On computing integral points of a Mordell curve over rational function fields in characteristic > 3

Claus Fieker *
Fachbereich Mathematik, Universität Kaiserslautern
Postfach 3049, D-67653 Kaiserslautern, Germany
email: fieker@mathematik.uni-kl.de

István Gaál †
University of Debrecen, Mathematical Institute
H–4010 Debrecen Pf.12., Hungary
e–mail: igaal@science.unideb.hu

and Michael Pohst ‡
Technische Universtät Berlin, Institut für Mathematik
Straße des 17. Juni 136, 10623 Berlin, Germany
e-mail: pohst@math.tu-berlin.de

July 25, 2012

*The research was carried out while the author was working for the Magma group at the University of Sydney

†Research supported in part by K75566 and K100339 from the Hungarian National Foundation for Scientific Research and by the TAMOP 4.2.1./B-09/1/KONV-2010-0007 project implemented through the New Hungary Development Plan co-financed by the European Social Fund, and the European Regional Development Fund

‡Research supported in part by the Deutsche Forschungsgemeinschaft (Project 436 UNG 113/203/0-1)

Abstract

We develop an efficient algorithm to solve Mordell's equation over global function fields. Our method involves ideas from algebraic number theory, especially class field theory. For explicit calculations we used Magma and KASH. Contrary to the number field case the number of solutions can be infinite.

1 Introduction

Mordell's equation

$$Y^2 = X^3 + k$$

is one of the most classical diophantine equations. For special integers k the book [10] already contains investigations to find all integer solutions X, Y. Later this equation became important in connection with elliptic curves. A.Pethő, J.Gebel and H.G.Zimmer [11] solved this equation explicitly for $0 < |k| < 10^5$ by computing generators for the Mordell Weil group. Their methods failed, however, for 1182 curves. Using an idea of Mordell outlined below, K.Wildanger [15] reproduced their results and also solved those 1182 equations. By methods from the geometry of numbers he could compute solutions for $|k|$ up to several million. His methods were improved and extended by A. Jätzschmann in his diploma thesis [9] in which he calculated integral solutions for $|k|$ up to 10^9. With the new ideas from class field theory presented in this paper we are convinced that we can still extend that range considerably. This will be done in a forthcoming paper by the authors.

Recently we transfered the study of Thue equations, norm form equations and other decomposable form equations to the case of global function fields (see [5], [6], [7], for example). In this paper we investigate Mordell's equation over global function fields for the first time. Our methods involve ideas from algebraic number theory, especially class field theory. We illustrate our algorithm with several detailed examples. We used Magma [2] and KASH [3] for explicit calculations in function fields.

2010 *Mathematics Subject Classification*: Primary 11Y50; Secondary 11D25,11D61, 11G05

Key words and phrases: Mordell's equation; global function fields

A similar problem was considered by M.Schütt and A.Schweizer in [14]. Let $q = p^\ell$ be a prime power, denote by $\mathbb{F}_q$ the finite field with q elements and let $0 \neq \kappa \in \mathbb{F}_q[t]$. Let $X, Y \in \mathbb{F}_q[t]$ be an arbitrary solution of $Y^2 = X^3 + \kappa$ with $\deg X = 2M, \deg Y = 3M$. The authors call the inequality $\deg \kappa \geq M + 1$ a Davenport-Stothers inequality DS(M) mod p. If DS(M) mod p holds then all solutions X, Y satisfy

$$\deg X \leq 2(\deg \kappa - 1), \quad \deg Y \leq 3(\deg \kappa - 1).$$

The authors show that there exist counterexamples to DS(M) mod p with infinitely many solutions $X, Y \in \mathbb{F}_q[t]$. Also, if κ is a counterexample to DS(M) mod p, then every prime divisor π of κ has multiplicity at least 2.

We note that if DS(M) mod p holds and q is small the upper bounds for the degrees of the solutions X, Y can be used to calculate all of them by enumeration. Of course, this does not work for larger q, e.g. in our last example of Section 4.

Acknowledgement The autors are grateful to the referee for pointing out to us the paper on Davenport-Stothers inequalities [14]. Her/his careful reading of our manuscript helped to eliminate several flaws.

2 Mordell's equation over function fields

Let $\mathbb{F}_q$ be a finite field with $q = p^\ell$ elements, p a prime bigger than 3. We let $\mathbb{F}_q^\times = \langle \zeta \rangle$. By F we denote the rational function field $\mathbb{F}_q(t)$ and by R its maximal order $\mathbb{F}_q[t]$. For given $\kappa \in R$ we consider Mordell's equation

$$Y^2 \;=\; X^3 \,+\, \kappa \;. \tag{1}$$

In this paper we develop a method for computing all solutions $(X, Y) \in R^2$ of that equation. As we shall see in Example 1 of Section 4, Mordell's equation can have infinitely many solutions over function fields.

