one of the 10 most important problems in cagd in [9].

The problem of deciding whether an algebraic curve over an algebraically closed field of characteristic 0 is rational was solved by Hilbert and Hurwitz more that 100 years ago [1]. In fact, they prove that if the rational curve $\mathcal{C}$ is defined by a polynomial $f(x,y) \in \mathbf{K}[x,y]$, where $\mathbf{K}$ is not necessarily algebraically closed, then $\mathcal{C}$ has a parametrization with coefficients in an algebraic extension field $\mathbf{L}$ of $\mathbf{K}$ with $[\mathbf{L}:\mathbf{K}] \leq 2$ and $\mathbf{L}=\mathbf{K}$ for $\deg(f)$ odd. The construction of such an "optimal" parametrization requires $\mathcal{O}(\deg(f))$ birational transformation. Every such transformation decreases the degree of the curve by 2, and thus ultimately leads to either a line (in the odd degree case) or to an irreducible conic $\mathcal{C}_2$ defined over the same field as the original curve $\mathcal{C}$. This reduction process was abbreviated in [13] and actually the corresponding conic can simply be interpolated. Every point on the conic $\mathcal{C}_2$ corresponds rationally to a point on $\mathcal{C}$ and vice versa (with finitely many exceptions). So, if we can find a point of $\mathcal{C}_2$ in an extension field $\mathbf{L}$ of $\mathbf{K}$, then we can parametrize $\mathcal{C}_2$ and $\mathcal{C}$ with coefficients in $\mathbf{L}$.

In a geometric approach to the parametrization problem, we consider a linear system $\mathcal{L}$ of curves having prescribed multiplicities at the singular points of $\mathcal{C}$. In particular, it is reasonable (but not necessary) to consider a system $\mathcal{L}$ of curves of degree $\deg(\mathcal{C})-2$ and require that every singular point P of $\mathcal{C}$ be a point on every curve in $\mathcal{L}$ with multiplicity at least $\mathrm{mult}_P(\mathcal{C})-1$. $\mathcal{L}$ is called the system of adjoint curves of $\mathcal{C}$. The dimension of $\mathcal{L}$ is $\deg(\mathcal{C})-2$. So by fixing $\deg(\mathcal{C})-3$ simple points on $\mathcal{C}$ to also be simple points on every curve in $\mathcal{L}$, we reduce the dimension of $\mathcal{L}$ to 1, i.e. every curve in $\mathcal{L}$ will intersect $\mathcal{C}$ in the fixed points (the singularities and some fixed simple points of $\mathcal{C}$) and exactly 1 additional simple point on $\mathcal{C}$, which depends rationally on the free parameter of the sysem $\mathcal{L}$. This immediately yields the desired parametrization of $\mathcal{C}$. This geometric approach was theoretically described in [14] and was investigated from the computer algebra point of view in [12].

Example I.1: The irreducible curve $\mathcal{C}$ in the affine plane over the complex numbers C is defined by

$$f(x,y) \quad = \quad x^5+3x^4y-2x^3y^2+x^2y^3+y^5-2x^4-4x^3y+x^2y^2$$

$$-xy^3 - 2y^4 + x^3 + x^2y + xy^2 + y^3.$$

$\mathcal{C}$ has a triple point P_1 at the origin $(0,0)$, and double points $P_2 = (0,1), P_3 = (1,1), P_4 = (1,0)$. So the genus of $\mathcal{C}$ is 0, and it is parametrizable. In order to construct a subsystem of dimension 1 of the system of adjoints of $\mathcal{C}$, we need 2 simple points on $\mathcal{C}$. Intersecting $\mathcal{C}$ by the line $\overline{P_2P_3}$ we get the simple point $P_5 = (-3,1)$, and intersecting $\mathcal{C}$ by the line $\overline{P_2P_4}$ we get the simple point $P_6 = (5/6, 1/6)$. The system $\mathcal{A}$ of adjoints of degree 3 having multiplicity 2 at the base point P_1 and 1 at the base points P_2, P_3, P_4, P_5, P_6 is defined by

$$h(x,y,t) = -tx^3 - 3tx^2y + (3t-1)xy^2 + (5-7t)y^3 + tx^2 + xy + (7t-5)y^2.$$

Because of Bézout's theorem we expect the intersection multiplicity of curves in $\mathcal{A}$ with $\mathcal{C}$ to be $5 \cdot 3 = 15$. In the base points of $\mathcal{A}$ we get an intersection multiplicity of $6+2+2+2+1+1 = 14$. So a general element of $\mathcal{A}$ has one more intersection point with $\mathcal{C}$, depending rationally on the parameter t. This point traverses the curve $\mathcal{C}$ as t traverses the affine line, yielding the following rational parametrization of $\mathcal{C}$:

$$\begin{aligned} x(t) &= \frac{-648t^5 + 2502t^4 - 3900t^3 + 3067t^2 - 1217t + 195}{702t^5 - 2673t^4 + 4113t^3 - 3196t^2 + 1254t - 199}, \\ y(t) &= \frac{-216t^5 + 810t^4 - 1194t^3 + 859t^2 - 298t + 39}{702t^5 - 2673t^4 + 4113t^3 - 3196t^2 + 1254t - 199}. \end{aligned}$$

Since the simple points P_5, P_6 have coefficients in $\mathbf{Q}$, also the parametrization has coefficients in $\mathbf{Q}$, i.e. we need no algebraic extension of the field of coefficients. $\square$

Alternative algebraic approaches to the problem of parametrization of algebraic curves are investigated in [4] and [7]. But also in these approaches the field of coefficients $\mathbf{L}$ of the parametrization is precisely the field in which we can construct simple points of the curve $\mathcal{C}$.

