Compositio Mathematica **112:** 273–312, 1998.

Solving superelliptic Diophantine equations by Baker's method

YURI F. BILU[1]* and GUILLAUME HANROT[2]

[1]*Mathematisches Institut, Universität Basel Rheinsprung 21, CH-4051 Basel, Switzerland; e-mail: yuri@math.unibas.ch*

[2]*Algorithmique Arithmétique Expérimentale (A2X), UMR CNRS 9936, Université Bordeaux 1, 351, cours de la Libération, F-33405 Talence Cedex, France, e-mail: hanrot@math.u-bordeaux.fr*

Received March 12 1997; accepted March 23 1997

Abstract. We describe a method for complete solution of the superelliptic Diophantine equation $ay^p = f(x)$. The method is based on Baker's theory of linear forms in the logarithms. The characteristic feature of our approach (as compared with the classical method) is that we reduce the equation directly to the linear forms in logarithms, without intermediate use of Thue and linear unit equations. We show that the reduction method of Baker and Davenport [3] is applicable for superelliptic equations, and develop a very efficient method for enumerating the solutions below the reduced bound. The method requires computing the algebraic data in number fields of degree $pn(n-1)/2$ at most; in many cases this number can be reduced. Two examples with $p = 3$ and $n = 4$ are given.

Mathematics Subject Classifications: Primary: 11Y50; Secondary: 11D25, 11D41.

Key words: Diophantine equations, linear forms in logarithms.

1. Introduction

In this paper we propose a method for complete solution of the superelliptic Diophantine equation

$$ay^p = f(x), \tag{1}$$

where a is a nonzero integer, $p \geqslant 3$ and $f(x) \in \mathbb{Z}[x]$ a separable polynomial of degree $n \geqslant 2$. Recall that the first effective bound for the integral solutions of this equation was obtained by A. Baker [2] as an application of his theory of linear forms in logarithms [1]. For further advance and bibliography see [24, 26, 25, 9, 22, 21, 29]. In these papers the equation (1) is reduced to finitely many Thue equations over certain number fields, each of the latter being then reduced to finitely many linear unit equations, which can be analyzed using Baker's theory. (Voutier [29] reduces (1) directly to linear unit equations, without intermediate use of Thue equations.) However, this method (call it 'Thue descent') does not seem to

* Current address: Forschungsinstitut für Mathematik, ETH-Zentrum, CH-8092 Zurich, Switzerland.

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

be suitable for practical solution of the superelliptic equation, because the number of Thue (or linear unit) equations to be solved turns out to be very large, even when the equation has very moderate coefficients.

In the present paper we develop a different method, reducing the superelliptic equation directly to the linear forms in logarithms, without intermediate use of Thue and linear unit equations (as it is done in [6]). For simplicity, we deal with case when p is an odd prime. Since the case of an arbitrary $p \neq 2^k$ can be reduced to the case of an odd prime p, we almost preserve the generality. With a few changes, our method extends to the *hyperelliptic equation* $ay^2 = f(x)$, where $f(x)$ is a separable polynomial of degree at least 3 (see Appendix E).

In accordance with the general ideology of [5], our method can be described as follows.

(i) Construct functional units in an unramified extension of the field $\mathbb{Q}(x, (a^{-1}f(x))^{1/p})$;

(ii) Using the fact that the specialization of a functional unit at an integral point is 'almost a unit' of a certain number field, reduce the equation to finitely many inequalities of the type

$$0 < \left|\alpha_0\alpha_1^{b_1}\dots\alpha_n^{b_n} - 1\right| < \exp(-cB), \tag{2}$$

where $B = \max(|b_1|, \dots, |b_n|)$ and c is an effectively computable constant.

(iii) Obtain from (2) an upper bound for B by means of the theory of linear forms in logarithms.

Successful choice of functional units allowed us to reduce the degrees of number fields, occurring in the process of solution, from $pn(n-1)$, as required for the Thue descent, to $\frac{1}{2}pn(n-1)$, which is very important from the computational point of view. (See Subsection 5.5.)

The theoretical bound for B, obtained from the theory of linear forms in logarithms, is very large. As explained in [17, 27], in practical cases the bound for B can be significantly reduced with the help of the Lenstra–Lenstra–Lovász (further LLL) algorithm [13]. In [8] we showed that in the case of the Diophantine equations of Thue, one can replace the LLL by the simple continued fraction algorithm, as Baker and Davenport [3] did already in 1969. It turns out that the same idea works for the superelliptic equation, see Subsection 4.6.

Another difficult point in the numerical solution of Diophantine equations is enumerating all solutions below the reduced bound. Various approaches to this problem are suggested in [30, 28, 23] and other papers. Here we use the method of [6, 8], in a somewhat modified form.

We refer to [17, 27] for the history of the numerical solution of Diophantine equations and extensive bibliography up to 1989. Some of later references most close to the subject of the present paper are [14, 15, 16, 31, 32].

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

2. Notation and conventions

Throughout the paper p is a fixed prime number, and $f(x) \in \mathbb{Z}[x]$ a fixed separable polynomial of degree $n \geqslant 2$. For the sake of further applications, we do not exclude the case $p = 2$ wherever possible. In all cases where we had to assume that $p \neq 2$, this is explicitly specified. We fix a primitive root of unity ζ of degree p and put

$$\mathcal{P} = \{0, \dots, p-1\}.$$

Given $b \in \mathbb{Z}$, we denote by $b_{\operatorname{mod} p}$ the uniquely defined $b' \in \mathcal{P}$ such that $b \equiv b' \pmod p$.

We fix once and for all an embedding $\overline{\mathbb{Q}} \to \mathbb{C}$, so that any algebraic number has a well defined complex value. We use the branches of the functions $z^{1/p}$ and $\log z$ defined by $-\pi/p < \arg z^{1/p} \leqslant \pi/p$ and $-\pi < \operatorname{Im} \log z \leqslant \pi$. We write $z^{-1/p}$ instead of $(z^{1/p})^{-1}$. Note that

$$\operatorname{Re} z_1, \operatorname{Re} z_2 > 0 \Rightarrow (z_1 z_2^{\pm 1})^{1/p} = z_1^{1/p} z_2^{\pm 1/p}. \tag{3}$$

Put

$$\mathrm{Sol} = \{x \in \mathbb{Z} : (a^{-1} f(x))^{1/p} \in \mathbb{Z}\}.$$

Elements of the set Sol are referred to as ‘solutions’.

For a vector $\boldsymbol{b} = (b_1, \dots, b_\mu) \in \mathbb{C}^\mu$ put $|\boldsymbol{b}|_\infty = \max(|b_1|, \dots, |b_\mu|)$.

We use $O_1(\dots)$ as a quantitative version of the standard notation $O(\dots)$:

$$A = O_1(B)$$

means $|A| \leqslant B$.

We fix two distinct roots α and β of $f(x)$ and put

$$c_1 = \max(\overline{|\alpha|}, \overline{|\beta|}), \qquad X_1 = 3c_1,$$

where $\overline{|\alpha|}$ is the maximum of the absolute values of the conjugates of α over $\mathbb{Q}$, and $\overline{|\beta|}$ is defined similarly.

Solutions satisfying $|x| \leqslant X_1$ can be quickly found by direct enumeration. In the sequel we restrict ourselves on the solutions satisfying $|x| > X_1$. In particular, we say simply ‘solution’ instead of ‘solution with $|x| > X_1$’ and write ‘$x \in$ Sol instead of ‘$x \in$ Sol and $|x| > X_1$’.

The assumption $|x| > X_1$ allows us to avoid certain pathologies that occur for small solutions. In particular

$$x \neq 0, \alpha, \beta \quad \text{and} \quad \arg \frac{x-\alpha}{x-\beta} \neq \pi. \tag{4}$$

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

Table I. Specific notations

Notation	Where introduced	Notation	Where introduced
$\mathbb{K}_0$	Beginning of Subsection 4.1*	$\Xi(\alpha)$	Lemma 3.2
M_0	Equations (15) and (16)	M	Equation (17)
$\mathbb{K}, m, s, t, \sigma_i, \alpha_i, \beta_i$	Beginning of Subsection 4.2	$s_0,\ t_0$	Proposition 4.2.1
$\mathrm{Sol}(\mathbb{K}), k(x), k_i(x), \boldsymbol{k}(x)$	After Proposition 4.2.1	$\varphi(x)$	Subsection 4.3
$\eta_j, \Theta, \theta(x), b_j(x), \boldsymbol{b}(x)$	End of Subsection 4.3	$\varphi_i(x)$	Equation (39)
$\theta, \boldsymbol{k}, \mathrm{Sol}(\mathbb{K}, \boldsymbol{k}, \theta)$	Beginning of Subsection 4.4	ζ_i	After Equation (39)
$\theta_i, \eta_{ij}, \rho_i, \gamma_i$	Equation (40)	A, a_{ij}	After Equation (40)
Δ_i, λ_i	Equation (41)	X_4	Corollary 4.4.2
c_2–$c_{10}, X_2,\ X_3$	Equation (42)	c_{11}	Theorem 4.5.1
$i_1,\ i_2$	Equations (60), (61) and (62)	$\Phi(x)$	Equation (63)
c_{13}–c_{16}, B_0	End of Subsection 4.5	c_{12}	After Equation (66)
$j_1, j_2, \Delta, \lambda$	Subsection 4.6.1	$\Vert\ldots\Vert$	After Equation (79)
$c_{18},\ c_{19}$	After Equation (78)	B_0'	Subsection 4.7
$\omega_i, \gamma_i', c_{19}$–$c_{23}, X_5$	Before Lemma 4.7.1	$b_j'(x)$	Equation (87)
$\mathbb{K}_0', \tau : \mathbb{K}_0' \to \mathbb{K}_0'$	Beginning of Subsection 5.2	$s',\ s_0'$	Proposition 5.3.1
$\mathbb{K}', \tau : \mathbb{K}' \to \mathbb{K}'$	Beginning of Subsection 5.3	$X_7,\ X_8$	Appendix D

*In the case of (α, β)-symmetry $\mathbb{K}_0$ is defined in the beginning of Subsection 5.2.

We shall use properties (4) of the solutions without special reference.

More specific notations are introduced in the course of the paper. For the reader's convenience, we give a glossary of the most important notations in Table I.

For the practical implementation of our method one should be able to perform various operations in certain number fields. We distinguish here four operations:

(PD) find the prime ideal decomposition of a given fractional ideal;

(U) find the group of roots of unity and a system of fundamental units;

(PI) decide whether a given fractional ideal is principal and find its generator if it is;

(CG) compute the class group, construct a system of representatives of the ideal classes and find the representative of a given fractional ideal.

(Note that (CG) partially covers (PI).) Fulfilling these operations (which will be referred to as 'multiplicative') in the occurring fields seems to be the main difficulty of our method.

We do not mention here 'additive' operations (finding integral bases, etc.). Though these operations should also be performed, they are much easier algorithmically than the 'multiplicative' ones. See, for example, [10, 20, 19].

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

3. Classical background

In this section we review some classical facts [2, 25, 22, 21, 29], but in a very explicit setting. The results of this section do not require the assumption $|x| > X_1$.

Fix a root α of $f(x)$. A prime ideal $\mathfrak{p}$ of the field $\mathbb{Q}(\alpha)$ is *exclusive* if

$$\text{either}\quad \mathrm{Ord}_{\mathfrak{p}}(a) > 0 \quad\text{or}\quad \mathrm{Ord}_{\mathfrak{p}}(\alpha) < 0 \quad\text{or}\quad \mathrm{Ord}_{\mathfrak{p}}(f'(\alpha)) < 0,$$

where a is from (1). (Recall that $\mathrm{Ord}_{\mathfrak{p}}(\gamma)$ is the largest integer m such that $\gamma \in \mathfrak{p}^m$.)