We make use of Mordell's observation that the discriminant of the cubic polynomial $Z^3 - 3xZ - 2y$ in the variable Z is $\Delta := -108\kappa$. (This is the reason why we must stipulate that the characteristic of $\mathbb{F}_q$ is bigger than 3.) It therefore suffices to determine all monic cubic polynomials

$$g(Z) = Z^3 + aZ^2 + bZ + c \in R[Z] \tag{2}$$

of discriminant Δ. Since the discriminants of $g(Z+\delta)$ for $\delta \in R$, of $-g(-Z)$ and of $g(Z)$ coincide we need to search only for one representative in each corresponding equivalence class.

Hence, we need to solve a so-called discriminant form equation which is a difficult task. For irreducible polynomials all known methods at first determine potential field extensions and then solve index form equations in them. In the number field case, K. Wildanger [15] and A. Jätzschmann [9] used methods from the geometry of numbers for the generation of the candidates for the cubic fields which were developed by the third author earlier. In principal, it would be possible to transfer those methods also to the function field case. But they only yield bounds for the degrees of the (polynomial) coefficients of generating polynomials. Hence, the number of candidates to be tested becomes intractable for larger fields of constants. Therefore we rather apply methods from class field theory which go back to Hasse [8] and were recently transfered to function fields by the third author in [12]. They also have the advantage that we can relatively easy decide whether cubic extensions of prescribed discriminant exist at all.

3 Solving Mordell's equation

In this section we present an algorithm for determining all solutions of Mordell's equation (1). At first we treat the case of reducible $g(Z)$ for which the procedure is much simpler. For irreducible $g(Z)$ we need to distinguish Galois and non-Galois extensions.

3.1 Case I: $g(Z)$ is reducible

Then $g(Z)$ has a linear factor and therefore in the equivalence class of $g(Z)$ there exists a polynomial $h(Z) = Z^3 + AZ^2 + BZ$ of discriminant $d(h) = B^2(A^2 - 4B)$. This yields finitely many candidates for B. For each potential B we then need to check whether $\tau := -108\kappa B^{-2} + 4B$ is a square A^2 in R. We note that replacing B by $B\xi$ for $\xi \in \mathbb{F}_q^\times$ requires to check $\tau_\xi = -108\kappa B^{-2} + 4\xi^3 B$. This reduces the required amount of tests by a factor $1/3$. For any solution (A, B) we then transform $Z^3 + AZ^2 + BZ$ by a Tschirnhaus transformation into a polynomial $Z^3 + CZ + D$ and get a solution $x = -C/3$, $y = -D/2$ of (1).

We remark, however, that we do not know how to solve that task over field extensions with infinite unit groups.

3.2 Case II: $g(Z)$ is irreducible.

We let ρ be a zero of $g(Z)$ in $\bar{F}$. The extension $E = F(\rho)$ is of degree 3 over F. We denote by Λ the equation order $R[\rho]$ and by o_E the maximal order of E, i.e. the integral closure of R in E, and by d_E its discriminant. All known methods for solving discriminant form equations require the detour via generating the corresponding field E. We are looking for equation orders of discriminant $\Delta = -108\kappa$. We know that

$$\Delta \ = \ I^2 d_E \ . \tag{3}$$

Again, the square of the index I divides Δ so that we obtain finitely many candidates for (I, d_E). For these we need to generate the corresponding fields E of discriminant $d = d_E$.

Our approach via Kummer, respectively class field theory requires to consider Galois and non-Galois cubic extensions separately. (This distinction is unnecessary if we use methods from the geometry of numbers instead.) Clearly, Galois extensions are easier and therefore treated first.

3.2.1 Cyclic cubic extensions E of F of prescribed discriminant d

For those extensions their discriminant is necessarily a square. If Δ itself is not a square this case cannot occur.

In order to apply Kummer theory we would like the constant field to contain a primitive third root of unity. This is satisfied in case $q \equiv 1 \bmod 3$. For $q \equiv 2 \bmod 3$ we take the quadratic extension $\mathbb{F}_{q^2}$ of the constant field, and carry out the subsequent program. Eventually, we need to step down from cubic extensions defined over $\mathbb{F}_{q^2}(t)$ to the corresponding extensions over $\mathbb{F}_q(t)$ if they exist. We remark on this at the end of this subsection. In the remainder of this subsection we can therefore assume that the field of constants $\mathbb{F}$ contains a primitive third root of unity, also implying that -3 is a square in $\mathbb{F}$. Then we are looking for cubic Galois extensions E of $\mathbb{F}(t)$. They are of the form $E = F(\sqrt[3]{\mu})$ for suitable elements μ of the maximal order $R = \mathbb{F}[t]$. The calculation of all candidates for μ is described next.

We are looking for pure cubic extensions $E = F(\rho)$, ρ a root of an irreducible polynomial $f(Z) = Z^3 - \mu \in R[Z]$. (It is easily seen that f is irreducible if we choose $\mu \in \mathbb{F}[t]$ cube-free of positive degree.)

The discriminant $d(f)$ of the polynomial f (with respect to the variable Z) is $-27\mu^2$. We write $\mu = hk^2$ with h square-free and $\gcd(h,k) = 1$. The equation order $S := R[\rho]$ for $R = \mathbb{F}[t]$ can be non-maximal only for those primes $\pi \in R$ which divide μ.