So in any case, the determination of an optimal field of parametrization $\mathbf{L}$, i.e. a field achieving the bound on the extension degree in the paper of Hilbert and Hurwitz, hinges on the ability to determine points on irreducible conics. Let us demonstrate this fact by a simple example.

Example I.2: We consider the tacnode curve $\mathcal{C}$ in the affine plane over $\mathbf{C}$ defined by

$$f(x,y) = 2x^4 - 3x^2y + y^2 - 2y^3 + y^4.$$

The tacnode curve has double points at $(0,0)$ and $(0,1)$, and one more double point in the first neighborhood of $(0,0)$. So we need one more point on $\mathcal{C}$ for determining a system of adjoints of degree 2 and dimension 1.

(a) Intersection of $\mathcal{C}$ with the line $y = -1$ yields the simple point $P_1 = (\alpha, 1)$ on $\mathcal{C}$, where α is any one of the 4 roots of the irreducible polynomial $2z^4 + 3z^2 + 4$. This leads to the following parametrization over $\mathbf{Q}(\alpha)$:

$$\begin{aligned} x(t) &= \frac{-36\alpha t^4 + (48\alpha^2 + 144)t^3 + (108\alpha^3 + 18\alpha)t^2 - (40\alpha^2 - 84)t + 24\alpha^3 + 20\alpha)}{4 \cdot (9t^4 + 24\alpha t^3 - (16\alpha^2 + 60)t^2 - (24\alpha^3 + 20\alpha)t + 12\alpha^2 + 6)}, \\ y(t) &= \frac{-9t^4 - (18\alpha^3 + 3\alpha)t^3 + (2\alpha^2 - 33)t^2 - (12\alpha^3 + 2\alpha)t - 4}{(9t^4 + 24\alpha t^3 - (16\alpha^2 + 60)t^2 - (24\alpha^3 + 20\alpha)t + 12\alpha^2 + 6)}. \end{aligned}$$

The coefficients of this parametrization are in $\mathbf{C} \backslash \mathbf{R}$.

(b) Intersection of $\mathcal{C}$ with the line $y = 1$yields the simple point $P_2 = (\beta, 1)$ on $\mathcal{C}$, where β is any one of the 2 roots of the irreducible polynomial $2z^2 - 3$. This leads to the following parametrization over $\mathbf{Q}(\beta)$:

$$\begin{aligned} x(t) &= \frac{2\beta t^4 + 9t^3 - 27t - 18\beta}{11t^4 + 24\beta t^3 + 12t^2 + 18}, \\ y(t) &= \frac{2t^4 + 12\beta t^3 + 39t^2 + 36\beta t + 18}{11t^4 + 24\beta t^3 + 12t^2 + 18}. \end{aligned}$$

The coefficients of this parametrization are in $\mathbf{R}$.

(c) Intersection of $\mathcal{C}$ with the line $x = 1$ yields the simple point $P_3 = (1, 2)$ on $\mathcal{C}$. This leads to the following parametrization over $\mathbf{Q}(\beta)$:

$$\begin{aligned} x(t) &= \frac{2t^4 + 7t^3 - 21t - 18}{9t^4 + 40t^3 + 64t^2 + 48t + 18}, \\ y(t) &= \frac{4t^4 + 28t^3 + 73t^2 + 84t + 36}{9t^4 + 40t^3 + 64t^2 + 48t + 18}. \end{aligned}$$

Thus, the field in which we can find a simple point on $\mathcal{C}$ determines the coefficient field of the resulting parametrization.

Fig. 1

□

In fact, because every rational curve can be birationally transformed into a conic over the same coefficient field, it suffices to find simple points on irreducible conics.

Relation of parametrization to geometric reasoning

If in the term geometric reasoning we do not only include the process of proving or disproving geometric statements, but also the analysis and manipulation of geometric objects, then algorithms for parametrization play an important role in this wider view of geometric reasoning. Implicitization and parametrization are operations for changing the algebraic representation of geometric objects. For some operations we want implicit representations, e.g. for deciding whether a point actually belongs to a curve or surface. For other operations we want (some of) the geometric objects in parametric representation, e.g. for intersection of objects or for visualization.

II. Rational points on conics

In this section, we consider irreducible curves of degree two (so called "conics") with rational coefficients. Such a conic in the projective plane over $\mathbf{Q}$ is defined by an *irreducible* homogeneous polynomial $g \in \mathbf{Q}[x,y,z]$ of degree two as the set $\{(\overline{x}:\overline{y}:\overline{z}) \in \mathbf{P}^2(\mathbf{Q}) \mid g(\overline{x},\overline{y},\overline{z}) = 0\}$. In the sequel we refer to

$$\begin{aligned} g(x,y,z) &= ax^2+bxy+cy^2+dxz+eyz+fz^2 = 0, \text{ respectively} && (1)\\ g(x,y,1) &= ax^2+bxy+cy^2+dx+ey+f = 0 && (2)\end{aligned}$$

as the general conic equation (1). We call $(\overline{x}:\overline{y}:\overline{z}) \in \mathbf{P}^2(\mathbf{Q})$ a *rational point* on the conic defined by (1) if and only if $g(\overline{x},\overline{y},\overline{z}) = 0$. Our goal is to decide whether there is a rational point on the conic, and if so, compute one. We follow the presentation of [2], where any missing details can be found.
The following theorem shows that the existence of one rational point on a conic implies that there are infinitely many rational points on it. In particular, if the projective conic defined by (1) has a rational point, then the affine conic defined by (2) has a rational point in $\mathbf{A}^2(\mathbf{Q})$.