PROPOSITION 3.1. *Let* $\mathfrak{p}$ *be a prime ideal of* $\mathbb{Q}(\alpha)$ *with* $\mathrm{Ord}_{\mathfrak{p}}(\alpha) \geqslant 0$. *Then for any* $x \in \mathrm{Sol}$ *one has either*

$$0 \leqslant \mathrm{Ord}_{\mathfrak{p}}(x-\alpha) \leqslant \mathrm{Ord}_{\mathfrak{p}}(f'(\alpha)), \tag{5}$$

or[1]

$$0 \leqslant (\mathrm{Ord}_{\mathfrak{p}}(a) - \mathrm{Ord}_{\mathfrak{p}}(x-\alpha))_{\mathrm{mod}\, p} \leqslant \mathrm{Ord}_{\mathfrak{p}}(f'(\alpha)). \tag{6}$$

In particular, if $\mathfrak{p}$ *is non-exclusive then* $p|\mathrm{Ord}_{\mathfrak{p}}(x-\alpha)$.

Proof. We write Ord instead of $\mathrm{Ord}_{\mathfrak{p}}$. Denote by $\mathcal{O}_{\mathfrak{p}}$ the local ring of the ideal $\mathfrak{p}$ (recall that $\mathcal{O}_{\mathfrak{p}} = \{\gamma \in \mathbb{Q}(\alpha) : \mathrm{Ord}(\gamma) \geqslant 0\}$) and put $f_\alpha(x) = f(x)/(x-\alpha)$. Since $f'(\alpha)$ is the resultant of the polynomials $x-\alpha$ and $f_\alpha(x)$, both having coefficients in $\mathcal{O}_{\mathfrak{p}}$, we have

$$A(x)(x-\alpha) + B(x)f_\alpha(x) = f'(\alpha), \tag{7}$$

for some $A(x), B(x) \in \mathcal{O}_{\mathfrak{p}}[x]$.

Now let (x, y) be a solution of (1) with $\mathrm{Ord}(x-\alpha) > \mathrm{Ord}(f'(\alpha))$. Then $\mathrm{Ord}(f_\alpha(x)) \leqslant \mathrm{Ord}(f'(\alpha))$ by (7). Since

$$\begin{aligned}\mathrm{Ord}(x-\alpha) &= \mathrm{Ord}(f(x)) - \mathrm{Ord}(f_\alpha(x))\\ &= \mathrm{Ord}(ay^p) - \mathrm{Ord}(f_\alpha(x))\\ &\equiv \mathrm{Ord}(a) - \mathrm{Ord}(f_\alpha(x)) \pmod p,\end{aligned}$$

we have (6). The proposition is proved.

The following lemma is crucial for the effective study of superelliptic equations.

LEMMA 3.2. *There exists a finite effectively constructible set* $\Xi = \Xi(\alpha) \subset \mathbb{Q}(\alpha)$ *with the following property. For any* $x \in \mathrm{Sol}$

$$x - \alpha = \xi\lambda^p, \tag{8}$$

[1] Recall that for any $b \in \mathbb{Z}$ we denote by $b_{\mathrm{mod}\, p}$ the unique $b' \in \mathcal{P}$ such that $b \equiv b' (\mathrm{mod}\, p)$.

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

with $\xi \in \Xi$ *and* $\lambda \in \mathbb{Q}(\alpha)$.

Proof. We construct the set Ξ as follows. Write the principal ideal (α) as $(\alpha)_0/(\alpha)_\infty$, where $(\alpha)_0$ and $(\alpha)_\infty$ are coprime integral ideals of the field $\mathbb{Q}(\alpha)$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ be all exclusive ideals satisfying $\mathrm{Ord}_{\mathfrak{p}}(\alpha) \geqslant 0$. Consider ideals of the type

$$\mathfrak{a} = \mathfrak{a}(b_1, \dots, b_k) = (\alpha)_\infty^{-1}\mathfrak{p}_1^{b_1} \dots \mathfrak{p}_k^{b_k}, \tag{9}$$

where every $b_i \in \mathcal{P}$ satisfies either

$$b_i \leqslant \mathrm{Ord}_{\mathfrak{p}_i}(f'(\alpha)), \tag{10}$$

or

$$0 \leqslant (\mathrm{Ord}_{\mathfrak{p}_i}(a) - b_i)_{\mathrm{mod}\, p} \leqslant \mathrm{Ord}_{\mathfrak{p}_i}(f'(\alpha)). \tag{11}$$

For any such $\mathfrak{a}$ let $\Delta = \Delta(\mathfrak{a})$ be a maximal set of pairwise non-equivalent[2] ideals $\mathfrak{b}$ of the field $\mathbb{Q}(\alpha)$ such that $\mathfrak{a}\mathfrak{b}^p$ is principal for any $\mathfrak{b} \in \Delta$. (The set Δ can happen to be empty.) Constructing the set Δ requires the operation (CG) in the field $\mathbb{Q}(\alpha)$. If this field has class number 1, then we can put $\Delta(\mathfrak{a}) = \{(1)\}$ for any $\mathfrak{a}$.

Fix a generator ξ_0 for any principal ideal $\mathfrak{a}\mathfrak{b}^p$, where $\mathfrak{a}$ is of the type (9) and $\mathfrak{b} \in \Delta(\mathfrak{a})$. (Here the operation (PI) is needed.) Let Ξ_0 be the set of all numbers ξ_0 obtained this way. Also, let ω generate the group of roots of unity of the field $\mathbb{Q}(\alpha)$ and $\eta_1, \dots, \eta_r$ be a system of basic units (here (U) is needed). We put

$$\Xi = \{\xi_0\omega^{b_0}\eta_1^{b_1} \dots \eta_r^{b_r} : \xi_0 \in \Xi_0, b_0, \dots, b_r \in \mathcal{P}\}.$$

It is easy to see that the set Ξ is as desired. Let $x \in$ Sol. By Proposition 3.1 the principal ideal $(x - \alpha)$ can be presented in the form $\mathfrak{a}\mathfrak{b}_1^p$ where $\mathfrak{a}$ is an ideal of the type (9). Let $\mathfrak{b} \in \Delta(\mathfrak{a})$ be equivalent to $\mathfrak{b}_1$ and $\xi_0 \in \Xi_0$ generate $\mathfrak{a}\mathfrak{b}^p$. Then $(x - \alpha) = (\xi_0)(\lambda_0)^p$ with $\lambda_0 \in \mathbb{Q}(\alpha)$. Therefore we have (8) with $\xi \in \Xi$ and $\lambda \in \mathbb{Q}(\alpha)$. The lemma is proved.

The most important case of Equation (1) is when the polynomial $f(x)$ is irreducible. Under this assumption one has further (severe) restrictions for $\mathrm{Ord}_{\mathfrak{p}}(x-\alpha)$, which considerably reduces the set Ξ.

Indeed, denote by f_n the leading coefficient of $f(x)$, that is

$$f(x) = f_n x^n + \text{terms of lower degree.} \tag{12}$$

Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\alpha)$ and $\mathrm{f} = \mathrm{f}_{\mathfrak{p}}$ the residue degree of $\mathfrak{p}$ over $\mathbb{Q}$. That is, $\mathcal{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\mathfrak{p}) = P^{\mathrm{f}}$, where $P = P(\mathfrak{p})$ is the underlying prime. Since $\mathcal{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(x - \alpha) = (a/f_n)y^p$, we have

$$\mathrm{f}_{\mathfrak{p}}\, \mathrm{Ord}_{\mathfrak{p}}(x - \alpha) \equiv \mathrm{Ord}_P(a/f_n) \pmod{p}, \tag{13}$$

[2] Recall that ideals $\mathfrak{b}_1$ and $\mathfrak{b}_2$ are *equivalent* if the fractional ideal $\mathfrak{b}_1\mathfrak{b}_2^{-1}$ is principal.

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

for any solution[3] x. This defines $\mathrm{Ord}_{\mathfrak{p}}(x-\alpha)$ uniquely modulo p as soon as $\mathrm{f}_{\mathfrak{p}} \not\equiv 0 \pmod p$.

Hence, when $f(x)$ is irreducible, one can, for every $\mathfrak{p}_i$ with $\mathrm{f}_i := \mathrm{f}_{\mathfrak{p}_i}$ / $\equiv 0 \pmod p$, define the corresponding $b_i \in \mathcal{P}$ uniquely from $\mathrm{f}_i b_i \equiv \mathrm{Ord}_{P_i}(a/f_n) \pmod p$, rather than consider all possible b_i satisfying (10) or (11). (Here $P_i = P(\mathfrak{p}_i)$.) In particular, $b_i = 0$ whenever

$$\mathrm{f}_i \not\equiv 0 \pmod p \quad \text{and} \quad \mathrm{Ord}_{P_i}(a/f_n) \equiv 0 \pmod p. \tag{14}$$

Therefore the ideals $\mathfrak{p}_i$ which satisfy (14) can be excluded from consideration.

4. The general method

4.1. Admissible fields

Put $\mathbb{K}_0 = \mathbb{Q}(\alpha, \beta)$.

DEFINITION 4.1.1. A number field $\mathbb{K}$ is *admissible* for a solution x if

$$\mathbb{K} = \mathbb{K}_0\left(\zeta^k\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\right),$$

for some $k \in \mathcal{P}$. A system of number fields $\{\mathbb{K}\}$ is *a complete system of admissible fields* if it contains an admissible field for any solution x.

All conjugates of $(x-\alpha/x-\beta)^{1/p}$ over $\mathbb{K}_0$ are among the numbers $\zeta^k(x-\alpha/x-\beta)^{1/p}$, where $k \in \mathcal{P}$. Hence any field isomorphic to $\mathbb{K}$ over $\mathbb{K}_0$ is admissible for x as soon as $\mathbb{K}$ is admissible for x. A complete system is *minimal* if it consists of fields pairwise non-isomorphic over $\mathbb{K}_0$.

By Kummer's theory [12, Ch. 6, Thm 8.1], either $\zeta^k(x-\alpha/x-\beta)^{1/p} \in \mathbb{K}_0$ for some $k \in \mathcal{P}$, or

$$\left[\mathbb{K}_0\left(\zeta^k\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\right) : \mathbb{K}_0\right] = p \quad \text{for all } k \in \mathcal{P}$$

and the p fields $\mathbb{K}_0(\zeta^k(x-\alpha/x-\beta)^{1/p})$ are isomorphic over $\mathbb{K}_0$. This prompts the following procedure for constructing a complete system of admissible fields. Let $\Xi(\alpha)$ be the set constructed in Lemma 3.2 and $\Xi(\beta)$ a similar set for the root β. Put

$$\mathrm{M}_0 = \{\xi'/\xi'' \colon \xi' \in \Xi(\alpha), \xi'' \in \Xi(\beta)\} \subset \mathbb{Q}(\alpha, \beta). \tag{15}$$

[3] Sometimes (13) even provides a local obstruction for solubility of Equation (1): if $\mathrm{f}_{\mathfrak{p}} \equiv 0 \pmod p$ but $\mathrm{Ord}_P(a/f_n) \not\equiv 0 \pmod p$ then (1) has no solutions at all.

If α and β are conjugate over $\mathbb{Q}$ and $\tau\colon \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ is the automorphism taking α to β, then we can define M_0 alternatively as

$$\mathrm{M}_0 = \{\xi/\tau(\xi)\colon \xi \in \Xi(\alpha)\}. \tag{16}$$

Further, put

$$\mathrm{M} = \{\mu \in \mathrm{M}_0 : \mu \text{ is not a } p\text{-th power in } \mathbb{K}_0\}. \tag{17}$$

Then the fields $\mathbb{K}_0$ and all $\mathbb{K}_0\ (\mu^{1/p})$, where μ runs the set M, form a complete system of admissible fields. Testing them for isomorphism, we obtain a minimal complete system.

