

# Diophantine equations over global function fields II: R-integral solutions of Thue equations

István Gaál \*

University of Debrecen, Mathematical Institute  
H-4010 Debrecen Pf.12., Hungary  
e-mail: igaal@math.klte.hu

and Michael Pohst †

Technische Universität Berlin, Institut für Mathematik  
Straße des 17. Juni 136, Berlin, Germany  
e-mail: pohst@math.tu-berlin.de

August 17, 2005

## Abstract

Let  $K$  be an algebraic function field over a finite field. Let  $L$  be an extension field of  $K$  of degree at least three. Let  $R$  be a finite set of valuations of  $K$  and denote by  $S$  the set of extensions of valuations of  $R$  to  $L$ . Denote by  $O_{K,R}, O_{L,S}$  the ring of  $R$ -integers of  $K$  and  $S$  integers of  $L$ , respectively. Assume that  $\alpha \in O_{L,S}$  with  $L = K(\alpha)$ , let  $0 \neq \mu \in O_{K,R}$  and consider the solutions  $(x, y) \in O_{K,R}$  of the Thue equation

$$N_{L/K}(x - \alpha y) = \mu.$$

We give an efficient method for calculating the  $R$ -integral solutions of the above equation. The method is different from that in our previous paper [2] and is much more efficient in many cases.

---

\*Research supported in part by the Alexander von Humboldt Foundation and by Grant T 042985 from the Hungarian National Foundation for Scientific Research

†Research supported by the Deutsche Forschungsgemeinschaft

2000 Mathematics Subject Classification: 11D59; 11Y50; 11R58

Keywords: Thue equations, global function fields

# 1 Introduction

Keeping the notation of Part I [2], let  $k = \mathbb{F}_q$  denote a finite field with  $q = p^d$  elements. The rational function field of  $k$  is  $k(t)$  as usual, and  $K$  is a finite extension of  $k(t)$ . The integral closure of  $k[t]$  in  $K$  is denoted by  $O_K$ . We assume that  $K$  is separably generated over  $k(t)$  by an element  $z$  belonging to  $O_K$  and that  $k$  is the full constant field of  $K$ .

Denote by  $R$  a finite set of valuations of  $K$  containing the infinite valuations. Let  $L$  be an extension field of  $K$  of degree at least three. Let  $S$  be the set of extensions of valuations of  $R$  to  $L$  and denote by  $O_{K,R}, O_{L,S}$  the ring of  $R$ -integers of  $K$ , the ring of  $S$ -integers of  $L$ , respectively. (If  $R$  is just the set of infinite valuations of  $K$ , then  $O_{K,R}$  is just  $O_K$ , the ring of integers of  $K$ .) Assume that  $\alpha \in O_{L,S}$  with  $L = K(\alpha)$ , let  $0 \neq \mu \in O_{K,R}$  and consider the solutions of the Thue equation

$$N_{L/K}(x - \alpha y) = \mu \quad \text{in } x, y \in O_{K,R}. \quad (1)$$

The purpose of the present paper is to give an efficient method for calculating the  $R$ -integral solutions of the above equation.

Our algorithm has two goals. First, instead of just integer solutions, our algorithm calculates  $R$ -integral solutions of the equation. There may be finitely many (isolated) solutions and there may occur finitely many parametrized families of solutions. If equation (1) has infinitely many solutions (that is such families occur), we give a method how to parametrize them.

Secondly, our method turned out to be much more efficient than that of [2] in many cases. For explicit calculations in function fields both in [2] and here we use Kash [1]. In both cases the calculations can be split into two parts:

1. The explicit determination of certain function field elements, valuations etc. This is usually done in an interactive way and costs almost no CPU time.
2. The test of a certain set consisting of some thousands of elements. This is done by running some loops in Kash, costing some seconds of CPU time. However, the size of this set is much smaller by using the method presented in this paper than by applying the method of [2].