Theorem II.1: *On a curve of order two with rational coefficients lie no or infinitely many rational points.*

Proof: We give only a sketch of the proof. Suppose there is a rational point on the conic. Then we intersect the conic with a line through this rational point having a rational direction-vector. We will usually get two intersection points - the original rational point and an additional rational point. Varying the slope of the line leads to infinitely many other rational points on the conic. $\square$

We will see that it makes sense to distinguish between parabolas on the one hand and ellipses and hyperbolas on the other hand, since on a parabola we are guaranteed to find one (and therefore infinitely many) rational point(s). Indeed, in the parabolic case we can give a formula for a rational point on the conic (namely a rational function in the coefficients of (1)). On the other hand, on an ellipse or hyperbola we are not guaranteed that such a rational point even exists. In case it does (we will show how to decide that) we can compute such a point by an algorithm that is based on a constructive proof of the so called *Legendre Theorem*. So let us first deal with the parabolic case.

The parabolic case

We speak of a parabola if the coefficients of (1) satisfy one of the following relations :

$$b^2 = 4ac, \text{ or } d^2 = 4af, \text{or } e^2 = 4cf.$$

W. l. o. g. we assume now the case $b^2 = 4ac$, i. e. we consider a parabola with respect to x and y, whereas z is the homogenizing variable (which will be set to 1 in the following).

The following transformations can be found in [6]. First of all, let us assume $c \neq 0$. Then we have $g(x, y, 1) = 0$ iff $4cg(x, y, 1) = 0$. The following lemma is proved by simple expansion.

Lemma II.2: (Transformed parabolic equation) *For g with $b^2 = 4ac$ and $c \neq 0$ we have*

$$4cg(x, y, 1) = (bx + 2cy + e)^2 + d'x + f',$$

where $d' = 4cd - 2be$, $f' = 4cf - e^2$.

Thus

$$g(x, y, 1) = 0 \quad \text{if and only if} \quad (bx + 2cy + e)^2 + d'x + f' = 0,$$

and since we have $d' \neq 0$ (otherwise we would not have an irreducible conic), a rational solution is given by

$$\overline{x} = -\frac{f'}{d'},\ \overline{y} = -\frac{e + b\overline{x}}{2c},\ (\overline{z} = 1).$$

(One gets this solution by setting the terms inside and outside the brackets to zero separately).

Now the only remaining case to treat is the one when $c = 0$. Again by irreducibility, we have $a \neq 0$. A rational solution is then given by

$$\begin{aligned} \overline{y} &= -\frac{f'}{d'},\ \overline{x} = -\frac{d + b\overline{y}}{2a},\ (\overline{z} = 1), \\ \text{where } d' &= 4ae - 2bd,\ f' = 4af - d^2. \end{aligned}$$

Example II.1: Consider

$$g(x, y, 1) = x^2 + 2xy + y^2 + x + 2y - 2,$$

i.e. $(a, b, c, d, e, f) = (1, 2, 1, 1, 2, -2)$.
Since $a \neq 0$ and $c \neq 0$ we might use both formulae. Let us first use the formula for the case $c \neq 0$.

$$d' = 4cd - 2be = -4, \text{ and } f' = 4cf - e^2 = -12.$$

So we get

$$\overline{x} = -\frac{f'}{d'} = -3,\ \overline{y} = -\frac{e + b\overline{x}}{2c} = 2.$$

Indeed $g(-3, 2, 1) = 0$, as one might check.
Now we use the formula for the case $a \neq 0$:

$$d' = 4ae - 2bd = 4, \text{ and } f' = 4af - d^2 = -9.$$

Hence we get

$$\overline{y} = -\frac{f'}{d'} = \frac{9}{4},\ \overline{x} = -\frac{d + b\overline{y}}{2a} = -\frac{11}{4}.$$

Again, $g(-\frac{11}{4}, \frac{9}{4}, 1) = 0$ holds. □

The hyperbolic/elliptic case

We consider (1), but we impose other conditions on the coefficients. We use again ideas from [6]. The hyperbolic/elliptic case is characterized by

$$b^2 \neq 4ac \text{ and } d^2 \neq 4af \text{ and } e^2 \neq 4cf.$$

We consider the dehomogenization with respect to z (i. e. in what follows, we will only make use of $b^2 \neq 4ac$). Let us define

$$N = 4de - 4bf,\ D = 4ac - b^2,$$
$$M_1 = 4c^2d^2 - 4bcde + 4ace^2 + 4b^2cf - 16ac^2f,$$
$$M_2 = 4a^2e^2 - 4bade + 4acd^2 + 4b^2af - 16ca^2f.$$

We consider two cases.
(CASE $a = c = 0$**)** In this case we have $b \neq 0$ and $N \neq 0$ (by irreducibility). In the new coordinates

$$x' = b(x+y) + d + e,$$
$$y' = b(x-y) - d + e$$

the equation $4bg(x, y, 1) = 0$ has the following form :

$$(x')^2 - (y')^2 = N.$$

(CASE $c \neq 0$**)** We have $M_1 \neq 0$ and $(D > 0 \Rightarrow M_1 > 0)$ (both conditions are consequences of irreducibility). Under the coordinate change

$$x' = Dx + 2dc - be,$$
$$y' = bx + 2cy + e$$

the equation $4cDg(x, y, 1) = 0$ becomes

$$(x')^2 + D(y')^2 = M_1.$$

Observe that the case $a \neq 0$ is totally analogous to the case $c \neq 0$ (just interchange the roles of x and y and therefore also those of a and c and those of d and e; in addition use M_2 instead of M_1).