Applying the Dedekind test [13] for such primes π we easily see that S is π-maximal precisely for $\pi|h$. For $\pi|k$, however, we obtain an overorder $S_\pi = R + R\rho + R\rho^2/\pi$ in E. Computing the π-radical of S_π and the corresponding ring of multipliers we find that S_π is already π-maximal. Hence, we have demonstrated the following theorem.

Theorem 1. *An R-basis of the maximal order o_E of E is given by $\omega_1 = 1$, $\omega_2 = \rho$, $\omega_3 = \rho^2/k$.*

The discriminant d_E of E becomes

$$d_E = \det(\mathrm{Tr}(\omega_i\omega_j)) = \begin{vmatrix} 3 & 0 & 0 \\ 0 & 0 & 3\mu/k \\ 0 & 3\mu/k & 0 \end{vmatrix} = -27\mu^2/k^2 = -27h^2k^2 \ .$$

Therefore we obtain all candidates for E from the finitely many solutions $(h,k) \in R^2$ for which

$$\frac{-108\kappa}{-27h^2k^2}$$

is a square.

Remarks
(i) The number of non-isomorphic extensions of the same discriminant is easily seen to be 2^r where r denotes the number of different primes dividing hk. (We note that μ and $\zeta\mu$ (for $\mathbb{F}^\times = \langle\zeta\rangle$) generate non-isomorphic fields of the same discriminant.)
(ii) A similar integral basis for E is also given by Wu in [16]. His proof differs from our's substantially.

Let us assume that we have computed all candidates for E. In case E has constant field $\mathbb{F}_{q^2}$ and we are looking for a corresponding cubic extension with constant field $\mathbb{F}_q$ we still need to determine whether the fixed field of the map $x \mapsto x^q$ yields an appropriate candidate. For the remaining fields we must still solve an index form equation in o_E for I from formula (3) .

3.2.2 Non-Galois cubic extensions

In the general case, when $g(Z)$ is irreducible and the extension E/F is not Galois, we proceed as follows.

For all possible D for which

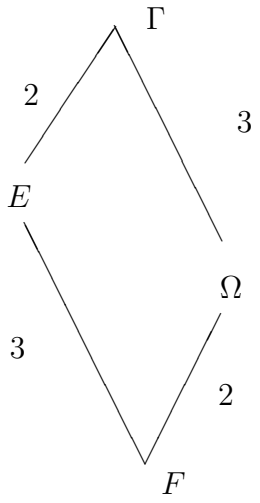
$$\frac{\Delta}{D} = i^2 \tag{4}$$

is a full square we write D in the form

$$D = d \cdot f^2 \tag{5}$$

where the square free d is the discriminant of a quadratic field $\Omega = F(\sqrt{d})$.

The composite of E and Ω is a non-abelian Galois extension Γ of degree 6 over F. In [12] the third author describes an algorithm for determining Γ and all its cubic subfields E of discriminant D following ideas of Hasse [8] in the number field case. Major ingredients are the relations between the arithmetical invariants of the fields E, Ω, Γ by means of class field theory. We just sketch the most important facts.



According to Pohst [12] we call the discriminant d of Ω and the ideal group H of index 3 in the ray class group $Cl_{\mathbf{f}}$ of Ω of conductor $\mathbf{f}$ the invariants of the cubic field E. We denote the non-trivial automorphism of Ω (which maps $\sqrt{d}$ to $-\sqrt{d}$) by τ. Then all calculations are based on the following lemmas and remarks from [12].

Lemma 2. *For $d, H, \mathbf{f}, \Omega, \tau$ as above the following statements are equivalent:*

1. *d, H are the invariants of a cubic field E.*
2. *$\tau(H) = H$ and for $H \neq \tilde{H} \in Cl_{\mathbf{f}}/H$ we have $\tau(\tilde{H}) = \tilde{H}^{-1}$.*
3. *H contains all elements of F which are coprime to $\mathbf{f}$.*

Lemma 3. *The discriminants Δ, d and the conductor $\mathbf{f}$ satisfy*

$$\Delta \;=\; dN_{\Omega/F}(\mathbf{f}) \;=\; df^2 \quad \textit{and} \quad \mathbf{f} = fo_\Omega \;.$$

Lemma 4. *The generating element f of the conductor $\mathbf{f}$ is a product of distinct primes π of o_F. For $q \equiv 1 \bmod 3$ all prime divisors π of f must be decomposed in Ω. For $q \equiv 2 \bmod 3$ only those primes π can divide f which are either decomposed with $\deg(\pi)$ even or inert with $\deg(\pi)$ odd.*

Further, Pohst [12] gives an algorithm for determining the number $N(\Delta)$ of cubic subfields of Γ by using invariants of Ω only. It is remarkable that in certain cases it is easy to predict the non-existence of cubic fields E.

Remark There are two special cases with $N(\Delta) = 0$:
(i) f contains a prime divisor which is not of the form prescribed by Lemma 4.
(ii) f equals 1 and the class number of Ω is not divisible by 3.

We note that the computation of $N(\Delta)$ essentially requires the computation of the (3–part) of the class group of Ω. Only in the case $N(\Delta) > 0$ we proceed as follows.