It is worth mentioning here that, though the set M can be large, we expect that the size of the minimal complete system obtained this way would be reasonable, because distinct $\mu \in \mathrm{M}$ often give rise to $\mathbb{K}_0$-isomorphic fields $\mathbb{K}_0\ (\mu^{1/p})$. This expectation was confirmed in all examples we considered. For instance, in the second of the examples discussed in Section 6, we had $|\mathrm{M}| = 18$, while the minimal complete system included only 4 fields (together with $\mathbb{K}_0$).

4.2. A fixed admissible field

Starting from this subsection we fix an admissible field $\mathbb{K}$ from the complete system constructed in the previous subsection. Let $m = [\mathbb{K} : \mathbb{Q}] = s + 2t$, where $\sigma_1, \ldots, \sigma_s\colon \mathbb{K} \to \mathbb{R}$ are the real embeddings of $\mathbb{K}$, and $\sigma_{s+1}, \ldots, \sigma_{s+2t}\colon \mathbb{K} \to \mathbb{C}$ are the complex ones, σ_{s+i} and σ_{s+i+t} being complex conjugate. We write α_i and β_i instead of $\sigma_i(\alpha)$ and $\sigma_i(\beta)$, respectively.

The following observation is immediate.

PROPOSITION 4.2.1. *If* $[\mathbb{K} : \mathbb{K}_0] = p \geqslant 3$, *then each real embedding of* $\mathbb{K}_0$ *has exactly one real prolongation to* $\mathbb{K}$, *and* $p - 1/2$ *pairs of complex conjugate prolongations. In particular, in this case* $s = s_0$ *and* $t = pt_0 + (p - 1/2)s_0$, *where* s_0 *and* $2t_0$ *are the numbers of real and complex embeddings of* $\mathbb{K}_0$, *respectively.*

We denote by $\mathrm{Sol}(\mathbb{K})$ the set of solutions x such that $\mathbb{K}$ is admissible for x. For any $x \in \mathrm{Sol}(\mathbb{K})$ there exists $k(x) \in \mathcal{P}$ such that $\zeta^{k(x)}(x - \alpha/x - \beta)^{1/p} \in \mathbb{K}$. Of course, $k(x)$ is not well-defined in the case $\zeta \in \mathbb{K}_0$.

Given $x \in \mathrm{Sol}(\mathbb{K})$ and $i \in \{1, \ldots, m\}$, define $k_i(x) \in \mathcal{P}$ from

$$\sigma_i\left(\zeta^{k(x)}\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\right) = \zeta^{k_i(x)}\left(\frac{x-\alpha_i}{x-\beta_i}\right)^{1/p}. \tag{18}$$

Then

$$k_1(x) = \cdots = k_s(x) = 0, \tag{19}$$

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

$$k_i(x) + k_{i+t}(x) \equiv 0 \pmod p \quad (s < i \leqslant s+t). \tag{20}$$

Therefore there are at most p^t possibilities for the vector $\boldsymbol{k}(x) = (k_1(x), \dots, k_m(x))$.

Now assume that $[\mathbb{K} : \mathbb{K}_0] = p$. Then any embedding of $\mathbb{K}_0$ has p distinct prolongations to $\mathbb{K}$. If σ_{i_1} and σ_{i_2} are distinct embeddings of $\mathbb{K}$ coinciding on $\mathbb{K}_0$ then $k_{i_1} \neq k_{i_2}$. Therefore, in addition to (19)–(20), we have the following:

if $\sigma_{i_1}, \dots, \sigma_{i_p}$ are the p distinct prolongations of a fixed embedding of $\mathbb{K}_0$, then $\{k_{i_1}(x), \dots, k_{i_p}(x)\} = \mathcal{P}$. (21)

It follows from Proposition 4.2.1 and (19)–(21) that in the case $[\mathbb{K} : \mathbb{K}_0] = p \geqslant 3$ there at most $(2^{p-1/2}(p-1/2)!)^{s_0}\ (p!)^{t_0}$ possibilities for $\boldsymbol{k}(x)$. See Appendix B for further ideas how to reduce the number of possibilities for $\boldsymbol{k}(x)$.

4.3. FUNCTION $\varphi(x)$ AND SET Θ

For any $x \in \mathrm{Sol}(\mathbb{K})$ put

$$\varphi(x) = (x-\beta)\left(\zeta^{k(x)}\left(\frac{x-\alpha}{x-\beta}\right)^{1/p} - 1\right)^p. \tag{22}$$

PROPOSITION 4.3.1. *There exists a finite effectively constructible set $\Theta_0 \subset \mathbb{K}$ with the following property: for any $x \in \mathrm{Sol}(\mathbb{K})$ there are $\theta_0 \in \Theta_0$ and a unit η of the field $\mathbb{K}$ such that*

$$\varphi(x) = \theta_0\eta. \tag{23}$$

Proof. For any prime ideal $\mathfrak{p}$ of $\mathbb{K}$ put

$$u_1(\mathfrak{p}) = \max(0, -\mathrm{Ord}_{\mathfrak{p}}(\alpha), -\mathrm{Ord}_{\mathfrak{p}}(\beta)), \tag{24}$$

$$u_2(\mathfrak{p}) = \max(0, \mathrm{Ord}_{\mathfrak{p}}(\alpha-\beta)). \tag{25}$$

Then u_1 and u_2 are non-negative integers both equal to 0 for all but finitely many $\mathfrak{p}$. If the polynomial $f(x)$ is monic then $u_1(\mathfrak{p}) = 0$ for all $\mathfrak{p}$.

Let Θ_0 be a maximal set of pairwise non-associate $\theta_0 \in \mathbb{K}$ satisfying

$$-u_1(\mathfrak{p}) \leqslant \mathrm{Ord}_{\mathfrak{p}}(\theta_0) \leqslant pu_2(\mathfrak{p}) + (p-1)u_1(\mathfrak{p}), \tag{26}$$

for all $\mathfrak{p}$. (Recall that two algebraic numbers are *associate* if their ratio is a unit.) Note that, in order to construct Θ_0, one should be able to perform the operations (PD) and (PI) in the field $\mathbb{K}$.

Now let x be a solution. Then

$$\varphi(x)\tilde{\varphi}(x) = (\beta-\alpha)^p, \tag{27}$$

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

where

$$\tilde{\varphi}(x) = \prod_{\substack{k' \in \mathcal{P} \\ k' \neq k(x)}} (x-\beta) \left(\zeta^{k'} \left(\frac{x-\alpha}{x-\beta} \right)^{1/p} - 1 \right)^p .$$

For some $k'' \in \mathcal{P}$ we have

$$\varphi(x) = ((x-\alpha)^{1/p} - \zeta^{k''}(x-\beta)^{1/p})^p, \tag{28}$$

$$\tilde{\varphi}(x) = \prod_{\substack{k' \in \mathcal{P} \\ k' \neq k''}} ((x-\alpha)^{1/p} - \zeta^{k'}(x-\beta)^{1/p})^p. \tag{29}$$

Fix a prime ideal $\mathfrak{p}$ of the field $\mathbb{K}$. Let $| \dots |_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic valuation on $\mathbb{K}$, extended somehow to the field $\mathbb{K}(\zeta, (x-\alpha)^{1/p}, (x-\beta)^{1/p})$. As follows from (28) and (29), we have

$$|\varphi(x)|_{\mathfrak{p}} \leqslant \max\left(1, |\alpha|_{\mathfrak{p}}, |\beta|_{\mathfrak{p}}\right),$$

$$|\tilde{\varphi}(x)|_{\mathfrak{p}} \leqslant \left(\max\left(1, |\alpha|_{\mathfrak{p}}, |\beta|_{\mathfrak{p}}\right)\right)^{p-1}.$$

Together with (27) this yields

$$-u_1(\mathfrak{p}) \leqslant \mathrm{Ord}_{\mathfrak{p}}(\varphi(x)) \leqslant pu_2(\mathfrak{p}) + (p-1)u_1(\mathfrak{p}). \tag{30}$$

Thus

$$\varphi(x) \text{ is associate to some } \theta_0 \in \Theta_0. \tag{31}$$

The proposition is proved.

Remark 4.3.2. In the case $[\mathbb{K} : \mathbb{K}_0] = p$ the set Θ_0 can be made smaller. Indeed, in this case

$$\mathcal{N}_{\mathbb{K}/\mathbb{K}_0}(\varphi(x)) = (\beta - \alpha)^p. \tag{32}$$

Hence all θ_0 such that the principal ideals

$$(\mathcal{N}_{\mathbb{K}/\mathbb{K}_0}(\theta_0)) \quad \text{and} \quad ((\beta-\alpha)^p) \tag{33}$$

are distinct, can be excluded from the set Θ_0.

Let Ω be the group of roots of unity of the field $\mathbb{K}$, and $\eta_1, \dots, \eta_r$ a system of fundamental units. (Of course $r = s + t - 1$.) Put

$$\Theta = \{\theta_0\omega \colon \theta_0 \in \Theta_0, \omega \in \Omega\}.$$

Then for any $x \in \mathrm{Sol}(\mathbb{K})$ there exists $\theta(x) \in \Theta$ such that

$$\varphi(x) = \theta(x)\eta_1^{b_1(x)} \cdots \eta_r^{b_r(x)}, \tag{34}$$

with $\boldsymbol{b}(x) = (b_1(x), \dots, b_r(x)) \in \mathbb{Z}^r$.

4.4. Fixed admissible field, θ and $\boldsymbol{k}$

Starting from this point, we fix $\theta \in \Theta$ and $\boldsymbol{k} = (k_1, \dots, k_m) \in \mathcal{P}^m$ and consider the set

$$\mathrm{Sol}(\mathbb{K}, \boldsymbol{k}, \theta) = \{x \in \mathrm{Sol}(\mathbb{K}) : \boldsymbol{k}(x) = \boldsymbol{k}, \theta(x) = \theta\}. \tag{35}$$

As we have seen in the Subsection 4.2, we have to consider only vectors $\boldsymbol{k}$ satisfying

$$k_1 = \cdots = k_s = 0, \tag{36}$$

$$k_i + k_{i+t} \equiv 0 \pmod p \quad (s < i \leqslant s+t). \tag{37}$$

In the case $[\mathbb{K} : \mathbb{K}_0] = p$ we also require that

if $\sigma_{i_1}, \dots, \sigma_{i_p}$ are the p distinct prolongations of a fixed embedding of $\mathbb{K}_0$, then $\{k_{i_1}, \dots, k_{i_p}\} = \mathcal{P}$. (38)

For any $x \in \mathrm{Sol}(\mathbb{K}, \boldsymbol{k}, \theta)$ put

$$\varphi_i(x) = (x - \beta_i)\left(\zeta_i\left(\frac{x - \alpha_i}{x - \beta_i}\right)^{1/p} - 1\right)^p = \sigma_i(\varphi(x)), \tag{39}$$

where $\zeta_i = \zeta^{k_i}$. We also write

$$\begin{aligned} &\theta_i = \sigma_i(\theta), && \eta_{ij} = \sigma_i(\eta_j), \\ &\rho_i = \begin{cases} 1-p, & k_i = 0, \\ 1, & k_i \neq 0, \end{cases} && \gamma_i = \begin{cases} \left(\frac{\beta_i - \alpha_i}{p}\right)^p, & k_i = 0, \\ (\zeta_i - 1)^p, & k_i \neq 0, \end{cases} \end{aligned} \tag{40}$$

where $1 \leqslant i \leqslant m$. Let $A = [a_{ij}]_{1 \leqslant j, i \leqslant r}$ be the inverse for the matrix $[\log|\eta_{ij}|]_{1 \leqslant i, j \leqslant r}$. For $1 \leqslant j \leqslant r$ put

$$\delta_i = \sum_{j=1}^{r} a_{ij}\rho_j, \quad \lambda_i = \sum_{j=1}^{r} (a_{ij} \log|\gamma_j \theta_j^{-1}|). \tag{41}$$