In both cases we arrive at an equation of the form

$$X^2 + KY^2 = L, \tag{3}$$

where $K, L \in Q$, and in both cases we do not have $(K > 0 \wedge L < 0)$, which would exclude the existence of a real solution.

So let us now consider equations of this form . Switching to homogeneous coordinates we set

$$X = \frac{x}{z},\ Y = \frac{y}{z},\ K = \frac{b'}{a'},\ L = -\frac{c'}{a'}.$$

Note that if $K = k_1/k_2$, $L = l_1/l_2$ we may choose $a' = \mathrm{lcm}(k_2, l_2)$, $b' = k_1 l_2/\gcd(k_2, l_2)$, and $c' = -l_1 k_2/\gcd(k_2, l_2)$. Then (3) becomes the Diophantine equation

$$a'x^2 + b'y^2 + c'z^2 = 0. \tag{4}$$

Clearly a', b', and c' are nonzero and do not all have the same sign (look at their definitions and use $\neg(K > 0 \wedge L < 0)$). But we want to achieve more, namely the reduction of (4) to an equation of similar form whose coefficients are squarefree and pairwise relatively prime. We use ideas from [11]. Let us assume that

$$a' = a'_1\, r_1^2,\ b' = b'_1\, r_2^2,\ c' = c'_1\, r_3^2,$$

where a_1', b_1', and c_1' are squarefree. Consider

$$a_1'x^2 + b_1'y^2 + c_1'z^2 = 0. \tag{5}$$

(5) has an integral solution iff (4) has one.
Now, we divide (5) by $\gcd(a_1', b_1', c_1')$, getting

$$a''x^2 + b''y^2 + c''z^2 = 0. \tag{6}$$

What remains is to make the coefficients pairwise relatively prime.
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 (6). 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 $z = g_1 z'$ and cancelling (6) by g_1, we arrive at

$$a'''x^2 + b'''y^2 + \underbrace{c''g_1}_{c'''}(z')^2 = 0. \tag{7}$$

We have $\gcd(a''', b''') = 1$ 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 arrive at

$$a(x')^2 + b(y')^2 + c(z')^2 = 0, \tag{8}$$

the so called Legendre Equation. We note : a, b, and c are nonzero, do not all have the same sign, are squarefree, and pairwise relatively prime. We will now try to find an integral solution of this diophantine equation that can then be transformed back to a rational solution of the original equation. Algorithmic formulations (in pseudocode) of the above steps (including the parabolic case) can be found in [2], where in the appendix one can also find a Maple implementation.

So far we saw that the problem of finding a rational point on an ellipse/ hyperbola reduces to the problem of finding a nontrivial integral solution of the so called Legendre Equation

$$ax^2 + by^2 + cz^2 = 0, \tag{9}$$

where a, b, and c are integers such that $abc \neq 0$. By a nontrivial integral solution we mean a solution $(\overline{x}, \overline{y}, \overline{z}) \in \mathbf{Z}^3$ with $(\overline{x}, \overline{y}, \overline{z}) \neq (0, 0, 0)$ and $\gcd(\overline{x}, \overline{y}, \overline{z}) = 1$. We also pointed out that we may assume, w. l. o. g.,

$$\begin{aligned} a &> 0,\ b < 0 \text{ and } c < 0, && (10)\\ & a,\ b, \text{ and } c \text{ are squarefree}, && (11)\\ \gcd(a, b) &= \gcd(a, c) = \gcd(b, c) = 1. && (12) \end{aligned}$$

We now deal with necessary and sufficient conditions in order that (9) has nontrivial integral solutions. Such conditions are given by the Theorem of Legendre. For a formulation of Legendre's Theorem we need the notion of quadratical residues.

Definition II.1: Let m, n be nonzero integers. Then m is a *quadratic residue* modulo n (written $m\,R\,n$) iff $\exists x \in \mathbf{Z} : x^2 \equiv_n m$ □

Now we can state the theorem.

Theorem II.3: (Legendre, Version 1) *Suppose a, b, and c satisfy (10), (11) and (12). Then (9) has a nontrivial integral solution iff*

$$-ab\,R\,c,\ -bc\,R\,a, \text{ and } -ac\,R\,b. \tag{13}$$

We prove only the necessity of (13) for this first version of the theorem and prove the sufficiency then for a second (equivalent) version.

Proof: (Legendre's Theorem, necessity of (13))
Let $(\overline{x}, \overline{y}, \overline{z})$ be a solution of (9); it follows that $\gcd(c, \overline{x}) = 1$. For if any prime p divides $\gcd(c, \overline{x})$, then p divides $b\overline{y}^2$ but p does not divide b (since $\gcd(b, c) = 1$ by (12)) and so p divides $\overline{y}$. Consequently we have p^2 divides $a\overline{x}^2 + b\overline{y}^2$ and hence p^2 divides $c\overline{z}^2$. But c is squarefree and so p divides $\overline{z}$. This contradicts the assumption $\gcd(\overline{x}, \overline{y}, \overline{z}) = 1$.