We calculate the ray class group of Ω of conductor $\mathbf{f}$. Then we determine all subgroups of index 3 and the corresponding class fields Γ. We check whether Γ has the correct conductor and a non-abelian Galois group. Finally, we compute the cubic subfields E of Γ. All these tasks can be carried out easily with Magma.

For each of the computed cubic extensions E we then need to calculate solutions of the index form equation corresponding to (4). We note that calculating elements of given index in a cubic field just requires to solve cubic Thue equations. For solving index form equations and Thue equations in general we refer to [4], and for the function field case to [5], [6]. The solutions of the index form equations provide all elements whose minimal polynomials have the correct discriminant.

4 Examples

In the last section we illustrate our procedure by several examples. We remark that for $\kappa \in \mathbb{F}_q$ all solutions X, Y of (1) also belong to $\mathbb{F}_q$ by Lüroth's theorem. If κ is a constant times a sixth power in $\mathbb{F}_q[t]$ the solutions of (1) are easily reduced to the case $\kappa \in \mathbb{F}_q^\times$.

4.1 Example 1

We consider the equation

$$Y^2 \;=\; X^3 \,+\, (t^2+3t-1)^2 \;. \tag{6}$$

over $F = \mathbb{F}_{25}(t)$. We denote by ζ a fixed generator of the cyclic multiplicative group $\mathbb{F}_{25}^*$ satisfying $\zeta^2 = \zeta + 3$. We note that (X, Y) is a solution of (6) if and only if $(X_0, Y_0) = (X/\zeta^2, Y/\zeta^3)$ is a solution of

$$Y_0^2 \;=\; X_0^3 \,+\, 3(t^2+3t-1)^2 \;. \tag{7}$$

This requires to find cubic polynomials of discriminant

$$-108 \cdot 3 \cdot (t^2+3t-1)^2 = (t^2+3t-1)^2.$$

A root of this polynomial generates a cyclic cubic extension E of F, see Section 3.2.1. This field must be of the form $E = F(\sqrt[3]{\mu})$. The irreducible factorization of t^2+3t-1 over $\mathbb{F}_{25}[t]$ is

$$t^2+3t-1 = (t-\zeta^2)(t-\zeta^{10}),$$

hence by the arguments of Section 3.2.1 there are four possible values of μ:

$$\mu_1 = t^2+3t-1, \;\; \mu_2 = \zeta\mu_1, \;\; \mu_3 = (t-\zeta^{10})\mu_1, \;\; \mu_4 = \zeta\mu_3.$$

In order to show that equation (6) has infinitely many solutions, it suffices to consider $\mu = \mu_3$. The other values of μ will not be discussed.

We observe that $E = F(\sqrt[3]{\mu})$ is the same field as $F(\alpha)$ where α is a root of the polynomial $f(y) = y^3 - ty^2 - (t+3)y - 1$. Indeed the roots of f can be represented in the integral basis

$$(1, \sqrt[3]{\mu}, \frac{(\sqrt[3]{\mu})^2}{t-\zeta^{10}})$$

of E with the coordinates

$$(2t, -\zeta^{10}, -\zeta^2), (2t, -\zeta^2, -\zeta^{10}), (2t, 2, 2).$$

Therefore in the following it is easier to work with E as $E = F(\alpha)$ with integral basis $(1, \alpha, \alpha^2)$. The three roots of the polynomial f are

$$\alpha = \alpha_1, \alpha_2 = \frac{-1}{1+\alpha_1}, \alpha_3 = \frac{-1}{1+\alpha_2}.$$

Because of $d_E = d(\alpha) = (t^2+3t-1)^2$, determining integers of E of discriminant $(t^2+3t-1)^2$ requires the calculation of integers of index 1 in E. Hence, we have to calculate $x, y \in \mathbb{F}_{25}[t]$ such that $\vartheta = x\alpha + y\alpha^2$ has index 1 in E. We set $\vartheta_i = x\alpha_i + y\alpha_i^2$ $(i = 1, 2, 3)$. By standard arguments we have

$$1 = I(\vartheta) = \frac{1}{\sqrt{d_E}} \prod_{1\le i<j\le 3} (\vartheta_i - \vartheta_j) = \prod_{1\le i<j\le 3} \frac{\vartheta_i - \vartheta_j}{\alpha_i - \alpha_j}$$

$$= \prod_{1\le i<j\le 3} \frac{(x\alpha_i + y\alpha_i^2) - (x\alpha_j + y\alpha_j^2)}{\alpha_i - \alpha_j} = \prod_{1\le i<j\le 3} (x + (\alpha_i + \alpha_j)y)$$

$$= \prod_{1\le k\le 3} (x + (t - \alpha_k)y) = \prod_{1\le k\le 3} (x_0 - \alpha_k y_0)$$

with $x_0 = x + ty, y_0 = y$.