The reason for this is the following. In [2] we calculated the fundamen-

tal units and represented the element  $\beta = x - \alpha y$  as a power product of the fundamental units. We derived inequalities for the exponents of the fundamental units and all possible sets of exponents must then be checked.

On the other hand, in the present paper we directly deal with the possible prime divisors of  $\beta_i/\beta_n$  ( $\beta_i$  being the conjugates of  $\beta = x - \alpha y \in L$  over  $K$ ) and use the fact that  $\beta_i/\beta_n$  determines  $x/y$ . Using an upper bound for the height of  $\beta_i/\beta_n$  we construct all divisors that are composed of the given prime divisors and have bounded height. Calculating a basis of the corresponding Riemann-Roch space we find out if such a divisor is principal, that is if it can be the splitting of the element  $\beta_i/\beta_n$  into prime divisors. This simple test (performed very fast by Kash) makes the number of possible  $\beta_i/\beta_n$  to be checked much smaller, than the number of cases to be tested with the method of [2].

## 2 Auxiliary results

In this section we recall the "fundamental inequality" (Lemma 3.1) of [2].

Let  $K$  be a finite extension of  $k(t)$  of genus  $g_K$ . The set of all (exponential) *valuations* of  $K$  is denoted by  $V$ , the subset of infinite valuations by  $V_\infty$ . For a non-zero element  $f \in K$  we denote by  $v(f)$  the value of  $f$  at  $v$ . For the normalized valuations  $v_N(f) = v(f) \cdot \deg v$  of  $K$  the *product formula*

$$\sum_{v \in V} v_N(f) = 0 \quad \forall f \in K \setminus \{0\}$$

holds. The *height* of a non-zero element  $f$  of  $K$  is defined to be

$$H(f) := \sum_{v \in V} \max\{0, v_N(f)\} = - \sum_{v \in V} \min\{0, v_N(f)\} .$$

Let  $V_0$  be a finite subset of  $V$ . Then the non-zero elements  $\gamma \in K$  satisfying  $v(\gamma) = 0$  for all  $v \notin V_0$  form a multiplicative group in  $K$ . These elements are called  *$V_0$ -units*. (For  $V_0 = V_\infty$  the  $V_0$ -units are just the units of the ring  $O_K$  of integers of  $K$ .) We consider the unit equation

$$\gamma_1 + \gamma_2 + \gamma_3 = 0 \tag{2}$$

where the  $\gamma_i$  are  $V_0$ -units.

Remark: It suffices to assume that  $\gamma_1/\gamma_3$  and  $\gamma_2/\gamma_3$  are  $V_0$ -units which makes the set  $V_0$  smaller, cf. the proof of Lemma 3.1 in [2].

**Lemma 2.1** *Let  $V_0$  be a finite subset of  $V$  and let  $\gamma_i$  ( $1 \leq i \leq 3$ ) be  $V_0$ -units satisfying (2). Then either  $\frac{\gamma_1}{\gamma_3}$  is in  $K^p$  or its height is bounded:*

$$H\left(\frac{\gamma_1}{\gamma_3}\right) \leq 2g_K - 2 + \sum_{v \in V_0} \deg v . \quad (3)$$

### 3 $R$ -integral solutions of the Thue equation

In this section we detail our algorithm for determining all  $R$ -integral solutions of equation (1).

Assume that  $(x, y)$  is a solution of (1). Denote by  $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$  the conjugates of  $\alpha$  over  $K$  and set  $\beta_i = x - \alpha_i y$ ,  $1 \leq i \leq n$ . Fix indices  $i, j$  with  $1 \leq i < j < n$ . Using the notation

$$\gamma_i = (\alpha_j - \alpha_n)\beta_i, \quad \gamma_j = (\alpha_n - \alpha_i)\beta_j, \quad \gamma_n = (\alpha_i - \alpha_j)\beta_n,$$

we can write Siegel's identity

$$(\alpha_i - \alpha_j)\beta_n + (\alpha_j - \alpha_n)\beta_i + (\alpha_n - \alpha_i)\beta_j = 0$$