As $\gcd(c, \overline{x}) = 1$ we can find $\overline{x}'$ satisfying $\overline{x}\overline{x}' \equiv_c 1$. Also, clearly

$$a\overline{x}^2 + b\overline{y}^2 \equiv_c 0,$$

and so, by multiplying with $b(\overline{x}')^2$,

$$b^2(\overline{x}')^2\overline{y}^2 \equiv_c -ab(\overline{x}\overline{x}')^2 \equiv_c -ab.$$

Thus $-ab\, R\, c$ holds. The remaining conditions can be derived similarly. □

Theorem II.4: (Legendre, Version 2) *Let a and b be positive squarefree integers. Then*

$$ax^2 + by^2 = z^2 \tag{14}$$

has a nontrivial solution if and only if the following three conditions are satisfied.

$$a\, R\, b, \tag{15}$$

$$b\, R\, a, \tag{16}$$

$$-\frac{ab}{\gcd(a,b)^2}\, R\, \gcd(a,b). \tag{17}$$

The equivalence of these two versions is easily established (see [2]). The following constructive proof of the Legendre Equation can be found in [5], we give the presentation from [2] (where all missing details can be found).

Proof: (theorem II.4) The necessity of (15) to (17) is established by the necessity of (13) for the solvability of (9) and the claimed equivalence of the two versions of Legendres Theorem. So we show sufficiency and hence assume now that (15) to (17) hold.

Let us first of all consider two special (simple) instances of (14)

(Case a = 1) Obviously, $(\overline{x}, \overline{y}, \overline{z}) = (1, 0, 1)$ is a solution.

(Case a = b) Condition (17) requires -1 to be a square modulo b. If this is the case, we can find integers r and s such that $b = r^2 + s^2$ (consider this as an easy lemma), leading to a solution $(\overline{x}, \overline{y}, \overline{z}) = (r, s, r^2 + s^2)$.

Now we proceed to the general case. We may assume $a > b$, for if $b > a$ just interchange the roles of x and y. The strategy will be the following : We construct a new form $Ax^2 + by^2 = z^2$ satisfying the same hypotheses as (14), $0 < A < a$, and having a nontrivial solution iff (14) does so (and a solution of (14) can be computed from a solution of the new form). After a finite number of steps, interchanging A and b in case A is less than b, we arrive at one of the cases $A = 1$ or $A = b$, each of which has been settled. Now for the details.

We assume now that (15) - (17) hold. By (16) there exist integers x and k such that

$$x^2 = b + ka. \tag{18}$$

Let $k = Am^2$, where A is the squarefree part of k. Also note that we can choose x such that $|x| \leq a/2$ by choosing the absolute least residue of x modulo a ("*symmetric representation* of the integers modulo a"). Let us now restate (18) as

$$x^2 = b + Am^2 a. \tag{19}$$

First of all we show that $0 < A < a$. Since

$$0 \leq x^2 \overset{\text{by (19)}}{=} b + Am^2 a \overset{\text{since } b<a}{<} a + Am^2 a = a(1 + Am^2)$$

we have $0 < 1 + Am^2$, and hence $A \geq 0$. But if $A = 0$, then (19) gives $x^2 = b$, contradicting the fact that b is squarefree. So we established $A > 0$. On the other hand

$$Am^2 a \overset{\text{by (19) \& } b>0}{<} x^2 \overset{|x|\leq a/2}{\leq} \frac{a^2}{4,}$$

and so we have $A \leq Am^2 < a/4 (< a)$. So we consider now

$$Ax^2 + bY^2 = Z^2. \tag{20}$$

Clearly A, b are positive and squarefree integers. So we want to show

$$A\,R\,b, \tag{21}$$
$$b\,R\,A, \tag{22}$$
$$-\frac{Ab}{\gcd(A,b)^2}\,R\,\gcd(A,b). \tag{23}$$

In addition, we need that (14) has a nontrivial solution if and only if (20) has one, which will be shown constructively.

ad (21) With $g = \gcd(a,b)$, let $b_1 = b/g$, $a_1 = a/g$. We show $A\,R\,g$ and $A\,R\,b_1$. Then, we have $A\,R\,b_1 g$ (consider this as a lemma), i. e. $A\,R\,b$. First of all, note that (19) may be written as

$$x^2 = b_1 g + Am^2 a_1 g. \tag{24}$$

Since g is squarefree we have that g divides x. Setting $x_1 = \frac{x}{g}$ and cancelling gives

$$g x_1^2 = b_1 + Am^2 a_1. \tag{25}$$

Thus $Am^2 a_1 \equiv_g -b_1$, and hence

$$Am^2 a_1^2 \equiv_g -a_1 b_1. \tag{26}$$

Also note that $\gcd(m,g) = 1$, since a common factor would divide b_1 (by (25)) and hence $b = b_1 g$ would not be squarefree. But also $\gcd(a_1, g) = 1$ since $a = a_1 g$ is squarefree. Let m' and a_1' be the inverses of m respectively a_1 modulo g. By (17) (i. e. by $-a_1 b_1\,R\,g$) we may choose y such that $y^2 \equiv_g -a_1 b_1$. Now (26) becomes $A \equiv_g (m')^2 (a_1')^2 y^2$, i.e. $A\,R\,g$. So this part is done. It remains to show $A\,R\,b_1$.
By (24) we have