Also, we need some constants

$$\begin{aligned}
&c_2 = 4|2^{-1/p} + (2p)^{-1} - 1|, && c_3 = 2(1 - 2^{-1/p}),\\
&c_4 = 2\sin(\pi/p), && c_5 = \max_{1\leqslant i\leqslant m}\left(|\alpha_i| + |\beta_i|\right),\\
&c_6 = \max_{1\leqslant i\leqslant m}\frac{|\alpha_i|^2+|\beta_i|^2}{|\alpha_i-\beta_i|}, && c_7 = 1.39p\max(c_3c_4^{-1}c_5, pc_2c_6),\\
&c_8 = \max_{1\leqslant j\leqslant r}|\delta_j|, && X_2 = \max(X_1, 2c_3c_4^{-1}c_5, 2pc_2c_6),\\
&c_9 = \tfrac{1}{20} + \max_{1\leqslant j\leqslant r}|\lambda_j|, && c_{10} = c_7\max_{1\leqslant i\leqslant r}\sum_{j=1}^{r}|a_{ij}|,\\
&X_3 = \max(X_2, 20c_{10}).
\end{aligned} \tag{42}$$

PROPOSITION 4.4.1. *Suppose that* $x \in \mathrm{Sol}(\mathbb{K}, \boldsymbol{k}, \theta)$ *and* $|x| > X_2$. *Then*

$$\varphi_i(x) = \gamma_i x^{\rho_i} e^{O_1(c_7|x|^{-1})} \quad (1 \leqslant i \leqslant m), \tag{43}$$

$$b_i(x) = \delta_i \log|x| + \lambda_i + O_1(c_{10}|x|^{-1}) \quad (1 \leqslant j \leqslant r), \tag{44}$$

Also, if $|x| > X_3$ *then*

$$|\boldsymbol{b}(x)|_\infty \leqslant c_8 \log|x| + c_9. \tag{45}$$

(Recall that $b_j(x)$ were defined in the previous section, and $\boldsymbol{b}(x) = (b_1(x), \ldots, b_r(x))$.)

Proof. Let z be a complex number with the condition $|z| \leqslant \frac{1}{2}$. Then

$$(1+z)^{1/p} = 1 + p^{-1}z + O_1(c_2|z|^2) = 1 + O_1(c_3|z|), \tag{46}$$

$$1 + z = e^{O_1(1.39|z|)}. \tag{47}$$

For (47) see [27, p. 106]. For (46), put

$$\psi(z) = z^{-2}((1+z)^{1/p} - 1 - p^{-1}z).$$

Then

$$|\psi(z)| = \left|\sum_{\nu=2}^{\infty}\binom{1/p}{\nu}z^{\nu-2}\right| \leqslant \sum_{\nu=2}^{\infty}\left|\binom{1/p}{\nu}\right|(1/2)^{\nu-2} = |\psi(-1/2)| = c_2,$$

which proves the first equality in (46). The second one can be obtained in the same manner.

As follows from (3), for $|x| \geqslant X_1$ we have

$$\varphi_i(x) = x(\zeta_i(1-\alpha_i x^{-1})^{1/p} - (1-\beta_i x^{-1})^{1/p})^p. \tag{48}$$

When $k_i \neq 0$ we have $\zeta_i \neq 1$ and, moreover, $|\zeta_i - 1| \geqslant c_4$. Therefore

$$\varphi_i(x) = (\zeta_i - 1)^p x(1 + O_1(c_3 c_4^{-1} c_5 |x|^{-1}))^p.$$

Since $|x| \geqslant X_2$, the O_1-term is bounded by $\frac{1}{2}$, and we obtain

$$\varphi_i(x) = \gamma_i x e^{O_1(1.39pc_3c_4^{-1}c_5|x|^{-1})},$$

which proves (43) in the case $k_i \neq 0$.

When $k_i = 0$ we have

$$\varphi_i(x) = \left(\frac{\beta_i - \alpha_i}{p}\right)^p x^{1-p}(1 + O_1(pc_2c_6|x|^{-1}))^p.$$

Again the O_1-term is bounded by $\frac{1}{2}$, and we obtain

$$\varphi_i(x) = \gamma_i x^{1-p} e^{O_1(1.39p^2c_2c_6|x|^{-1})},$$

and (43) is established in the case $k_i = 0$ as well.

Now prove (44). Since

$$\log|\theta_i^{-1}\varphi_i(x)| = b_1(x)\log|\eta_{i1}| + \cdots + b_r(x)\log|\eta_{ir}| \quad (1 \leqslant i \leqslant r), \tag{49}$$

we have

$$b_i(x) = \sum_{j=1}^{r} a_{ij}\log|\theta_j^{-1}\varphi_j(x)| \tag{50}$$

$$= \left(\sum_{j=1}^{r} a_{ij}\rho_j\right)\log|x| + \sum_{j=1}^{r}(a_{ij}\log|\gamma_j\theta_j^{-1}|)$$

$$+O_1\left(c_7|x|^{-1}\sum_{j=1}^{r}|a_{ij}|\right), \tag{51}$$

which is (44). Finally, (45) is a direct consequence of (44). The proposition is proved.

We conclude this subsection observing that in the case

$$\big|\{i\colon k_i(x) = 0\}\big| \neq m/p, \tag{52}$$

an upper bound for the solutions follows already from Proposition 4.4.1. Note that, in view of (38), the inequality (52) can take place only for $\mathbb{K} = \mathbb{K}_0$, and that (52) is always the case when $m \not\equiv 0 \pmod p$.

COROLLARY 4.4.2. *Suppose that* (52) *holds, and put* $\rho' = m - p\,|\{i\colon\, k_i(x) = 0\}|$. *Then any* $x \in \mathrm{Sol}\,(\mathbb{K}, \boldsymbol{k}, \theta)$ *satisfies*

$$|x| \leqslant X_4 := \max(X_2, 3mc_7, e^{1/(3|\rho'|)}\,|\gamma_1 \dots \gamma_m|^{-1/\rho'}\,|\theta_1 \dots \theta_m|^{1/\rho'}). \tag{53}$$

Proof. On the one hand

$$\varphi_1(x) \dots \varphi_m(x) = \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\varphi(x)) = \pm\theta_1 \dots \theta_m. \tag{54}$$

On the other hand,

$$\varphi_1(x) \dots \varphi_m(x) = \gamma_1 \dots \gamma_m x^{\rho_1 + \cdots + \rho_m} e^{O_1(mc_7|x|^{-1})}.$$

Since $\rho_1 + \cdots + \rho_m = \rho'$, the result follows.

4.5. A LARGE UPPER BOUND FOR $|\boldsymbol{b}(x)|_\infty$

In this subsection, assuming that $p \geqslant 3$, $[\mathbb{K} : \mathbb{Q}] \geqslant 3$ and $|x| \geqslant X_3$, we obtain a large upper bound for $|\boldsymbol{b}(x)|$ as a consequence of Baker's theory of linear forms in logarithms. We apply a result of Baker and Wüstholz [4].

THEOREM 4.5.1. [4, p. 20] *Let* $\vartheta_0, \dots, \vartheta_r$ *be complex algebraic numbers distinct from* 0 *and* 1, *and* $\boldsymbol{b} = (b_1, \dots, b_{r+1}) \in \mathbb{Z}^{r+1}$. *Also, let*

$$d \geqslant [\mathbb{Q}(\vartheta_0, \dots, \vartheta_r) : \mathbb{Q}], \tag{55}$$

$$h_i \geqslant \max(h(\vartheta_i), d^{-1}|\log\vartheta_i|, d^{-1}) \quad (0 \leqslant i \leqslant r), \tag{56}$$

where $h(\dots)$ *is the absolute logarithmic height. Then either*

$$\Lambda = \log\vartheta_0 + b_1\log\vartheta_1 + \cdots + b_r\log\vartheta_r + b_{r+1}\pi i = 0, \tag{57}$$

or

$$|\Lambda| \geqslant \exp(-c_{11}\log B). \tag{58}$$

Here $B = \max(|b_1|, \dots, |b_{r+1}|, e)$ *and*

$$c_{11} = 18\pi \cdot 32^{r+4}(r+3)!(r+2)^{r+3}d^{r+3}\log(2d(r+2))h_0 \dots h_r.$$

Remark 4.5.2. The parameters $n, h'(\alpha_1), \dots, h'(\alpha_n), h'(L)$ of the original theorem in [4] correspond in Theorem 4.5.1 to $r+2, h_0, \dots, h_r, \pi/d, \log B$, respectively.

We have slightly modified the statement in [4], to allow inequalities in (55) and (56). It is often much easier (and quicker) to find an upper bound for the degree of a number field or for the height of an algebraic number, than to compute any of them exactly.

LEMMA 4.5.3. *Let z and C_1 be positive real numbers and C_2 an arbitrary real number. Suppose that*

$$z \leqslant C_1 \log z + C_2. \tag{59}$$

Then

$$z \leqslant 2(C_1 \log C_1 + C_2).$$

Proof. This is the case $h = 1$ of Lemma 2.2 from [18].

Now we can obtain an upper bound for $|\boldsymbol{b}(x)|_\infty$. By (21), in the case $[\mathbb{K}:\mathbb{K}_0] = p$ there exist $i_1, i_2 \in \{1, \ldots, m\}$ such that

$$\sigma_{i_1}|_{\mathbb{K}_0} = \sigma_{i_2}|_{\mathbb{K}_0}, \tag{60}$$

$$k_{i_1} \neq 0, \qquad k_{i_2} \neq 0, \qquad k_{i_1} \neq k_{i_2}. \tag{61}$$

It follows from (60) that

$$\alpha_{i_1} = \alpha_{i_2}, \qquad \beta_{i_1} = \beta_{i_2}.$$

In the case $\mathbb{K} = \mathbb{K}_0$ choose i_1 and i_2 such that among the numbers

$$\alpha_{i_1},\ \alpha_{i_2},\ \beta_{i_1},\ \beta_{i_2}, \tag{62}$$

there are at least three distinct. The required choice of i_1 and i_2 is possible by the condition $[\mathbb{K}:\mathbb{Q}] \geqslant 3$.

Let i_1 and i_2 be as defined above. Put

$$\Phi(x) = \frac{\gamma_{i_2}^{\rho_{i_1}} \varphi_{i_1}(x)^{\rho_{i_2}}}{\gamma_{i_1}^{\rho_{i_2}} \varphi_{i_2}(x)^{\rho_{i_1}}}. \tag{63}$$

By the choice of i_1 and i_2, the equation

$$\Phi(x) = 1 \tag{64}$$

has finitely many solutions, which can be easily found in practice (see Appendix C for the details). Now suppose that

$$\Phi(x) \neq 1. \tag{65}$$

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

By (43) we have (assuming $|x| \geqslant X_2$)

$$\Phi(x) = e^{O_1(c_{12}|x|^{-1})}, \tag{66}$$

with $c_{12} = 2pc_7$. On the other hand

$$\Phi(x) = \vartheta_0\vartheta_1^{b_1(x)} \cdots \vartheta_r^{b_r(x)}, \tag{67}$$

where

$$\vartheta_0 = \frac{\gamma_{i_2}^{\rho_{i_1}}\theta_{i_1}^{\rho_{i_2}}}{\gamma_{i_1}^{\rho_{i_2}}\theta_{i_2}^{\rho_{i_1}}}, \qquad \vartheta_j = \frac{\eta_{i_1j}^{\rho_{i_2}}}{\eta_{i_2j}^{\rho_{i_1}}}. \tag{68}$$

Taking the logarithm, we obtain

$$\log\Phi(x) = \log\vartheta_0 + b_1(x)\log\vartheta_1 + \cdots + b_r(x)\log\vartheta_r + b_{r+1}(x)\pi i, \tag{69}$$

for some $b_{r+1}(x) \in \mathbb{Z}$. Comparing the imaginary parts in (69), and using (66), we get

$$|b_{r+1}(x)| \leqslant 1 + |b_1(x)| + \cdots + |b_r(x)| + \pi^{-1}c_{12}|x|^{-1}, \tag{70}$$

$$\leqslant 1 + \pi^{-1}c_{12} + r\,|\boldsymbol{b}(x)|_\infty\,. \tag{71}$$

Apply Theorem 4.5.1 to the right-hand side of (69). Since $\log\Phi(x) \neq 0$, we obtain

$$|\log\Phi(x)| \geqslant \exp(-c_{11}\log B(x)), \tag{72}$$

where

$$\begin{aligned} B(x) &:= \max\left(b_1(x), \ldots, b_r(x), b_{r+1}(x), e\right) \\ &\leqslant 1 + \pi^{-1}c_{12} + r\,|\boldsymbol{b}(x)|_\infty \qquad (73) \\ &\leqslant c_{13}\log|x| + c_{14} \qquad (74) \end{aligned}$$

with $c_{13} = rc_8$ and $c_{14} = \max\left(1 + \pi^{-1}c_{12} + rc_9, e\right)$.