in the form

$$\gamma_i + \gamma_j + \gamma_n = 0. \quad (4)$$

Denote by  $V_0$  the set of valuations of  $L_{ijn} = K(\alpha_i, \alpha_j, \alpha_n)$  containing the extensions of the valuations of  $R$ , the extensions of those valuations which have non-trivial value for  $\mu$  and all those valuations which have non-trivial value for one of the elements  $(\alpha_j - \alpha_n)/(\alpha_j - \alpha_i)$  and  $(\alpha_n - \alpha_i)/(\alpha_j - \alpha_i)$ . Then  $\gamma_i/\gamma_n$  and  $\gamma_j/\gamma_n$  are  $V_0$ -units. By Lemma 2.1 these fractions are either of bounded height or are  $p$ th powers in  $K$ . According to these two possibilities in the following we shall consider Case I and Case II. In order to obtain all solutions of equation (1) both possible cases must be considered. In Case I we get finitely many (isolated) solutions  $(x, y)$ . In Case II we can get finitely many parametrized families of solutions, cf. Section 3.1.

**Case I.** Assume that  $\gamma_i/\gamma_n$  is not a  $p$ th power in  $L_{ijn}$ . Then by applying Lemma 2.1 in the field  $M = L_{ijn}$  we derive an upper bound for the height of  $\gamma_i/\gamma_n$ .

Because of

$$\frac{\beta_i}{\beta_n} = \frac{\alpha_i - \alpha_j}{\alpha_j - \alpha_n} \frac{\gamma_i}{\gamma_n}$$

this implies

$$H\left(\frac{\beta_i}{\beta_n}\right) \leq H\left(\frac{\gamma_i}{\gamma_n}\right) + H\left(\frac{\alpha_i - \alpha_j}{\alpha_j - \alpha_n}\right). \quad (5)$$

We are going to construct all possible elements  $\beta_i/\beta_n$ . Observe that this element is contained in  $L_{in} = K(\alpha_i, \alpha_n)$ . Denote by  $W_0$  the set of valuations of  $L_{in}$  that are extensions of the valuations of  $R$  and those valuations that have nonzero values for  $\mu$ . Then  $\beta_i/\beta_n$  is a  $W_0$ -unit of  $L_{in}$ . We consider the divisors  $D_v$  corresponding to the valuations  $v$  of  $W_0$ . We form linear combinations

$$D = \sum_{v \in V_0} a_v \cdot D_v \quad (6)$$

of these divisors with suitable coefficients  $a_v \in \mathbb{Z}$  so that the height

$$\sum_{v \in V_0} \max(0, a_v) \cdot \deg v$$

does not exceed the bound in (5), and the product formula holds

$$\sum_{v \in V_0} a_v \cdot \deg v = 0.$$

We calculate a basis of the Riemann-Roch space corresponding to the divisors  $D$ . If this space is of dimension 1, then there is an element in  $L_{in}$  that splits into divisors in the given way and this element is determined (up to a non-zero factor in  $k$ ) by the basis element of the Riemann-Roch space. Otherwise, if this space is of dimension  $> 1$ , then there is no element of  $K$  that splits into divisors in the given way, and there is no possible value of  $\beta_i/\beta_n$  corresponding to the divisor (6).

Following the argument of R.C.Mason [3] (page 18) by  $\beta_i = x - \alpha_i y$ ,  $\beta_n = x - \alpha_n y$  we obtain

$$\frac{x}{y} = \frac{\alpha_n \beta_i - \alpha_i \beta_n}{\beta_i - \beta_n} = \frac{\alpha_n \frac{\beta_i}{\beta_n} - \alpha_i}{\frac{\beta_i}{\beta_n} - 1},$$

therefore  $\beta_i/\beta_n$  determines  $x/y$ . For  $y = 0$  the corresponding  $x$  can be calculated easily from (1). Note that if  $\beta_i/\beta_n = 1$  then we again obtain  $y = 0$ . Finally, equation (1) implies