The Thue equation

$$\prod_{1\le k\le 3} (x_0 - \alpha_k y_0) = 1 \tag{8}$$

was already considered in [6] (over $\mathbb{F}_5$ instead of $\mathbb{F}_{25}$ but we shall have the same phenomenon also over $\mathbb{F}_{25}$). Setting $\beta_i = x_0 - \alpha_k y_0$ Siegel's identity can be written as

$$(\alpha_1 - \alpha_2)\beta_3 + (\alpha_2 - \alpha_3)\beta_1 + (\alpha_3 - \alpha_1)\beta_2 = 0$$

from which we obtain the unit equation

$$\varepsilon + \eta = 1 \tag{9}$$

with the unknown units

$$\varepsilon = \frac{(\alpha_2 - \alpha_3)\beta_1}{(\alpha_2 - \alpha_1)\beta_3}$$

and

$$\eta = \frac{(\alpha_3 - \alpha_1)\beta_2}{(\alpha_2 - \alpha_1)\beta_3}$$

in E. (We note that by equation (8) the β_i as well as the cross ratios of the conjugates of α are units in E.) In E there are three infinite valuations, all of degree 1. Using the fundamental Lemma 2.2 of [6] we obtain that all solutions of (9) are either of height ≤ 1, or are 5^m-th powers of such solutions. Enumerating all possible elements of heights ≤ 1 we obtain constant solutions (ε, η) of (9), and on the other hand the solutions

$$(\varepsilon, \eta) = (4\alpha_1\alpha_2, 4\alpha_2), \left(\frac{4}{\alpha_1}, \frac{4}{\alpha_1\alpha_2}\right), \left(4\alpha_1, \frac{4}{\alpha_2}\right) \quad , \tag{10}$$

and three more solutions by interchanging the roles of ε and η.

We recall from [6] that if (ε, η) is a solution of (9), then the β_i satisfy

$$\frac{\beta_1}{\beta_3} = \frac{\alpha_2 - \alpha_1}{\alpha_2 - \alpha_3}\varepsilon$$

and

$$\frac{\beta_2}{\beta_3} = \frac{\alpha_2 - \alpha_1}{\alpha_3 - \alpha_1}\eta..$$

By equation (8) we then have

$$\beta_3^3 \frac{\beta_1}{\beta_3}\frac{\beta_2}{\beta_3} = 1,$$

hence,

$$\beta_3^3 \frac{(\alpha_2 - \alpha_1)^2}{(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)}\varepsilon\eta = 1,$$

and

$$\beta_3^3 = \frac{1}{\varepsilon\eta}\frac{(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)}{(\alpha_2 - \alpha_1)^2} = \frac{1}{\varepsilon\eta}\frac{1}{\alpha_1^2\alpha_2}.$$

Similarly as in [6], for $(\varepsilon, \eta) = (4\alpha_1\alpha_2, 4\alpha_2), (4/\alpha_1, 4/(\alpha_1\alpha_2)), (4/\alpha_2, 4\alpha_1)$ the solutions $(\varepsilon^{5^m}, \eta^{5^m})$ give rise to infinite families of solutions of the Thue equation (8). Therefore we get infinitely many integers $\vartheta = x\alpha + y\alpha^2$ of index 1 in E, infinitely many solutions (X_0, Y_0) of (7) as well as infinitely many solutions (X, Y) of the original Mordell equation (6).

To show that the number of solutions of the Mordell equation is indeed infinite (i.e. the solutions of the Mordell equation deduced from the infinitely many solutions of the Thue equation are indeed distinct) we take for example the solution $(\varepsilon, \eta) = (4\alpha_1\alpha_2, 4\alpha_2)$ of the unit equation. We set

$$A = \alpha_1^{(-5^{2m}+1)/3}, \quad B = \alpha_2^{(5^{2m}+2)/3}.$$

According to [6] the solutions of the Thue equation (8) are

$$x_0 = \frac{1}{\alpha_1 - \alpha_2}\left(\alpha_1 AB - \frac{\alpha_1 B}{A^2}\right), \quad y_0 = \frac{1}{\alpha_1 - \alpha_2}\left(AB - \frac{\alpha_1 B}{\alpha_2 A^2}\right).$$

From (x_0, y_0) we get the solutions $(x, y) = (x_0 - ty_0, y_0)$ of the index form equation $I(\vartheta) = 1$. Using symmetric polynomials we can easily calculate the minimal polynomial of $\vartheta = x\alpha_1 + y\alpha_1^2$ and the quadratic term can be eliminated from it. In this way we obtain a trinomial y^3+Uy+V which has a root $\vartheta+w$ for a suitable additive constant $w \in \mathbb{F}_{25}[t]$. Then $X = 3U$, $Y = 2V$ is a solution of the Mordell equation.

We want to show that we obtain infinitely many different trinomials y^3+Uy+V. It is easily seen that we obtain infinitely many elements ϑ. Namely, E has three infinite valuations which can be computed with KASH [3]. We choose v satisfying $v(\alpha_1) = -1$. A straightforward calculation yields $v(y_0) = (-5^{2m} + 1)/3$. As a consequence, we get infinitely many minimal polynomials for the elements ϑ. When we apply the Tschirnhaus transformation $\vartheta \to \vartheta + w$ from above we could get the same trinomial for, say $\vartheta_1 \neq \vartheta_2$. But then the elements ϑ_1, ϑ_2 can only differ by an additive constant from $\mathbb{F}_{25}[t]$. The presentation $\vartheta = x\alpha_1 + y\alpha_1^2$ from above shows that this cannot be the case. (We recall that $y = y_0$.) Hence, we indeed obtain infinitely many solutions of the Mordell equation.