Combining (66) and (72), we obtain

$$\log|x| \leqslant c_{11}\log B(x) + \log c_{12}. \tag{75}$$

Assuming $|x| \geqslant X_3$, we deduce from here that $B(x) \leqslant c_{15}\log B(x) + c_{16}$ with $c_{15} = c_{11}c_{13}$ and $c_{16} = c_{13}c_{12} + c_{14}$. By Lemma 4.5.3 we have

$$|\boldsymbol{b}(x)|_\infty \leqslant B(x) \leqslant B_0 := 2(c_{15}\log c_{15} + c_{16}).$$

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

4.6. Reduction of Baker's bound

4.6.1. *Preliminaries*

In practice, the value of B_0 is too large for directly enumerating all possibilities for $\boldsymbol{b}(x)$. However, B_0 may be significantly reduced by applying an appropriate version of the LLL-reduction algorithm, as described in [27]. We use here (see also [8]) a modification making the reduction process much more efficient; in particular, LLL can be replaced by the classical continued fractions algorithm, as in [3] (see also [33]).

Let j_1 be defined by the condition

$$|\delta_{j_1}| = \max_{1\leqslant j\leqslant r} |\delta_j| = c_8. \tag{76}$$

(Recall that the numbers δ_j are defined in (41).) We have $\delta_{j_1} \neq 0$, because the matrix A is non-degenerated.

The method of reduction we use depends on what we heuristically believe about the mutual arithmetic behaviour of the numbers δ_j and λ_j. We shall distinguish between the following cases.

(1) **Irrational case.** For some $j_2 \in \{1, \dots, r\}$, we believe that the number $\delta_{j_2}\lambda_{j_1} - \delta_{j_1}\lambda_{j_2}$ is not a linear combination of δ_{j_1} and δ_{j_2} with rational coefficients.

(2) **Semirational case.** For some $j_2 \in \{1, \dots, r\}$, we believe that the quotient $\delta_{j_1}^{-1}\delta_{j_2}$ is irrational, but the number $\delta_{j_2}\lambda_{j_1} - \delta_{j_1}\lambda_{j_2}$ is a linear combination of δ_{j_1} and δ_{j_2} with rational coefficients.

(3) **Totally rational case.** We believe that for all $j \in \{1, \dots, r\}$ the numbers $\delta_{j_1}^{-1}\delta_j$ and $\delta_{j_1}^{-1}\left(\delta_j\lambda_{j_1} - \delta_{j_1}\lambda_j\right)$ are rational.

In the first two cases we fix such a j_2 and put

$$\delta = \delta_{j_1}^{-1}\delta_{j_2}, \qquad \lambda = \delta_{j_1}^{-1}\left(\delta_{j_2}\lambda_{j_1} - \delta_{j_1}\lambda_{j_2}\right).$$

By (44) and by the definition of δ and λ one has

$$|b_{j_2}(x) - \delta b_{j_1}(x) + \lambda| \leqslant (1 + |\delta|)c_{10}|x|^{-1} \leqslant 2c_{10}|x|^{-1}, \tag{77}$$

because by the choice of j_1 and j_2 we have $|\delta| \leqslant 1$. Combining this with (45), we obtain

$$|b_{j_2}(x) - \delta b_{j_1}(x) + \lambda| \leqslant c_{18} \exp(-c_{17}|\boldsymbol{b}(x)|_\infty), \tag{78}$$

with $c_{18} = 2c_{10}\exp(c_9/c_8)$ and $c_{17} = c_8^{-1}$.

Notice that in the first two cases $j_1 \neq j_2$, in particular $r \geqslant 2$. On the other hand, the rational case covers the case $r = 1$.

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

4.6.2. *The irrational case*

Choose a not very large number $\kappa > 2$. (We discuss the practical choice of κ in Subsection 4.6.5.) By the theorem of Dirichlet, there exists a positive integer $q \leqslant \kappa B_0$ such that

$$\|q\delta\| \leqslant (\kappa B_0)^{-1}, \tag{79}$$

where $\| \ldots \|$ is the distance to the nearest integer. In practice q can be quickly found from the continuous fraction expansion of δ. Multiplying (78) by q, we obtain

$$\| \pm b_{j_1}(x)\|q\delta\| + q\lambda\| \leqslant c_{18}\kappa B_0 \exp(-c_{17}|\boldsymbol{b}|_\infty), \tag{80}$$

where '$\pm$' should be '$+$' if $q\delta$ is smaller than the nearest integer and '$-$' otherwise.

It follows from (79) that $|b_{j_1}(x)| \cdot \|q\delta\| \leqslant \kappa^{-1}$. Therefore (80) implies that

$$\|q\lambda\| - \kappa^{-1} \leqslant c_{18}\kappa B_0 \exp(-c_{17}|\boldsymbol{b}(x)|_\infty). \tag{81}$$

If $\|q\lambda\| \geqslant 2\kappa^{-1}$, which is heuristically plausible when κ is large enough, then we have a new estimate for $|\boldsymbol{b}(x)|_\infty$

$$|\boldsymbol{b}(x)|_\infty \leqslant c_{17}^{-1}(\log B_0 + \log(c_{18}\kappa^2)), \tag{82}$$

(compare this with the lemma from [3, Section 3]).

The reduced bound for $|\boldsymbol{b}(x)|_\infty$ can be reduced again, using the same procedure, etc.

4.6.3. *The semirational case*

We have

$$q_1 + q_2\delta + q_3\lambda = 0, \tag{83}$$

where q_1, q_2 and q_3 are integers, $q_3 \neq 0$, and $\gcd(q_1, q_2, q_3) = 1$. We expect that the integers q_1, q_2 and q_3 are 'very small' (around 10 or so in absolute value). This was confirmed in all examples we considered.

Multiplying (78) by q_3 and using (83), we obtain

$$|b_{j_2}(x) - q_1 - \delta(b_{j_1}(x) + q_2)| \leqslant |q_3|c_{18} \exp(-c_{17}|\boldsymbol{b}(x)|_\infty).$$

It follows that

$$\min_{b\in\mathbb{Z}, |b|\leqslant B_0+|q_2|} \|b\delta\| \leqslant |q_3|c_{18} \exp(-c_{17}|\boldsymbol{b}(x)|_\infty). \tag{84}$$

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

However, this minimum can be quickly computed using continued fractions, and we expect it to be $(\kappa' B_0)^{-1}$, where κ' is a reasonable number. We conclude that

$$|\boldsymbol{b}(x)|_\infty \leqslant c_{17}^{-1}(\log B_0 + \log(|q_3|c_{18}\kappa')). \tag{85}$$

4.6.4. *The totally rational case*

Since this case requires a rather lengthy case-by-case analysis, and seldom occurs in practice (when $r \geqslant 2$), it is treated in Appendix D.

4.6.5. *The technology of reduction*

When $r \geqslant 2$, we pick $j_2 \neq j_1$ and continue as if it were irrational case. We take as a starting value $\kappa = 10$, and try the first reduction. When it is $\|q\lambda\| < 2\kappa^{-1}$, we change κ by 10κ and repeat the process. In most of the cases we obtained successful reduction in two or three iterations at most.

When we do not obtain successful reduction after seven-eight iterations of κ, we conclude that probably γ is a linear combination of 1 and δ with rational coefficients. This can be easily verified (see the second comment in Subsection 4.6.6), and this guess was always confirmed. Now if δ is irrational then we continue as in the semirational case. If δ is rational, then we redefine j_2 and repeat the process.

If δ and γ are rational for all possible j_2 then we are in the totally rational case, see Appendix D.

When $r = 1$ we are in the totally rational case from the very beginning.

4.6.6. *Computational comments*

(1) Since in practice we deal with approximate values of δ and λ, we usually obtain, instead of (83), an inequality of the form

$$|q_1 + q_2\delta + q_3\lambda| \leqslant \varepsilon, \tag{86}$$

where ε is a very small positive number ($\varepsilon = 10^{-20}B_0^{-2}$ is typical). Though we do believe that, whenever (86) is detected with small integers q_i, it corresponds to the actual equality (83), we do not prove this, and in fact we do not need this: (86) is completely sufficient for our purposes.

For simplicity of exposition we assumed the exact equality (83) in our treatment of the semirational case. However, in real computations we used (86), with all constant correspondingly modified.

The similar convention applies to the totally rational case.

(2) It is very easy to verify whether (86) holds with small integers q_i. One has to find, using the three-dimensional LLL, the (almost) shortest vector of the lattice generated by $(C, [C\delta], [C\lambda])$, $(0, 1, 0)$ and $(0, 0, 1)$, where C is a sufficiently large positive integer (we used $C = 10^{10}$).

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

We refer to [8, Subsection 2.4.3] for further computational details and other subtleties.

4.7. Final enumeration

Unfortunately, the reduced bound B_0' may also be too large for the direct enumeration, because one has to check $(2B_0'+1)^r$ possibilities for the vector $\boldsymbol{b}(x)$. One can imagine several ways to overcome this difficulty, for instance:

- sieving modulo several primes, as in [28] and [23];
- use of Fincke–Pohst algorithm for finding all short vectors in a lattice, as in [30] and [28].

In [6, 8] one further approach to final enumeration was proposed, based on the inequality (77). In the present paper we use a more efficient version of this method. For $1 \leqslant j \leqslant r$ put

$$b_j'(x) = \delta_{j_1}^{-1}\delta_j b_{j_1}(x) - \delta_{j_1}^{-1}\left(\delta_j\lambda_{j_1} - \delta_{j_1}\lambda_j\right), \tag{87}$$

where j_1 is defined from (76). Then, replacing in (77) index j_2 by j, we rewrite it as $|b_j(x) - b_j'(x)| \leqslant 2c_{10}|x|^{-1}$. Since $X_3 \geqslant 20c_{10}$, we obtain

$$|b_j(x) - b_j'(x)| < 0.1 \quad (1 \leqslant j \leqslant r) \tag{88}$$

as soon as $|x| > X_3$. In particular,

$$\|b_j'(x)\| < 0.1 \quad (1 \leqslant j \leqslant r). \tag{89}$$

Now we do as follows. For every integer b such that $|b| \leqslant B_0'$, compute the real numbers $b_j' := \delta_{j_1}^{-1}\delta_j b - \delta_{j_1}^{-1}\left(\delta_j\lambda_{j_1} - \delta_{j_1}\lambda_j\right)$, and for each j, check for the condition $\|b_j'\| < 0.1$. This condition trivially holds for $j = j_1$, but for $j \neq j_1$ it needs not. *If it is false for at least one j, then there is no solution x with $|x| > X_3$ such that* $b_{j_1}(x) = b$, and we go to the next b.

The heuristic probability that the integer b passes this severe test is 5^{1-r}, quite a small number (when $r \geqslant 2$). For those very few b that survive after the test, we used the second test, based on Lemma 4.7.1 below.