$$y^n \cdot \prod_{h=1}^n \left( \frac{x}{y} - \alpha_h \right) = \mu,$$

whence by

$$y^n = \frac{\mu}{\prod_{h=1}^n \left( \frac{x}{y} - \alpha_h \right)}$$

we can determine the possible values of  $y$  and from  $x/y$  and  $y$  all possible values of  $x$ , as well. In order to determine the solutions of equation (1) in Case I we have to check all possible values of  $x$  and  $y$  if they are in  $O_{K,R}$  and if (1) is satisfied.

**Case II.** Consider now the case when  $\gamma_i/\gamma_n$  is a complete  $p$ th power in  $K$ . In the prime divisor decomposition of  $\beta_i/\beta_n$  only divisors from  $W_0$  can occur. Since

$$\frac{\gamma_i}{\gamma_n} = \frac{\alpha_j - \alpha_n}{\alpha_i - \alpha_j} \frac{\beta_i}{\beta_n},$$

in this case the values of finite valuations of  $L_{ijn}$ , appearing only in  $(\alpha_j - \alpha_n)/(\alpha_i - \alpha_j)$  and not being an extension of a valuation of  $W_0$ , must be divisible by  $p$ . If this is not satisfied for certain finite valuations, then this case is excluded. Else we replace  $p$ -th powers of elements in the unit equation by the elements themselves and repeat the argument.

This phenomenon can indeed occur as is shown by Example 2. In such a case we are lead in a straightforward way (see Section 3.1) to an infinite parametrized family of solutions. Note that only finitely many such parametrized families of solutions can occur. The character of the parametrized families of solutions is described in Section 3.1, as well as indicated why the number of such families is finite.

### 3.1 Infinite families of solutions

Now we turn to the case when in all possible unit equations the solutions are  $p$ th powers. We describe how to find the corresponding parametrized families of solutions.

In this case, for  $1 \leq i < j \leq n - 1$  equation (4) implies

$$-\frac{\gamma_i}{\gamma_n} = \eta_i^{p^m}, \quad -\frac{\gamma_j}{\gamma_n} = \eta_j^{p^m}$$

where  $m$  is a positive integer and  $\eta_i$  and  $\eta_j$  are  $V_0$ -units in  $L_{ijn}$  not being  $p$ th powers, such that  $\eta_i + \eta_j = 1$ . These equations give rise to the infinite parametric families of solutions (see below, cf. Example 2). Since there are only finitely many possibilities for  $\eta_i$  and  $\eta_j$  (there are finitely many  $V_0$ -units in  $L_{ijn}$  of bounded height), hence there can be at most finitely many infinite families of solutions.

We have

$$\frac{\beta_i}{\beta_n} = \frac{\alpha_j - \alpha_i}{\alpha_j - \alpha_n} \cdot \eta_i^{p^m}, \quad \frac{\beta_j}{\beta_n} = \frac{\alpha_j - \alpha_i}{\alpha_n - \alpha_i} \cdot \eta_j^{p^m}$$

and we can derive similar formulas for all the other  $\beta_h$ -s. Using  $\beta_1 \dots \beta_n = \mu$  we get

$$\beta_n^n \cdot \frac{\beta_1}{\beta_n} \dots \frac{\beta_{n-1}}{\beta_n} = \mu,$$

whence we obtain an expression for  $\beta_n^n$  which can be written as a power product of the fundamental  $S_n$ -units  $\varepsilon_1, \dots, \varepsilon_r$  in  $L_n = K(\alpha_n)$  ( $S_n$  denotes the set of extensions of valuations of  $R$  to  $L_n$ ). This can be used to decide if there are certain values of  $m$  for which the product is a complete  $n$ th power and if yes, which are the suitable values of  $m$ : we obtain congruence conditions for  $m$ . In this way we determine the value of  $\beta_n$  which we then use to determine  $\beta_1, \dots, \beta_{n-1}$  as a product of some fixed elements of  $L_1, \dots, L_{n-1}$  and a power product of  $\varepsilon_1, \dots, \varepsilon_r$ . Then we can check if these expressions are indeed conjugates of  $\beta_n$ , and if yes then