Remark 1 The valuation theoretical considerations above also provide a relation between the size (degree) of the solutions of the unit equation and the solutions of the Mordell equation. Hence, the bounds for the latter at the end of the introduction can be used to establish bounds for the degrees of the solutions of the unit equation. Contrary to the number field case, at present there is no direct method known how to calculate small solutions of a unit equation in the function field case. (In the number field case this can be done by continued fraction expansions.) The method of [6] allows to calculate solutions of the unit equation which are not p-th powers. Hence,

the bounds of the introduction can certainly be used to fasten the calculation of potential p-th powers. For example, these bounds will often apply in the non-Galois case when κ is not a square.

Remark 2 We note that we can replace the generating polynomial $f(y) = y^3 - ty^2 - (t+3)y - 1$ by $f(y) = y^3 - h(t)y^2 - (h(t)+3)y - 1$ with suitable square-free polynomials $h(t)$ of F. Then the same considerations as above yield an infinite family of elliptic curves which have infinitely many integral points.

4.2 Example 2

We consider the equation

$$Y^2 \;=\; X^3 \,+\, t^2(1-t) \;. \tag{11}$$

over $F = \mathbb{F}_7(t)$. Then our task is to compute cubic polynomials of discriminant

$$\Delta = -108t^2(1-t) = 3t^2(t-1).$$

Using the procedure described in Section 3.2.2 we find that there is only one cubic field with discriminant dividing Δ, namely the one generated by the root ρ of the polynomial

$$f(y) = y^3 + 6ty^2 + 2ty + 5t^2 + 2t.$$

over F. The function field $E = F(\rho)$ has integral basis $\{1, \rho, (4 + 5\rho + \rho^2)/(t+2)\}$ and discriminant $d_E = 6t^2(t-1)$. According to (3) we have to find integral elements of index 1 in this field.

We denote by ρ_1, ρ_2, ρ_3 the conjugates of ρ. The index of any element $\alpha = a + x\rho + y(4 + 5\rho + \rho^2)/(t+2)$ (with $a, x, y \in \mathbb{F}_7[t]$) can be written as

$$I(x,y) = \frac{1}{\sqrt{d_E}} \prod_{1\le i<j\le 3} \left[(\rho_i - \rho_j)x + \frac{5(\rho_i - \rho_j) + (\rho_i^2 - \rho_j^2)}{t+2} y\right]$$

$$= (t+2) \cdot \prod_{1\le i<j\le 3} \left[x + \frac{5 + \rho_i + \rho_j}{t+2} y\right] = (t+2) \cdot \prod_{k=1}^{3} \left[x + \frac{5 - 6t - \rho_k}{t+2} y\right]$$

Using symmetric polynomials it is easily shown that

$$I(x,y) = (t+2)x^3 + 2(t+4)x^2y + (t+6)xy^2 + 5y^3.$$

For our task, to find elements of index 1 we rather write $I(x,y) = c$ ($c \in \mathbb{F}_7^\times$) in the form

$$\prod_{k=1}^{3} ((t+2)x + (5-6t-\rho_k)y) = c \cdot (t+2)^2,$$

that is

$$\prod_{k=1}^{3} (z - \rho_k y) = c \cdot (t+2)^2$$

with $z = (t+2)x + (5-6t)y$.

This Thue equation can be solved using the method of [5]. In the field E the fundamental unit is

$$\eta = 1 + 4 \cdot \frac{4 + 5\rho + \rho^2}{t+2},$$

and up to unit factors there are two elements of norm $(t+2)^2$, namely

$$(3t+4) + 5\rho + 6 \cdot \frac{4 + 5\rho + \rho^2}{t+2}, \quad 1 + 2\rho. \tag{12}$$

This yields that $\beta = z - \rho y$ can be written in the form

$$\beta = c \cdot \mu \cdot \eta^\ell \,,$$

where $c \in \mathbb{F}_7^\times$, μ is one of the elements in (12) and $\ell \in \mathbb{Z}$. Using Siegel's identity (denoting the conjugates of any $\gamma \in E$ by $\gamma_1, \gamma_2, \gamma_3$) we obtain

$$c_1 \cdot \frac{(\rho_1 - \rho_2)\mu_3\eta_3^\ell}{(\rho_1 - \rho_3)\mu_2\eta_2^\ell} + c_2 \cdot \frac{(\rho_2 - \rho_3)\mu_1\eta_1^\ell}{(\rho_1 - \rho_3)\mu_2\eta_2^\ell} = 1, \tag{13}$$

with suitable $c_1, c_2 \in \mathbb{F}_7^\times$. This is a unit equation in two variables. 7-th powers can be excluded by considering finite valuations ocurring in the cross ratios of ρ. Hence the bound for the heights of the solutions of this unit equation gives directly a bound for $|\ell|$.