$$x^2 \equiv_{b_1} Am^2 a. \tag{27}$$

By (15) (i. e. by $a\,R\,b$) we have $a\,R\,b_1$. Note also that $\gcd(a, b_1) = 1$ since a common factor would divide b_1 and g, contradicting the fact that $b = b_1 g$ is squarefree. Similarly, $\gcd(m, b_1) = 1$ (use(24)). Let a^* and m^* be the inverses of a respectively m modulo b_1. Let z be such that $z^2 \equiv_{b_1} a$ and let z^* be its inverse modulo b_1. Now (27) becomes

$$A \equiv_{b_1} x^2 (m^*)^2 a^* \equiv_{b_1} x^2 (m^*)^2 (z^*)^2,$$

i. e. $A\,R\,b_1$.

ad (22) By (19), we have $b\,R\,A$ immediately.

ad (23) With $r = \gcd(A, b)$ let $A_1 = A/r$, $b_2 = b/r$. We have to show $-A_1b_2\,R\,r$.
From (19) we conclude

$$x^2 = b_2r + A_1rm^2a.$$

Since r is squarefree we have r divides x. So

$$\begin{aligned} A_1m^2a &\equiv -b_2 \pmod{r}, \text{ or} \\ -A_1b_2m^2a &\equiv b_2^2 \pmod{r}. \end{aligned} \tag{28}$$

Since $\gcd(a, r) = \gcd(m, r) = 1$, we may choose a^+ and m^+ as the inverses of a respectively m modulo r. Furthermore, from (15) (i. e. from $a\,R\,b$) we obtain $a\,R\,r$. Choose w such that $w^2 \equiv_r a$. Denote by w^+ the inverse of w modulo r. Then (28) becomes

$$-A_1b_2 \equiv_r b_2^2(m^+)^2a^+ \equiv_r b_2^2(m^+)^2(w^+)^2,$$

i. e. $-A_1b_2\,R\,r$.

So we established (21) - (23) for (20). Assume now that (20) has a nontrivial solution $(\overline{X}, \overline{Y}, \overline{Z})$. Then

$$A\overline{X}^2 = \overline{Z}^2 - b\overline{Y}^2. \tag{29}$$

Multiplying this by (19) (i. e. by $Am^2a = x^2 - b$) gives

$$\begin{aligned} a(A\overline{X}m)^2 &= (\overline{Z}^2 - b\overline{Y}^2)(x^2 - b) = \\ &= (\overline{Z}x + b\overline{Y})^2 - b(x\overline{Y} + \overline{Z})^2. \end{aligned}$$

Thus a solution of (14) is

$$\overline{x} = A\overline{X}m,\ \overline{y} = x\overline{Y} + \overline{Z},\ \overline{z} = \overline{Z}x + b\overline{Y}.$$

Written in matrix-form we have

$$\begin{bmatrix} \overline{x} \\ \overline{y} \\ \overline{z} \end{bmatrix} = \begin{bmatrix} Am & 0 & 0 \\ 0 & x & 1 \\ 0 & b & x \end{bmatrix} \cdot \begin{bmatrix} \overline{X} \\ \overline{Y} \\ \overline{Z} \end{bmatrix}.$$

The matrix is invertible since its two blocks are : the second (2×2) block has determinant $x^2 - b \neq 0$ (since b is squarefree). The solution is nontrivial since we claim that $\overline{x} = Am\overline{X} \neq 0$. Suppose $Am = 0$. Then by (19) we have $x^2 = b$, contradicting the squarefreeness of b. Suppose $\overline{X} = 0$. Then by (29) we have $\overline{Z}^2 = b\overline{Y}^2$, contradicting the squarefreeness of b. □

Algorithm for solving the Legendre Equation

The constructive proof for the existence of a nontrivial integral solution of the Legendre Equation in the previous section clearly leads to a recursive algorithm for computing such a solution. We will give a formulation in a Pascal-like pseudocode. We will here not consider an algorithmic formulation of the transformations that lead from the General Conic Equation to the Legendre Equation, see [2] for that purpose. We assume the procedure *msqrt* ("modular squareroot"), that has the following meaning : for integers a, b with $a\,R\,b$ we have

$$msqrt(a, b)^2 \equiv_b a.$$

Such a procedure exists for example in Maple™. We work in symmetric representation of the integers modulo any number. In addition, we use the knowledge that for a natural number r with

$-1\, R\, r$ there exist integers x, y such that $r = x^2 + y^2$ (for a proof of that fact and a procedure *Circle* that computes such x and y for given r see again [2]). Finally we need a procedure *sqfrp* ("*squarefree part*") for computing the squarefree part of an integer, i.e. for $n = \prod_{p\ prime} p^{n_p}$ we have

$$sqfrp(n) = \prod_{p\ prime} p^{\mathrm{mod}(n_p\,,2)}.$$

Now we can give the pseudocode.