$$y = \frac{\beta_j - \beta_i}{\alpha_i - \alpha_j}$$

is certainly in  $O_{L,S}$ . Moreover, since the conjugates of  $y$  are equal (these equations are identical with Siegel's identity) we have  $y \in O_{K,R}$ . Finally,  $x$  is given by

$$x = \frac{\alpha_i \beta_j - \alpha_j \beta_i}{\alpha_i - \alpha_j}$$

and similarly as above we have  $x \in O_{K,R}$ . Carrying out those calculations in Cases I and II yields all solutions of (1).

## 4 Examples

### 4.1 Example 1

Let  $k = \mathbb{F}_5$  and let  $\alpha$  be a root of

$$z^4 + (4t + 2)z^2 + 1 = 0.$$

Let  $K = k(t)$  and  $R$  the set of infinite valuations of  $K$  together with the valuation corresponding to  $t + 2$ . Let  $L = K(\alpha)$ ,  $\mu = 1/(t + 2)^4$ . Consider the solutions  $x, y \in O_{K,R}$  of the equation

$$N_{L/K}(x - \alpha y) = \mu. \quad (7)$$

The extension set  $S$  of set  $R$  of valuations of  $K$  to  $L$  consists of two infinite valuations  $v_{\infty,1}, v_{\infty,2}$  both of degree 1 and two valuations  $v_{t+2,1}, v_{t+2,2}$  extending  $t + 2$  to  $L$ , both of degree 2. The field  $L$  is Galois, we have  $\alpha = \alpha_1 = \sqrt{t} + \sqrt{t+1}$  and its conjugates  $\alpha_2 = -\sqrt{t} + \sqrt{t+1}$ ,  $\alpha_3 = \sqrt{t} - \sqrt{t+1}$  and  $\alpha_4 = -\sqrt{t} - \sqrt{t+1}$  are also contained in  $L$ . The field  $L$  has genus 0. To construct the set  $V_0$  of valuations of  $L$  we have to add to  $S$  the extensions  $v_{t,1}, v_{t,2}$ , both of degree 1, of the valuation corresponding to  $t$ , and the extensions  $v_{t+1,1}, v_{t+1,2}$ , both of degree 1, of the valuation corresponding to  $t + 1$ . Then we have  $\gamma_1/\gamma_4, \gamma_2/\gamma_4$  as  $V_0$  units in  $L$  and the application of Lemma 2.1 implies, that these elements are either of height  $\leq 8$  or they are 5th powers. In Case I, if they are not 5th powers, then for the height of  $\beta_1/\beta_4$  we obtain the bound 10. This element  $\beta_1/\beta_4$  may have nontrivial values only at one of  $v_{\infty,1}, v_{\infty,2}, v_{t+2,1}, v_{t+2,2}$ . Searching over all elements of  $L$  with this property, we obtain the solutions

$$(x, y) = \left( \frac{1}{t+2}, 0 \right), \left( \frac{2}{t+2}, 0 \right), \left( \frac{3}{t+2}, 0 \right), \left( \frac{4}{t+2}, 0 \right), \\ \left( 0, \frac{1}{t+2} \right), \left( 0, \frac{2}{t+2} \right), \left( 0, \frac{3}{t+2} \right), \left( 0, \frac{4}{t+2} \right).$$

Case II can be excluded by considering

$$\frac{\gamma_1}{\gamma_4} = \frac{\alpha_2 - \alpha_4}{\alpha_1 - \alpha_2} \cdot \frac{\beta_1}{\beta_4}.$$

On the right hand side the valuations  $v_{t+1,1}, v_{t+1,2}$  occur only in  $(\alpha_2 - \alpha_4)/(\alpha_1 - \alpha_2)$  with value 1, hence the left hand side can not be a 5th power. Hence the above list consists of all  $R$ -integral solutions of equation (7).