We note that according to [5] all elements should be represented in a sextic field containing all conjugates of ρ. This function field is generated by a root of

$$y^6 + (5t + 5t^2)y^4 + (t^4 + 2t^3 + t^2)y^2 + (t^5 + 3t^4 + 3t^2)$$

over F.

Using the fundamental lemma of [5] we get bounds for the heights of the solutions of the unit equation above. (13) yields

$$|\ell| \cdot H\left(\frac{\eta_3}{\eta_1}\right) \leq H\left(\frac{(\rho_1-\rho_2)\mu_3}{(\rho_1-\rho_3)\mu_2}\right) + H\left(\frac{(\rho_1-\rho_3)\mu_2}{(\rho_1-\rho_2)\mu_3}\right).$$

The first term on the right-hand side is bounded by the fundamental lemma, the other terms can be calculated easily. We obtain

$$|\ell| < 5\ .$$

Finally, we have to check if the systems of equations

$$tx - \rho_1 y = c \cdot \mu_1 \eta_1^\ell$$
$$tx - \rho_2 y = c \cdot \mu_2 \eta_2^\ell$$

has solutions $x, y \in \mathbb{F}_7[t]$ for some ℓ. We note that μ is only determined up to a constant factor $c \in \mathbb{F}_7^\times$. Hence, if (x, y) is a solution of the index form equation, then also (cx, cy) is a solution. Calculating the defining polynomials of

$$cx\rho + cy\frac{4+5\rho+\rho^2}{t+2}$$

we obtain distinct solutions (X, Y) of the Mordell equation (11).

From the solution $(x, y) = (0, 5)$ of the index form equation we obtain the solutions

$$\begin{aligned}(X,Y) \;=\; & (2t^2+6t, t^3+t^2+6t), (t^2+3t, t^3+t^2+6t), (4t^2+5t, 6t^3+6t^2+t),\\ & (4t^2+5t, t^3+t^2+6t), (t^2+3t, 6t^3+6t^2+t), (2t^2+6t, 6t^3+6t^2+t)\end{aligned}$$

of the Mordell equation. From the solution $(x, y) = (2, 5)$ of the index form equation we obtain the solutions

$$(X, Y) = (2t, 6t), (t, 6t), (4t, t), (4t, 6t), (t, t), (2t, t)$$

of the Mordell equation.

Looking for reducible polynomials we follow the arguments of Section 3.1. The solutions of

$$3t^2(t-1) = B^2(A^2 - 4B)$$

are $B = t, A = 2, 5$, $B = 2t, A = 1, 6$ and $B = 4t, A = 3, 4$. The polynomial $h(Z) = Z^3 + AZ^2 + BZ$ is transformed into the polynomial $Z^3 + (B + 2A^2)Z + (5A^3 + 2AB)$ from which we get the corresponding solutions $X = 4A^2 + 2B$, $Y = A^3 + 6AB$ of the Mordell equation which are

$$(X, Y) = (t+1, \pm(2t+6))), (2t+2, \pm(2t+6)), (4t+4, \pm(2t+6)).$$

4.3 Example 3

We consider the equation

$$Y^2 \;=\; X^3 \,+\, 3t^6 + 2t^3 \;. \tag{14}$$

over $F = \mathbb{F}_{11}(t)$. This requires to find cubic polynomials of discriminant

$$-108(3t^6 + 2t^3) = 6t^6 + 4t^3.$$

By Section 3.2.2 we conclude that the only cubic field with suitable discriminant is $E = F(\rho)$ where ρ is a root of the polynomial

$$f(y) = y^3 - ty + t^3.$$

The function field $E = F(\rho)$ has an integral basis $\{1, \rho, \rho^2/t\}$ and discriminant $d_E = 6t^4 + 4t$. Therefore we have to find integral elements of index t in this field.

We denote by ρ_1, ρ_2, ρ_3 the conjugates of ρ. The index of any element $\alpha = a + x\rho + y\rho^2/t$ (with $a, x, y \in \mathbb{F}_{11}[t]$) can be written as

$$I(x,y) = \frac{1}{\sqrt{d_E}} \prod_{1\le i<j\le 3} \left[(\rho_i - \rho_j)x + \frac{\rho_i^2 - \rho_j^2}{t} y\right]$$

$$= t \cdot \prod_{1\le i<j\le 3} \left[x + \frac{\rho_i + \rho_j}{t} y\right] = t \cdot \prod_{k=1}^{3} \left[x - \frac{\rho_k}{t} y\right].$$