Fix i such that $k_i \neq 0$. For $x \in \mathbb{Z}$ put

$$\omega_i(x) := \gamma_i^{-1}\varphi_i(x) - \gamma_i',$$

where $\gamma_i' = \beta_i - \zeta_i\alpha_i/\zeta_i - 1$. Also, put

$$\begin{aligned}
c_{19} &= 4(\tfrac{3}{2})^p - 4 - 2p, & c_{20} &= c_2(|\alpha_i|^2 + |\beta_i|^2)|\zeta_i - 1|^{-1},\\
c_{21} &= p^{-1}|\gamma_i'| + c_{20}X_3^{-1}, & c_{22} &= c_{21}X_3^{-1},\\
c_{23} &= c_{19}c_{21} + pc_{20}, & X_5 &= \max(X_3, 2c_{22}, 2c_{23}).
\end{aligned}$$

LEMMA 4.7.1. *If* $|x| > X_5$ *then*

$$|x - \omega_i(x)| < \min(\tfrac{1}{2}, c_{23}/(|\omega_i(x)| - \tfrac{1}{2})). \tag{90}$$

Proof. For $|z| \leqslant \frac{1}{2}$ we have

$$(1+z)^p = 1 + pz + O(c_{19}z^2), \tag{91}$$

which can be proved in the same manner as (46). As follows from (91), (46) and (48), for $|x| > X_3$ we have

$$\begin{aligned}\varphi_i(x) &= \gamma_i x(1 + \gamma_i' x^{-1}/p + O_1(c_{20}x^{-2}))^p,\\ &= \gamma_i x(1 + \gamma_i' x^{-1} + O_1(c_{23}x^{-2})),\end{aligned}$$

which yields

$$|x - \omega_i| \leqslant c_{23}x^{-1}. \tag{92}$$

Since $|x| > 2c_{23}$, this proves $|x - \omega_i| < \frac{1}{2}$. In particular, $|\omega_i(x)| < |x| + \frac{1}{2}$, which together with (92) yields $|x - \omega_i(x)| < c_{23}/(|\omega_i(x)| - \frac{1}{2})$. This proves the lemma.

The second test is: If $\omega_i = \omega_i(x)$ for a solution x with $|x| > X_5$ then

$$|\omega_i| > X_5 - \tfrac{1}{2} \quad \text{and} \quad \|\omega_i\| < c_{23}/(|\omega_i(x)| - \tfrac{1}{2}). \tag{93}$$

We computed $b_1, \ldots, b_r$ as the nearest integers to $b_1', \ldots, b_r'$, respectively, and verified whether

$$\omega_i := \gamma_i^{-1}\theta_i\eta_{i1}^{b_1}\cdots\eta_{ir}^{b_r} - \gamma_i' \tag{94}$$

satisfied (93). If it did, we put x to be the nearest integer to ω_i and checked whether it is a solution, just substituting it to the Equation (1).

4.8. The algorithm

We summarize the contents of this section in the following algorithm for complete solution of the superelliptic Equation (1), where $p \geqslant 3$.

Step 1. Construct a complete system of admissible fields, as described in Subsection 4.1.

Step 2. Fix an admissible field $\mathbb{K}$ not considered yet. If all admissible fields have already been considered, go to Step 10.

Step 3. Construct the set Θ, as described in Subsection 4.2.

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

Step 4. Fix $\theta \in \Theta$ and $\boldsymbol{k} \in \mathcal{P}^m$ (subject to restrictions formulated in the beginning of Subsection 4.4). If all possible pairs $(\theta, \boldsymbol{k})$ have already been considered, go to Step 2.

Step 5. If (52) holds, compute X_4 and go to Step 4. Otherwise, compute X_3 and go to the next step.

Step 6. Construct the function $\Phi(x)$ and find all integral solutions of (64). For each of the latter check whether it is a solution of (1).

Step 7. Compute Baker's bound B_0.

Step 8. Find the reduced bound B_0', as described in Subsection 4.6.

Step 9. Final enumeration (see Subsection 4.7).
Go to Step 4.

Step 10. Find X_6 as the maximum of all X_4, computed at Step 5, and all X_5, computed at Step 9.[4]

Step 11. For any $x \in \mathbb{Z}$ such that $|x| \leqslant X_6$ check whether x is a solution of (1).

Step 12. Collect all solutions obtained at Steps 6, 9, and 11.

Step 13. End.

Note in conclusion that we should be able to perform the operations (PD), (U), (CG) in the fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$, and the operations (PD), (U), (PI) in any admissible field $\mathbb{K}$ constructed on the Step 1 of the algorithm. The last demand seems to be the most difficult point of the proposed method. Indeed, the maximal degree of admissible fields will be $pn(n-1)$ in the worst case. Even for $(p, n) = (3, 4)$ we shall have to perform 'multiplicative' operations in fields of degree 36 (in the worst case), which is beyond the possibilities of the Algorithmic Algebraic Number Theory at its present state.

In the next section we shall see how to reduce the degrees of the fields occurring in the process of solution.

5. The (α, β)-symmetry

In this section we assume that $p \geqslant 3$.

5.1. Preliminary preparations

We say that we have an (α, β)-*symmetry* if there exists an automorphism of $\mathbb{Q}(\alpha, \beta)$ sending α to β and β to α. The roots α and β are called in this case *symmetric*. We shall see that, in the case of (α, β)-symmetry, the field $\mathbb{Q}(\alpha, \beta)$ can be replaced by

[4] If the totally rational case occurred (see Appendix D), then one should also take into account X_7 and X_8.

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

$\mathbb{Q}(\alpha+\beta, \alpha\beta)$. Our considerations will be based on the following lemma.

LEMMA 5.1.1. *Let $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2$ be a tower of number fields with the following properties*

$$[\mathbb{K}_1 : \mathbb{K}_0] = 2 \quad \textit{and} \quad [\mathbb{K}_2 : \mathbb{K}_1] = p,$$

$$\mathbb{K}_2 = \mathbb{K}_1(\nu),$$

where $\nu^p = \mu \in \mathbb{K}_1$ and μ is conjugate to μ^{-1} over $\mathbb{K}_0$. Then

(a) $[\mathbb{K}_0(\nu+\nu^{-1}) : \mathbb{K}_0] = p$.
Furthermore, let $\mathbb{K}$ be a number field such that $\mathbb{K}_0 \subset \mathbb{K} \subset \mathbb{K}_2$ and $[\mathbb{K} : \mathbb{K}_0] = p$. Then

(b) *if $\zeta \notin \mathbb{K}_0$ then $\mathbb{K} = \mathbb{K}_0(\nu+\nu^{-1})$;*

(c) *if $\zeta \in \mathbb{K}_0$ then $\mathbb{K}$ is one of the p distinct fields $\mathbb{K}_0(\zeta^k\nu + \zeta^{-k}\nu^{-1})$, where $k \in \mathcal{P}$;*

(d) *the composite $\mathbb{K}_1\mathbb{K}$ is $\mathbb{K}_2$.*

Proof. Clearly, $\mathbb{K}_2 = \mathbb{K}_0(\nu)$. Further, ν and ν^{-1} are conjugate over $\mathbb{K}_0$. Define the automorphism $\tau\colon \mathbb{K}_2 \to \mathbb{K}_2$ by $\tau(\nu) = \nu^{-1}$. Then $\nu + \nu^{-1}$ is stable with respect to τ, whence the degree $[\mathbb{K}_0(\nu+\nu^{-1}) : \mathbb{K}_0]$ divides p. This proves (a), because $\nu + \nu^{-1} \notin \mathbb{K}_0$. (If it were $\nu + \nu^{-1} \in \mathbb{K}_0$, then we would have had $[\mathbb{K}_2 : \mathbb{K}_0] = [\mathbb{K}_0(\nu) : \mathbb{K}_0] \leqslant 2$, a contradiction).

Assertion (d) is obvious: since p is odd, we have $\mathbb{K}_1 \not\subset \mathbb{K}$, whence $\mathbb{K} \subsetneqq \mathbb{K}_1\mathbb{K} \subseteq \mathbb{K}_2$, and the single option is $\mathbb{K}_1\mathbb{K} = \mathbb{K}_2$.

To prove (b) and (c) note that the fields $\mathbb{K}$ correspond to non-trivial involutions of $\mathbb{K}_2$ over $\mathbb{K}_0$, i.e. automorphisms $\tau\colon \mathbb{K}_2 \to \mathbb{K}_2$ satisfying

$$\tau \neq \mathrm{id}, \quad \tau^2 = \mathrm{id}, \quad \tau|_{\mathbb{K}_0} = \mathrm{id}_{\mathbb{K}_0}.$$

The conjugates of ν over $\mathbb{K}_0$ are among the numbers

$$\nu, \zeta\nu, \ldots, \zeta^{p-1}\nu, \nu^{-1}, \zeta\nu^{-1}, \ldots, \zeta^{p-1}\nu^{-1}. \tag{95}$$

Since $[\mathbb{K}_0(\nu) : \mathbb{K}_0] = 2p$, all the numbers (95) are conjugate to ν over $\mathbb{K}_0$.

We distinguish between three cases.

(b)′ $\zeta \notin \mathbb{K}_1$. Then, among the conjugates of ν over $\mathbb{K}_0$, only ν^{-1} belongs to $\mathbb{K}_2$. Hence the unique involution of $\mathbb{K}_2$ over $\mathbb{K}_0$ is the one taking ν to ν^{-1}, and the single possibility for $\mathbb{K}$ is $\mathbb{K}_0(\nu+\nu^{-1})$.

(b)″ $\zeta \in \mathbb{K}_1 \backslash \mathbb{K}_0$. In this case all the numbers (95) belong to $\mathbb{K}_2$. Hence $\mathbb{K}_2$ is normal over $\mathbb{K}_0$ and the group $\mathcal{G} := \mathrm{Gal}(\mathbb{K}_2/\mathbb{K}_0)$ is generated by $\tau\colon \nu \to \nu^{-1}$ and $\sigma\colon \nu \to \zeta\nu$. Clearly, $\tau|_{\mathbb{K}_1}$ is the non-trivial involution of $\mathbb{K}_1/\mathbb{K}_0$, whence $\tau(\zeta) = \zeta^{-1}$. Therefore $\tau\sigma = \sigma\tau$, whence $\mathcal{G}$ is abelian, and again τ is the unique involution of $\mathbb{K}_2/\mathbb{K}_0$.

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

(c) $\zeta \in \mathbb{K}_0$. In this case $\tau\sigma = \sigma^{-1}\tau$, and there are exactly p distinct involutions $\tau_k := \sigma^k\tau\sigma^{-k}$, where $k \in \mathcal{P}$. Indeed, the involutions τ_k are pairwise distinct because the numbers $\tau_k(\nu) = \zeta^{-2k}\nu$ are distinct for distinct $k \in \mathcal{P}$. Further, by the theorem of Sylow, all two-element subgroups of $\mathcal{G}$ are conjugate. Since there are at most $[\mathcal{G}\colon \{1, \tau\}] = p$ subgroups conjugate to $\{1, \tau\}$, there are no involutions other than $\tau_0 = \tau, \tau_1, \ldots, \tau_{p-1}$. The involutions τ_k correspond to the p distinct fields $\mathbb{K}_0(\zeta^k\nu + \zeta^{-k}\nu^{-1})$, which completes the proof.

The lemma is proved.

5.2. Admissible fields

In the case of (α, β)-symmetry we define admissible fields in a way different from the general case. We put $\mathbb{K}_0' = \mathbb{Q}(\alpha, \beta)$ and let $\tau\colon \mathbb{K}_0' \to \mathbb{K}_0'$ be defined by $\tau(\alpha) = \beta$, $\tau(\beta) = \alpha$. Put $\mathbb{K}_0 = \mathbb{Q}(\alpha + \beta, \alpha\beta) = (\mathbb{K}_0')^\tau$.