## 4.2 Example 2

Let  $k = \mathbb{F}_5$ ,  $K = k(t)$ ,  $A = t^3 + t + 1$  and let  $\alpha = \alpha_1$  be a root of

$$z^3 - Az^2 - (A + 3)z - 1 = 0.$$

Let  $L = K(\alpha)$ , denote by  $\alpha_2, \alpha_3$  the other roots of the polynomial. This is an analogue of a simplest cubic number field, cf. D.Shanks [5]. The field  $L$  is cyclic,  $\alpha_2 = -1/(\alpha_1 + 1)$ ,  $\alpha_3 = -1/(\alpha_2 + 1)$ . The elements  $\alpha_1$  and  $\alpha_2$  are fundamental units in  $L$ . This function field has genus 4, it has three infinite valuations  $v_{\infty,1}, v_{\infty,2}, v_{\infty,3}$ , all of degree 1. Let  $S = \{v_{\infty,1}, v_{\infty,2}, v_{\infty,3}\}$ . Let  $\mu = 1$  and consider the ( $S$ -)integral solutions  $x, y \in O_K$  of

$$(x - \alpha_1 y)(x - \alpha_2 y)(x - \alpha_3 y) = 1. \quad (8)$$

In this case  $\beta_i = x - \alpha_i y$  as well as  $(\alpha_2 - \alpha_3)/(\alpha_1 - \alpha_2)$  and  $(\alpha_3 - \alpha_1)/(\alpha_1 - \alpha_2)$ , hence  $\varepsilon = -\gamma_1/\gamma_3$  and  $\eta = -\gamma_2/\gamma_3$  are units of  $L$ . Consider the unit equation

$$\varepsilon + \eta = 1 \quad (9)$$

in units  $\varepsilon, \eta$  of  $L$ .

In Case I, if  $\varepsilon$  is not a 5th power, then the application of Lemma 2.1 gives the bound 9 for the height of  $\varepsilon = -\gamma_1/\gamma_3$ . In our case both  $V_0$  and  $W_0$  is just the set of infinite valuations, hence it is more economical to construct all possible units  $\varepsilon$  from the infinite valuations (instead of deriving a somewhat larger bound for the height of  $\beta_1/\beta_3$ ). We obtain the following 9 solutions of the unit equation (9). The solutions are represented by  $\alpha_1$  and  $\alpha_2$ .

#	$\varepsilon$	$\eta$
1.	$4\alpha_1\alpha_2$	$4\alpha_2$
2.	$4\alpha_2$	$4\alpha_1\alpha_2$
3.	$4/\alpha_1$	$4/\alpha_1\alpha_2$
4.	$4/\alpha_1\alpha_2$	$4/\alpha_1$
5.	$4\alpha_1$	$4/\alpha_2$
6.	$4/\alpha_2$	$4\alpha_1$
7.	2	4
8.	4	2
9.	3	3

None of the occurring values  $\varepsilon, \eta \in L \setminus k$  is a 5th power. The values of  $\varepsilon = -\gamma_1/\gamma_3$  enable us to calculate  $\beta_1/\beta_3$  and from that the solutions of equation (8), which are

$$(x, y) = (0, 4), (4, 1), (1, 0). \quad (10)$$

In Case II, if both  $\varepsilon$  and  $\eta$  are 5th powers, but not in  $k$ , the unit equation becomes

$$\varepsilon_0^5 + \eta_0^5 = 1$$

with some units  $\varepsilon_0, \eta_0$  implying

$$(\varepsilon_0 + \eta_0)^5 = 1^5,$$

hence

$$\varepsilon_0 + \eta_0 = 1.$$

If both  $\varepsilon_0$  and  $\eta_0$  are still 5th powers, we can repeat the argument. This implies, that all further solutions of the unit equation (9) are of the form  $(\varepsilon^{5^m}, \eta^{5^m})$  for one of the solutions  $(\varepsilon, \eta)$  of equation (9) and a positive integer  $m$ . We have