Using symmetric polynomials it is easy to show that

$$I(x,y) = tx^3 - xy^2 + ty^3.$$

In order to find elements of index t we rather write $I(x,y) = c \cdot t$ ($c \in \mathbb{F}_{11}^{\times}$) in the form

$$\prod_{k=1}^{3} (tx - \rho_k y) = c \cdot t^3.$$

This Thue equation can be solved using the method of [5]. In the field E the fundamental unit is

$$\eta = (9t^2 + 8t + 1) + (2t + 8)\rho + 9\rho^2,$$

and up to units factors there are three elements of norm t^3, namely

$$\rho,\ 10t+\rho+10\rho^2/t,\ t\ . \tag{15}$$

This yields that $\beta = tx - \rho y$ can be written in the form

$$\beta = c\cdot\mu\cdot\eta^{\ell}\ ,$$

where $c\in\mathbb{F}_{11}^{\times}$, μ is one of the elements in (15) and $\ell\in\mathbb{Z}$. Using Siegel's identity (denoting the conjugates of any $\gamma\in E$ by $\gamma_1,\gamma_2,\gamma_3$) we obtain

$$c_1\cdot\frac{(\rho_1-\rho_2)\mu_3\eta_3^{\ell}}{(\rho_1-\rho_3)\mu_2\eta_2^{\ell}}+c_2\cdot\frac{(\rho_2-\rho_3)\mu_1\eta_1^{\ell}}{(\rho_1-\rho_3)\mu_2\eta_2^{\ell}}=1$$

with some $c_1,c_2\in\mathbb{F}_{11}^{\times}$. This is a unit equation in two variables. 11-th powers can be excluded by considering finite valuations ocurring in the cross ratios of ρ. Hence, the bound for the heights of the solutions of this unit equation gives directly a bound for $|\ell|$. We note that according to [5] all elements should be represented in a sextic field containing all conjugates of ρ. Similarly as in Example 1 we obtain

$$|\ell|<16.$$

Finally, we have to check if the systems of equations

$$\begin{aligned} tx-\rho_1 y &= c\mu_1\eta_1^{\ell}\\ tx-\rho_2 y &= c\mu_2\eta_2^{\ell}\end{aligned}$$

has solutions $x,y\in\mathbb{F}_{11}[t]$ for some ℓ and $c\in\mathbb{F}_{11}^{\times}$.

From the solution $(x,y)=(1,0)$ we obtain the solutions

$$(X,Y)=(4t,\pm 5t^3)$$

of the Mordell equation (14). From the solution $(x,y)=(3t+1,8t)$ of the index form equation we obtain the solutions

$$\begin{aligned}(X,Y) \;=\; & (9t^4+6t^3+3t^2+4t,\,6t^6+6t^5+4t^4+10t^2),\\ & (9t^4+6t^3+3t^2+4t,\,5t^6+5t^5+7t^4+t^2)\end{aligned}$$

of the Mordell equation.

Looking for reducible polynomials (Section 3.1), we find that the equation

$$6t^6+4t^3=B^2(A^2-4B)$$

has no solutions A,B in $\mathbb{F}_{11}[t]$.

5 Computational aspects

In our calculations we used KASH [3] and Magma [2] in an interactive way. All computations took just a few seconds.

References

[1] E.Artin and G.Whaples, *Axiomatic characterization of fields by the product formula for valuations*, Bull. Am. Math. Soc. **51** (1945), 469-492.

[2] W.Bosma and J.Cannon, *Discovering mathematics with Magma. Reducing the abstract to the concrete*, Algorithms and Computation in Mathematics 19. Berlin, Springer, 2006.

[3] M. Daberkow, C.Fieker, J.Klüners, M.Pohst, K.Roegner and K.Wildanger, *KANT V4* , J. Symbolic Comput. **24** (1997), 267–283. http://www.math.tu-berlin.de/~kant/

[4] I.Gaál, *Diophantine equations and power integral bases*, Boston, Birkhäuser, 2002.

[5] I.Gaál and M.Pohst, *Diophantine equations over global function fields I: The Thue equation*, J. Number Theory **119** (2006), 49–65.

[6] I.Gaál and M.Pohst, *Diophantine equations over global function fields II: S-integral solutions of Thue equations*, Experimental Math. **15** (2006), 1–6.

[7] I.Gaál and M.Pohst, *Diophantine equations over global function fields IV: S-unit equations in several variables with an application to norm form equations*, J. Number Theory **130** (2010), 493–506.

[8] H.Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf klassenköpertheoretischer Grundlage*, Math. Z. **31** (1930), 565–582.

[9] A. Jätzschmann, *Zur Bestimmung ganzer Punkte auf elliptischen Kurven*, Diplomarbeit, Technische Universität Berlin, 2010.

[10] L.J.Mordell, *Diophantine equations*, Pure and Applied Mathematics **30**. London-New York, Academic Press, 1969.

[11] J.Gebel, A.Pethő and H.G.Zimmer, *On Mordell's equation*, Compos. Math. **110** (1998), 335-367.

[12] M.Pohst, *On computing non-Galois cubic global function fields of prescribed discriminant in characteristic* > 3, Publ. Math. Debrecen **79** (2011), 611–621.

[13] M.Pohst and H.Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of Mathematics and its Applications **30**, Cambridge University Press, 1989.

[14] M.Schütt and A.Schweizer, *On Davenport–Stothers inequalities and elliptic surfaces in positive characteristic*, Quart. J. Math. **59** (2008), 499–522.

[15] K. Wildanger, *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganzen Punkte einer Mordellschen Kurve*, Thesis, Technical University, Berlin, 1997.

[16] Q. Wu, *Explicit construction of integral bases of radical function fields*, J. Théor. Nombres Bordeaux **22** (2010), 259–270.