DEFINITION 5.2.1. A number field $\mathbb{K}$ is *admissible* for a solution x if for some $k \in \mathcal{P}$ we have

$$\mathbb{K} = \mathbb{K}_0\left(\zeta^k\left(\frac{x-\alpha}{x-\beta}\right)^{1/p} + \zeta^{-k}\left(\frac{x-\alpha}{x-\beta}\right)^{-1/p}\right).$$

A *complete system* of admissible fields and a *minimal complete system* are defined as in Subsection 4.1.

Let M be the finite subset of $\mathbb{Q}(\alpha, \beta)$ defined in (16) and (17).

PROPOSITION 5.2.2. *The fields* $\mathbb{K}_0$ *and* $\mathbb{K}_0(\mu^{1/p} + \mu^{-1/p})$, *where* μ *runs* M, *form a complete system of admissible fields.*

Proof. Suppose first that

$$\zeta^k\left(\frac{x-\alpha}{x-\beta}\right)^{1/p} \in \mathbb{K}_0',$$

for some $k \in \mathcal{P}$. We shall see that in this case $\mathbb{K}_0$ is admissible for the solution x. We have

$$\tau\left(\zeta^k\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\right) = \zeta^{k'}\left(\frac{x-\alpha}{x-\beta}\right)^{-1/p},$$

for some $k' \in \mathcal{P}$. Therefore

$$\zeta^{k+k'} = \mathcal{N}_{\mathbb{K}_0'/\mathbb{K}_0}\left(\zeta^k\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\right) \in \mathbb{K}_0.$$

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

If $\zeta \notin \mathbb{K}_0$ then $k' = -k$, whence

$$\zeta^k \left(\frac{x-\alpha}{x-\beta}\right)^{1/p} + \zeta^{-k} \left(\frac{x-\alpha}{x-\beta}\right)^{-1/p} = \mathrm{Tr}_{\mathbb{K}_0'/\mathbb{K}_0} \left(\zeta^k \left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\right) \in \mathbb{K}_0. \qquad (96)$$

When $\zeta \in \mathbb{K}_0$ we define $k'' \in \mathcal{P}$ by $2k'' = k - k' \pmod p$. Then

$$\begin{aligned}\tau\left(\zeta^{k''}\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\right) &= \zeta^{k''-k}\tau\left(\zeta^k\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\right)\\ &= \zeta^{k''-k}\zeta^{k'}\left(\frac{x-\alpha}{x-\beta}\right)^{-1/p}\\ &= \zeta^{-k''}\left(\frac{x-\alpha}{x-\beta}\right)^{-1/p},\end{aligned}$$

and we obtain (96) with k'' instead of k.

Now suppose that

$$\left[\mathbb{K}_0'\left(\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\right) : \mathbb{K}_0'\right] = p.$$

Then

$$\zeta^k\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\mu^{-1/p} \in \mathbb{K}_0',$$

for some $k \in \mathcal{P}$ and $\mu \in \mathrm{M}$. We shall see that the field $\mathbb{K} = \mathbb{K}_0(\mu^{1/p} + \mu^{-1/p})$ is admissible for x. By Lemma 5.1.1(a)

$$\left[\mathbb{K}_0\left(\zeta^k\left(\frac{x-\alpha}{x-\beta}\right)^{1/p} + \zeta^{-k}\left(\frac{x-\alpha}{x-\beta}\right)^{-1/p}\right) : \mathbb{K}_0\right] = [\mathbb{K} : \mathbb{K}_0] = p.$$

If $\zeta \notin \mathbb{K}_0$ then by Lemma 5.1.1(b) we have

$$\mathbb{K}_0\left(\zeta^k\left(\frac{x-\alpha}{x-\beta}\right)^{1/p} + \zeta^{-k}\left(\frac{x-\alpha}{x-\beta}\right)^{-1/p}\right) = \mathbb{K}.$$

If $\zeta \in \mathbb{K}_0$ then by Lemma 5.1.1(c) the field $\mathbb{K}$ coincides with one of the p fields

$$\mathbb{K}_0\left(\zeta^{k'}\left(\frac{x-\alpha}{x-\beta}\right)^{1/p} + \zeta^{-k'}\left(\frac{x-\alpha}{x-\beta}\right)^{-1/p}\right),$$

where $k' \in \mathcal{P}$. The proposition is proved.

5.3. A FIXED ADMISSIBLE FIELD

Fix an admissible field $\mathbb{K}$ from the complete system constructed in the previous subsection and define m, s, t, and σ_i as in the first paragraph of Subsection 4.2. In particular

$$\sigma_i(\gamma) = \overline{\sigma_{i+t}(\gamma)} \quad (s+1 \leqslant i \leqslant s+t), \tag{97}$$

for any $\gamma \in \mathbb{K}$.

Denote by $\mathbb{K}'$ the composite $\mathbb{K}_0'\mathbb{K}$. Then $[\mathbb{K}' : \mathbb{K}] = 2$, and the involution τ: $\mathbb{K}_0' \to \mathbb{K}_0'$ (defined in the beginning of the previous section) can be prolonged to the involution of $\mathbb{K}'/\mathbb{K}$, which will be also denoted by τ. (Thus, starting from this point, τ: $\mathbb{K}' \to \mathbb{K}'$ is the involution of $\mathbb{K}'$ satisfying $\tau|_{\mathbb{K}} = \mathrm{id}$.)

Further, there are exactly two prolongations of σ_i to the field $\mathbb{K}'$. We fix one of them, also denoting it by σ_i; then the other is $\sigma_i\tau$. The prolongations can be defined to satisfy (97) also for $\gamma \in \mathbb{K}'$. Having prolonged σ_i to $\mathbb{K}'$, we can define α_i and β_i as in the beginning of Subsection 4.2.

We say that a real embedding of $\mathbb{K}$ is *stable* if it has real prolongations to $\mathbb{K}'$, and *unstable* otherwise. Arrange $\sigma_i, \ldots, \sigma_s$ so that $\sigma_1, \ldots, \sigma_{s'}$ are stable, while $\sigma_{s'+1}, \ldots, \sigma_s$ are not. Then we have the following analogue of Proposition 4.2.1 (the proof is immediate).

PROPOSITION 5.3.1. *Each stable real embedding of* $\mathbb{K}_0$ *has exactly one real prolongation to* $\mathbb{K}$, (*which is stable as well*) *and* $p-1/2$ *pairs of complex conjugate prolongations. Each unstable real embedding of* $\mathbb{K}_0$ *has* p *real prolongation to* $\mathbb{K}$, *all of them being unstable. In particular,* $s' = s_0'$, $s - s' = p(s_0 - s_0')$ *and* $t = pt_0 + \frac{p-1}{2}s_0'$, *where* s_0, s_0' *and* $2t_0$ *are the numbers of real, stable real, and complex embeddings of* $\mathbb{K}_0$, *respectively.*

Again, denote by $\mathrm{Sol}(\mathbb{K})$ the set of $x \in \mathrm{Sol}$ such that $\mathbb{K}$ is admissible for x. For any $x \in \mathrm{Sol}(\mathbb{K})$ there exists $k(x) \in \mathcal{P}$ such that

$$\zeta^{k(x)} \left(\frac{x-\alpha}{x-\beta}\right)^{1/p} \in \mathbb{K}'.$$

Since σ_i are prolonged to $\mathbb{K}'$, the numbers

$$\sigma_i\left(\zeta^{k(x)} \left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\right)$$

are well-defined. As in the general case, we define $\boldsymbol{k}(x) = (k_1(x), \ldots, k_m(x))$ from the relation (18).

Again, as in the general case, we have (20) and (21). However, (19) should be relaxed as follows

$$k_1(x) = \cdots = k_{s'}(x) = 0. \tag{19$'$}$$

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

As in the general case, it is easy to observe from Proposition 5.3.1 and relations (19′), (20), and (21), that there are at most $(2^{p-1/2}(p-1/2)!)^{s'_0}(p!)^{t_0+s_0-s'_0}$ possibilities for $\boldsymbol{k}(x)$.

5.4. FUNCTION $\varphi(x)$, ETC.

Define $\varphi(x)$ as in (22). Though $\varphi(x)$ is merely in $\mathbb{K}'$, its square $\varphi^2(x)$ belongs to $\mathbb{K}$. To see this, notice first of all that

$$\zeta^{k(x)}\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}+\zeta^{-k(x)}\left(\frac{x-\alpha}{x-\beta}\right)^{-1/p}\in\mathbb{K}$$

and

$$\zeta^{k(x)}\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\cdot\zeta^{-k(x)}\left(\frac{x-\alpha}{x-\beta}\right)^{-1/p}=1\in\mathbb{K}.$$

Hence

$$\zeta^{k(x)}\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\quad\text{and}\quad\zeta^{-k(x)}\left(\frac{x-\alpha}{x-\beta}\right)^{-1/p}$$

are conjugate over $\mathbb{K}$, which means that

$$\tau\left(\zeta^{k(x)}\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}\right)=\zeta^{-k(x)}\left(\frac{x-\alpha}{x-\beta}\right)^{-1/p}.$$

Therefore

$$\begin{aligned}\varphi^2(x) &= -\ (x-\beta)\left(\zeta^{k(x)}\left(\frac{x-\alpha}{x-\beta}\right)^{1/p}-1\right)^p\\ &\qquad\times(x-\alpha)\left(\zeta^{-k(x)}\left(\frac{x-\alpha}{x-\beta}\right)^{-1/p}-1\right)^p\\ &= -\ \varphi(x)\tau(\varphi(x))\in\mathbb{K}.\end{aligned}$$

Now we have to repeat the material of Subsections 4.3–4.8, just replacing $\varphi(x)$ by $\varphi^2(x)$, and modifying accordingly the arguments and the constants. An interested reader can find in Appendix A the complete list of all required changes.

5.5. A FINAL REMARK

In the case of (α,β)-symmetry one should deal, in the worst situation, with fields of degree $\frac{1}{2}pn(n-1)$. The following proposition shows that, whether there is (α,β)-symmetry or not, only fields of degree at most $\frac{1}{2}pn(n-1)$ are to be considered.

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

PROPOSITION 5.5.1. *Let $f(x) \in \mathbb{Q}(x)$ have at least two distinct roots. Then either*

(i) *there exist two distinct roots α, β of $f(x)$ with (α, β)-symmetry, or*

(ii) *there exist two distinct roots α, β of $f(x)$ such that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leqslant \frac{1}{2}n(n-1)$, where $n = \deg f$.*

Proof. Only the case of irreducible f need to be considered. Let $\mathcal{G}$ be the Galois group of the polynomial f over $\mathbb{Q}$. If $|\mathcal{G}|$ is even, then there exists an element $\tau \in \mathcal{G}$ of order 2. Since $\tau \neq \mathrm{id}$, there is a root α such that $\beta = \tau(\alpha) \neq \alpha$. Since $\tau^2 = \mathrm{id}$, we obtain $\tau(\beta) = \alpha$, whence we have (i).

Now suppose that $|\mathcal{G}|$ is odd. Fix a root α. Then $g(x) = f(x)/(x - \alpha)$ is reducible over $\mathbb{Q}(\alpha)$; otherwise $n(n-1)$ would divide $|\mathcal{G}|$, which is impossible. Let now g_1 be an irreducible over $\mathbb{Q}(\alpha)$ factor of g of the smallest degree. Then $\deg g_1 \leqslant \frac{1}{2}(n-1)$, and for any root β of g_1 we have (ii). The proposition is proved.

Thus, in any case multiplicative operations should be performed in fields of degree at most $\frac{1}{2}pn(n-1)$. In particular cases this bound can be reduced. For example, if $f(x)$ has two symmetric roots, generating the same field over $\mathbb{Q}$ (as in the examples below), then fields of degree at most $\frac{1}{2}pn$ are to be dealt with.