PROC LegendreSolve($\downarrow a \downarrow b \uparrow x \uparrow y \uparrow z$)
IN :
$a,\ b \in Z$:
  positive, squarefree with $a\, R\, b$, $b\, R\, a$, $-ab/gcd(a,b)^2\, R\, gcd(a,b)$.
OUT :
$x,\ y,\ z \in Z$
  such that $ax^2 + by^2 = z^2$.
LOCAL
$r,\ s,\ T,\ A,\ B,\ X,\ Y,\ Z,\ m \in Z$
BEGIN
  if $a == 1$ **then**
    $x := 1;\ y := 0;\ z := 1$
  elseif $a == b$ **then**
    Call *Circle*($\downarrow b, \uparrow x, \uparrow y$);
    $z := x^2 + y^2$
  elseif $a > b$ **then**
    $s := msqrt(b, a)$;
    $T := (s^2 - b)/a$;
    $A := sqfrp(T);\ m := sqrt(T/A)$;
    Call *LegendreSolve*($\downarrow A, \downarrow b, \uparrow X, \uparrow Y, \uparrow Z$);
    $x := AXm;\ y := sY + Z;\ z := sZ + bY$
  else
    $s := msqrt(a, b)$;
    $T := (s^2 - a)/b$;
    $A := sqfrp(T);\ m := sqrt(T/B)$;
    Call *LegendreSolve*($\downarrow B, \downarrow a, \uparrow Y, \uparrow X, \uparrow Z$);
    $y := BYm;\ x := sX + Z;\ z := sZ + aX$
  end if
END LegendreSolve

Some words on the number of self-references in *LegendreSolve*. The worst thing that can happen is that we reduce both coefficients of

$$ax^2 + by^2 = z^2$$

to 1. The number of self-references of *LegendreSolve* needed to achieve this is bounded by $2\log_4(\max(a,b))$, since every time we reduce a coefficient, it is reduced by a factor of 4 at least. In the situation $a = b$ we call *Circle* (and no more call to *LegendreSolve* is needed), which calls himself not more than $log(a)$ times (compare [2]). So in all cases, the maximal number of any procedure calls is $O(\log(\max(a,b))$.

Example II.2: Consider the conic defined by

$$g(x, y, 1) = x^2 - 4xy - 3y^2 + 4x + 8y - 5.$$

Carrying out the above described transformations leads to the corresponding (special) Legendre Equation

$$7x^2 + 21z^2 = y^2.$$

Now we call LegendreSolve($\downarrow 7, \downarrow 21, \uparrow x, \uparrow z, \uparrow y$). Here is a trace of the corresponding values of the local variables s, T, B, m and the recursive calls of LegendreSolve :

$$(s, T, B, m) = (7, 2, 2, 1); \textbf{Call}\text{LegendreSolve}(\downarrow 2, \downarrow 7, \uparrow Y, \uparrow X, \uparrow Z);$$
$$(s, T, B, m) = (3, 1, 1, 1); \textbf{Call}\text{LegendreSolve}(\downarrow 1, \downarrow 2, \uparrow Y, \uparrow X, \uparrow Z);$$

Now the equation $Y^2+2X^2 = Z^2$ has the integral solution $(Y, X, Z) = (1, 0, 1)$. So the procedure produces the following integral solutions of the stacked equations :

$$(X, Y, Z) = (1, 1, 3),$$
$$(z, x, y) = (2, 10, 28),$$

the latter being an integral solution of $7x^2 + 21z^2 = y^2$, the (special) Legendre Equation. Inverting the above indicated transformations we arrive at a rational solution of $g(x, y, 1) = 0$:

$$(x, y) = (-\frac{3}{7}, \frac{16}{7}).$$

$\square$

Real points on conics[1]

Let us assume that no rational point lies on the conic. In this case we ask whether there is at least a real point on the conic, i. e. whether there exists $(\overline{x}, \overline{y}) \in \mathbf{R}^2$ such that

$$g(\overline{x}, \overline{y}, 1) = 0.$$

Since we saw already that every parabola contains a rational point, we only have to consider the elliptic/hyperbolic case. We know already how to transform the General Conic Equation to an equation of the form

$$x^2 + Ky^2 = L, \tag{30}$$

where K, L are rational numbers. A real point on the conic exists if and only if $\neg(K > 0 \wedge L < 0)$. In this case, a real solution of (30) is given by

$$\begin{aligned} (\overline{x}, \overline{y}) &= (\sqrt{L}, 0) \quad \text{if} \quad L > 0, \\ (\overline{x}, \overline{y}) &= (0, \sqrt{\frac{L}{K}}) \quad \text{if} \quad L < 0. \end{aligned}$$

By back transformation, we arrive at a real solution for the General Conic Equation.

[1]The question when a rational algebraic plane curve over $\mathbf{Q}$ is parametrizable over $\mathbf{R}$ is treated in section 3.3 ("Parametrizing over the reals") of [13]. We state here the main result.
Theorem 3.2 (in [13]) *A rational algebraic plane curve over $\mathbf{Q}$ is parametrizable over $\mathbf{R}$ if and only if it is not birationally equivalent over $\mathbf{R}$ to the conic $x^2 + y^2 + z^2$.*