$$\frac{\beta_1}{\beta_3} = \frac{\alpha_2 - \alpha_1}{\alpha_2 - \alpha_3} \cdot \varepsilon^{5^m} = 4\alpha_1 \cdot \varepsilon^{5^m}, \quad \frac{\beta_2}{\beta_3} = \frac{\alpha_2 - \alpha_1}{\alpha_3 - \alpha_1} \cdot \eta^{5^m} = 4\alpha_1\alpha_2 \cdot \eta^{5^m}. \quad (11)$$

Further,

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

that is

$$\beta_3^3 \cdot \frac{(\alpha_2 - \alpha_1)^2}{(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)} \cdot (\varepsilon\eta)^{5^m} = 1,$$

whence

$$\beta_3^3 = (\varepsilon\eta)^{-5^m} \frac{1}{\alpha_1^2\alpha_2}. \quad (12)$$

Since all occurring elements are units, for all the nine pairs  $(\varepsilon, \eta)$  of solutions of the unit equation (9) the right hand side of (12) can be represented as a power product of  $\alpha_1$  and  $\alpha_2$  and it can be easily decided if it is a cube or not.

We detail the calculations only for the first solution in the table. In this case we have  $\varepsilon\eta = \alpha_1\alpha_2^2$  hence

$$\beta_3^3 = \alpha_1^{-5^m-2} \cdot \alpha_2^{-2 \cdot 5^m-1}.$$

Here the exponents are divisible by 3 if and only if  $m = 2\ell$  with a positive integer  $\ell$ , that is

$$\beta_3 = \alpha_1^{(-5^{2\ell}-2)/3} \cdot \alpha_2^{(-2 \cdot 5^{2\ell}-1)/3}. \quad (13)$$

Similarly, for  $m = 2\ell$  we obtain  $\beta_3$  for the solutions No. 2, 3, 4, 5, 6, for the other solutions the exponents in the representation of  $\beta_3^3$  are not both divisible by 3.

For the first solution of the unit equation we have  $\varepsilon = 4\alpha_1\alpha_2, \eta = 4\alpha_2$ , hence using (11) and (13) we obtain

$$\beta_1 = (4\alpha_1) \cdot (4\alpha_1\alpha_2)^{5^{2\ell}} \cdot \alpha_1^{(-5^{2\ell}-2)/3} \cdot \alpha_2^{(-2 \cdot 5^{2\ell}-1)/3} = \alpha_1^{(2 \cdot 5^{2\ell}+1)/3} \cdot \alpha_2^{(5^{2\ell}-1)/3},$$

from which by taking conjugates (using  $\alpha_1' = \alpha_2$  and  $\alpha_2' = 1/\alpha_1\alpha_2$ ) we obtain

$$\beta_1' = \alpha_1^{(-5^{2\ell}+1)/3} \cdot \alpha_2^{(5^{2\ell}+2)/3}$$

which is the same as what we get for  $\beta_2$  from (11). Also, the conjugate of  $\beta_2$  is just  $\beta_3$ . Now if the values of  $\beta_1$  and  $\beta_2$  are indeed conjugates, then the value of

$$y = \frac{\beta_2 - \beta_1}{\alpha_1 - \alpha_2}$$

is an integer, as well as  $x = \beta_1 + \alpha_1 y = (\alpha_1\beta_2 - \alpha_2\beta_1)/(\alpha_1 - \alpha_2)$ . In this way we obtain the infinite parametric family of solutions