III. Points on conics over the rational function field

As pointed out above, we only have to consider the reduced equation

$$X^2 + K(t)Y^2 = L(t), \tag{31}$$

where K, $L \in \mathbf{Q}(t)$. Our goal is to find rational functions $X(t)$, $Y(t)$ satisfying (31). This solves the problem of finding rational functions satisfying the general conic equation with coefficients in $\mathbf{Q}(t)$ completely (compare the rational case). For solving (31), we try to exploit the method used for the rational case. In order to point out the analogy between these cases, we note that $\mathbf{Q}(t)$ is the quotient field of $\mathbf{Q}[t]$, a *Euclidean Domain* (ED for short), like $\mathbf{Q}$ is the quotient field of $\mathbf{Z}$ (*the* standard example of an ED). This means that we can make use of modular arithmetic, as we did in the rational case. Also those details of the rational case depending on factorization can be adapted, since every ED is a *Unique Factorization Domain* (UFD). So we can do all transformations that we did in the rational case and finally arrive at an equation of the form

$$a(t)x^2 + b(t)y^2 = z^2, \tag{32}$$

where a and b are nonzero and squarefree polynomials satisfying (at least if there exists a rational solution)

$$a \, R \, b, \tag{33}$$

$$b \, R \, a, \tag{34}$$

$$-\frac{ab}{\gcd(a,b)^2} \, R \, \gcd(a,b). \tag{35}$$

(The notion of quadratic residue for polynomials is analogous to the one for integers). W. l. o. g. let us assume $\deg(a) \geq \deg(b)$. From the proof of Legendre's Theorem for the rational case we know that in the new coordinates

$$\begin{aligned} x &= AXm, \\ y &= sY + Z, \\ z &= sZ + bY, \end{aligned}$$

where[2]

$$\begin{aligned} s(t) &= pmsqrt(b(t), a(t)), \\ k(t) &= \frac{s(t)^2 - b(t)}{a(t)}, \\ A(t) &= sqfrp(k(t)), \\ m(t) &= \sqrt{\frac{k(t)}{A(t)}}, \end{aligned}$$

(32) has the form

$$AX^2 + bY^2 = Z^2.$$

In analogy to the rational case A is smaller than a in some sense : in the rational case it was the absolute value of a that dropped; here it is the degree of the polynomial $a(t)$ that drops. The

[2] *pmsqrt* : "polynomial modular squareroot", i. e.

$$pmsqrt(b(t), a(t))^2 = b(t) \bmod a(t).$$

point now is that by iterated application of the above transformation (as in the rational case) we arrive at some simple instances of the (polynomial) Legendre Equation, where we can decide the existence of a rational (function) solution and - if one exists - give a solution. Technical details and algorithmic formulations can again be found in [2].

The problem treated in this chapter arises in the context of parametrizing surfaces over $\mathbf{Q}$. In particular, the following two problems are closely related :

1. Parametrize a conic $f(x,y) = 0$ (where $f \in \mathbf{Q}(t)[x,y]$) with rational functions in s and coefficients in $\mathbf{Q}(t)$.
2. Parametrize a surface $F(x,y,t) = 0$ (where $F \in \mathbf{Q}[x,y,t]$ is of total degree 2 in x and y) with rational functions in s and t.

The exact relationship and the application of our results to the parametrization of such surfaces needs to be investigated further.

Conclusion

Given an algebraic curve defined over the rational number field, we can decide whether the curve has genus 0 and infinitely many points over the rational numbers and therefore can be parametrized over the rationals. Similarly we can decide whether a real curve can be parametrized over the reals. We are able to extend these decision methods from $\mathbf{Q}$ to $\mathbf{Q}(t)$, the field of rational functions over $\mathbf{Q}$. We conjecture that this extension should lead to parametrization algorithms for certain surfaces of interest in computer-aided-geometric-design, such as discussed in [10]. This needs further investigation.

References

[1] D. Hilbert, A. Hurwitz, "Über die Diophantischen Gleichungen vom Geschlecht Null", *Acta math.* **14**, 217–224 (1890)

[2] E. Hillgarter, *Rational Points on Conics*, Diploma Thesis, RISC-Linz, J. Kepler Universität Linz, Austria (1996)

[3] J. Hoschek, D. Lasser, *Fundamentals of Computer Aided Geometric Design*, A.K. Peters, Wellesley MA (1993)

[4] M. van Hoeij, "Rational Parametrization of Algebraic Curves using a Canonical Divisor", *J. Symbolic Comp.* **March/April** (1996)

[5] K. Ireland, M. Rosen, "A classical introduction to modern number theory", Springer Verlag, 1982.

[6] E. Krätzel, "Zahlentheorie", VEB Dt. Verlag der Wissenschaften, 1981.

[7] M. Mňuk, *Algebraic and Geometric Approach to Parametrization of Rational Curves*, Ph.D. Dissertation, RISC-Linz, J. Kepler Universität Linz, Austria (1995)

[8] M. Mňuk, J.R. Sendra, F. Winkler, "On the Complexity of Parametrizing Curves", *Beiträge zur Algebra und Geometrie* **37/2**, 309–328 (1996)

[9] G.M. Nielson, “Cagd’s Top Ten: What to Watch”, *IEEE Computer Graphics & Applications* (Jan. 1993)

[10] M. Peternell, H. Pottmann, “Computing Rational Parametrizations of Canal Surfaces”, *J. Symbolic Comp.* **March/April** (1996)

[11] H. E. Rose, ”A Course in Number Theory”, Oxford Science Publications, 1988.

[12] J.R. Sendra, F. Winkler, “Symbolic Parametrization of Curves”, *J. Symbolic Comp.* **12**, 607–631 (1991)

[13] J.R. Sendra, F. Winkler, “Parametrization of Algebraic Curves over Optimal Field Extensions”, *J. Symbolic Comp.* **March/April** (1996)

[14] R.J. Walker, *Algebraic Curves*, Princeton University Press (1950)