$$\begin{aligned} x &= \frac{1}{\alpha_1 - \alpha_2} \cdot \left( \alpha_1 \cdot \alpha_1^{(-5^{2\ell}+1)/3} \cdot \alpha_2^{(5^{2\ell}+2)/3} - \alpha_2 \cdot \alpha_1^{(2 \cdot 5^{2\ell}+1)/3} \cdot \alpha_2^{(5^{2\ell}-1)/3} \right) \\ y &= \frac{1}{\alpha_1 - \alpha_2} \cdot \left( \alpha_1^{(-5^{2\ell}+1)/3} \cdot \alpha_2^{(5^{2\ell}+2)/3} - \alpha_1^{(2 \cdot 5^{2\ell}+1)/3} \cdot \alpha_2^{(5^{2\ell}-1)/3} \right). \end{aligned}$$

For the solutions No. 2, 4, 5 of the unit equation we obtain  $\beta_1' \neq \beta_2$  hence we do not get a solution  $(x, y)$ . For the solutions No. 3, 6 of the unit equation we obtain the following infinite parametric families of solutions  $(x, y)$ , respectively:

$$\begin{aligned} x &= \frac{1}{\alpha_1 - \alpha_2} \cdot \left( \alpha_1 \cdot \alpha_1^{(-5^{2\ell}+1)/3} \cdot \alpha_2^{(-2 \cdot 5^{2\ell}+2)/3} - \alpha_2 \cdot \alpha_1^{(-5^{2\ell}+1)/3} \cdot \alpha_2^{(5^{2\ell}-1)/3} \right) \\ y &= \frac{1}{\alpha_1 - \alpha_2} \cdot \left( \alpha_1^{(-5^{2\ell}+1)/3} \cdot \alpha_2^{(-2 \cdot 5^{2\ell}+2)/3} - \alpha_1^{(-5^{2\ell}+1)/3} \cdot \alpha_2^{(5^{2\ell}-1)/3} \right) \end{aligned}$$

and

$$x = \frac{1}{\alpha_1 - \alpha_2} \cdot \left( \alpha_1 \cdot \alpha_1^{(2 \cdot 5^{2\ell} + 1)/3} \cdot \alpha_2^{(5^{2\ell} + 2)/3} - \alpha_2 \cdot \alpha_1^{(-5^{2\ell} + 1)/3} \cdot \alpha_2^{(-2 \cdot 5^{2\ell} - 1)/3} \right)$$

$$y = \frac{1}{\alpha_1 - \alpha_2} \cdot \left( \alpha_1^{(2 \cdot 5^{2\ell} + 1)/3} \cdot \alpha_2^{(5^{2\ell} + 2)/3} - \alpha_1^{(-5^{2\ell} + 1)/3} \cdot \alpha_2^{(-2 \cdot 5^{2\ell} - 1)/3} \right).$$

Hence all solutions of equation (8) are given by the four isolated solutions (10) together with the above three parametrized families of solutions.

**Remark** The algorithms were implemented in KASH, the KANT-Shell [1]. The computations of the examples were carried out on an AMD Athlon i686 with 1733 MHz and 512 MB RAM under Suse Linux 8.0, and took just a few seconds.

**Acknowledgements.** The authors thank the referee for his detailed comments which helped to improve the quality of the paper.

## References

- [1] M. Daberkow, C.Fieker, J.Klüners, M.Pohst, K.Roegner and K.Wildanger, *KANT V4*, J.Symbolic Comput. **24**(1997), 267–283.
- [2] I.Gaál and M.Pohst, *Diophantine equations over global function fields I: The Thue equation*, submitted.
- [3] R.C.Mason, *Diophantine equations over function fields*, Cambridge University Press, 1984.
- [4] H.Niederreiter and Chaoping Xing, *Rational points on curves over finite fields*, London Math. Soc. Lecture Note Ser. 285, Cambridge University Press, 2001.
- [5] D.Shanks, *The simplest cubic fields*, Math. Comput., **28**(1974), 1137–1152.
- [6] A.Thue, *Über Annäherungswerte algebraischer Zahlen*, J.Reine Angew. Math., **135**(1909), 284–305.