6. Examples

To illustrate the efficiency of our method, we have completely solved two concrete superelliptic Diophantine equations. The computations were performed by a program written in C, using the PARI/GP programming library, version 1.917. Its listing can be obtained by e-mail from the second author.

6.1. THE EQUATION $y^3 = x^4 - x^3 - 3x^2 + x + 1$

The roots of $f(x) = x^4 - x^3 - 3x^2 + x + 1$ are

$$\frac{1+\sqrt{5}}{4} \pm \frac{1}{2}\sqrt{\frac{11+\sqrt{5}}{2}}, \quad \frac{1-\sqrt{5}}{4} \pm \frac{1}{2}\sqrt{\frac{11-\sqrt{5}}{2}}.$$

We take

$$\alpha = \frac{1-\sqrt{5}}{4} - \frac{1}{2}\sqrt{\frac{11-\sqrt{5}}{2}} = -1.355674\ldots,$$

$$\beta = \frac{1-\sqrt{5}}{4} + \frac{1}{2}\sqrt{\frac{11-\sqrt{5}}{2}} = 0.737640\ldots = \alpha^3 - \alpha^2 - 3\alpha + 1.$$

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

We have the (α, β)-symmetry, and

$$\begin{aligned}\mathbb{K}_0 &= \mathbb{Q}(\sqrt{5}), \quad \mathbb{K}_0' = \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha).\\ \mathrm{M} &= \{42\alpha^3 - 102\alpha^2 + 9\alpha + 32, 23\alpha^3 - 55\alpha^2 + 5\alpha + 17, \alpha^2,\\ &\quad 6\alpha^3 - 10\alpha^2 + 3, 3\alpha^3 - 6\alpha^2 + 2, 2\alpha^3 - 4\alpha^2 - \alpha + 2,\\ &\quad \alpha^3 + 3\alpha^2 - \alpha - 1, -2\alpha^3 + 4\alpha^2 + \alpha - 2,\\ &\quad -12\alpha^3 + 29\alpha^2 - 4\alpha - 8\}.\end{aligned}$$

A system of fundamental units of $\mathbb{K}_0'$ is given by

$$\alpha^3 - \alpha^2 - 2\alpha, \alpha, \alpha^3 - 2\alpha^2 - \alpha + 1.$$

For the admissible fields and data in them see Table II. (We write the fields as $\mathbb{Q}(\lambda)$, and express their elements in terms of the generator λ.)

We had $X_6 = 295$, and (the worst value of) Baker's bound B_0 was 6.18×10^{29}. After the first reduction we obtained $B_0 \leqslant 321$, after the second reduction we had $B_0 \leqslant 96$, and after the final reduction step it was $B_0 \leqslant 52$ (there were at most 5 reduction steps at each case).

The solutions are $(-1, -1)$, $(0, 1)$, $(1, -1)$, $(2, -1)$.

The total computational time on a PC Pentium Pro was 1 minute.

6.2. THE EQUATION $28y^3 = x^4 - 20x^2 - 32x + 28$

The roots of $f(x) = x^4 - 20x^2 - 32x + 28$ are

$$2\sqrt{2} \pm \sqrt{2 + 2\sqrt{2}}, \quad -2\sqrt{2} \pm \sqrt{2 - 2\sqrt{2}}$$

and we put

$$\alpha = 2\sqrt{2} - \sqrt{2 + 2\sqrt{2}}, \quad \beta = 2\sqrt{2} + \sqrt{2 + 2\sqrt{2}}.$$

We again have the (α, β)-symmetry, and

$$\mathbb{K}_0 = \mathbb{Q}(\sqrt{2}), \quad \mathbb{K}_0' = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha).$$

Though the set M included 18 elements, there were only 4 admissible fields (together with $\mathbb{K}_0$).

We had $X_6 = 873$, and (the worst value of) Baker's bound B_0 was 8.29×10^{35}. After the first reduction we obtained $B_0 \leqslant 233$, and after the final reduction step it was $B_0 \leqslant 56$ (again, there were at most 5 reduction steps at each case).

The solutions are $(-2, 1)$, $(0, 1)$.

The computation took 6 minutes on a PC Pentium Pro.

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

Table II. Admissible fields and data for $y^3 = x^4 - x^3 - 3x^2 + x + 1$

minimal polynomial of λ	fundamental units	the set Θ_0
$\lambda^2 - \lambda - 1$	λ	$1, \lambda - 6, 26\lambda - 11, -141\lambda + 92,$ $-\lambda - 5, 26\lambda - 15, -141\lambda + 49$
$\lambda^6 + 6\lambda^4 - \lambda^3 +$ $9\lambda^2 - 3\lambda - 1$	$\lambda^3 + 3\lambda, \lambda,$ $\lambda^5 + \lambda^4 + 6\lambda^3 +$ $\lambda^2 + 10\lambda - 6$	$2\lambda^5 + 9\lambda^3 - \lambda^2 + 12\lambda - 3,$ $\lambda^3 + 3\lambda + 5, -\lambda^4 + 2\lambda + 6$ $2\lambda^5 + 12\lambda^3 - \lambda^2 + 21\lambda$ $\lambda^3 + 3\lambda - 6$
$\lambda^6 - 6\lambda^4 - 7\lambda^3 +$ $9\lambda^2 + 21\lambda - 19$	$1/5\lambda^3 - 3/5\lambda - 1/5,$ $1/5\lambda^4 - 1/5\lambda^3 - 3/5\lambda^2 -$ $8/5\lambda + 11/5,$ $1/5\lambda^5 + 1/5\lambda^4 - 3/5\lambda^3 -$ $9/5\lambda^2 - 1/5\lambda + 2$	$-3/5\lambda^5 - 1/5\lambda^4 + 12/5\lambda^3 + 21/5\lambda^2 + 17/5\lambda - 23/5,$ $-1/5\lambda^3 + 3/5\lambda + 31/5,$ $-2/5\lambda^5 - 4/5\lambda^4 + 11/5\lambda^3 + 29/5\lambda^2 + 9/5\lambda - 13,$ $1/5\lambda^3 - 3/5\lambda - 31/5, \ -3/5\lambda^5 - \lambda^4 + 17/5\lambda^3 +$ $43/5\lambda^2 + 16/5\lambda - 48/5, 9\lambda^2 + 3/5\lambda - 52/5,$ $3/5\lambda^5 + 4/5\lambda^4 - 16/5\lambda^3 - 9\lambda^2 - 3/5\lambda + 52/5,$ $-\lambda^5 - 2/5\lambda^4 + 23/5\lambda^3 + 41/5\lambda^2 + 13/5\lambda - 58/5,$ $-4/5\lambda^5 - 2/5\lambda^4 + 17/5\lambda^3 + 9\lambda^2 - 3/5\lambda - 13,$ $8/5\lambda^5 + 2\lambda^4 - 38/5\lambda^3 - 98/5\lambda^2 - 33/5\lambda + 154/5,$ $-1/5\lambda^5 + \lambda^3 + 11/5\lambda^2 + 4/5\lambda + 8/5, 1/5\lambda^3 - 3/5\lambda + 24/5$ $-1/5\lambda^5 - 2/5\lambda^4 + 2\lambda^3 + 17/5\lambda^2 - 14/5\lambda - 37/5,$ $-\lambda^5 - \lambda^4 + 22/5\lambda^3 + 11\lambda^2 + 29/5\lambda - 77/5,$ $-\lambda^5 - 7/5\lambda^4 + 23/5\lambda^3 + 61/5\lambda^2 + 18/5\lambda - 103/5,$ $-6/5\lambda^3 + \lambda^2 + 23/5\lambda - 4/5$
$\lambda^6 - 3\lambda^4 - 3\lambda^3 -$ $9\lambda^2 - 18\lambda - 9$	$1/3\lambda^5 - 1/3\lambda^4 - 2/3\lambda^3 - 3\lambda - 3,$ $\lambda + 1$ $1/3\lambda^4 - 2/3\lambda^3 - \lambda - 1,$	$-4/3\lambda^5 + 7/3\lambda^4 + 2/3\lambda^3 + 10\lambda + 8,$ $1/3\lambda^5 - 1/3\lambda^4 - 2/3\lambda^3 - 3\lambda + 2$ $13/3\lambda^5 - 11/3\lambda^4 - 29/3\lambda^3 - 5\lambda^2 - 36\lambda - 52,$ $1/3\lambda^5 - 2/3\lambda^4 + \lambda^3 - \lambda^2 - 4\lambda - 4,$ $1/3\lambda^5 - 1/3\lambda^4 - 2/3\lambda^3 - 3\lambda - 9$
$\lambda^6 + 3\lambda^4 - 5\lambda^3 -$ $9\lambda^2 + 5$	$9/53\lambda^5 + 3/53\lambda^4 + 28/53\lambda^3 -$ $18/53\lambda^2 - 87/53\lambda - 29/53,$ $3/53\lambda^5 + 1/53\lambda^4 + 27/53\lambda^3 -$ $6/53\lambda^2 - 29/53\lambda + 8/53$ $6/53\lambda^5 + 2/53\lambda^4 + 1/53\lambda^3 -$ $12/53\lambda^2 - 111/53\lambda + 122/53$	$48/53\lambda^5 - 37/53\lambda^4 + 114/53\lambda^3 -$ $255/53\lambda^2 - 199/53\lambda + 128/53,$ $9/53\lambda^5 + 3/53\lambda^4 + 28/53\lambda^3 -$ $18/53\lambda^2 - 87/53\lambda + 289/53,$ $97/53\lambda^5 + 50/53\lambda^4 + 396/53\lambda^3 -$ $247/53\lambda^2 - 655/53\lambda - 554/53,$ $26/53\lambda^5 - 62/53\lambda^4 + 128/53\lambda^3 -$ $317/53\lambda^2 + 208/53\lambda + 299/53,$ $-9/53\lambda^5 - 3/53\lambda^4 - 28/53\lambda^3 +$ $18/53\lambda^2 + 87/53\lambda + 294/53$

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

Appendix

A. Modifications for the case of (α, β)-symmetry.

In this appendix we list the changes that should be made in Subsections 4.3–4.8 in the case of (α, β)-symmetry.

(1) Replace $\varphi(x)$ (with and without index) and $\Phi(x)$ by $\varphi^2(x)$ (with the same index, if there is any) and $\Phi^2(x)$, respectively, in the following equations: (23), (30), (31), (32), (34), (49), (50), (54), (64), (65), (67), (69), (72) and everywhere in Appendix D.

(2) Modify $u_1(\mathfrak{p})$ and $u_2(\mathfrak{p})$ (see (24–25)) as follows: $u_1(\mathfrak{p}) = \max(0, -\mathrm{Ord}_{\mathfrak{p}}(\alpha\beta))$ and $u_2(\mathfrak{p}) = \max\left(0, \mathrm{Ord}_{\mathfrak{p}}\left((\alpha-\beta)^2\right)\right)$.

(3) In (32) and (33) replace $(\beta-\alpha)^p$ by $(\beta-\alpha)^{2p}$.

(4) Modify δ_i and λ_i (see (41)) as follows: $\delta_i = 2\Sigma_{j=1}^r a_{ij}\rho_i$ and $\lambda_i = \Sigma_{j=1}^r (a_{ij}\log|\gamma_j^2\theta_j^{-1}|)$. Modify the right-hand side of (51) accordingly.

(5) Modify the following constants

$$\begin{aligned} c_{10} &= 2c_7 \max_{1\leqslant j\leqslant r}\sum_{j=1}^{r}|a_{ij}|, \quad c_{14} = \max\left(1 + 2\pi^{-1}c_{12} + rc_9, e\right), \\ c_{16} &= 2c_{13}c_{12} + c_{14}, \\ X_4 &= \max(X_2,\ 3mc_7,\ e^{1/(3|\rho'|)}\left|\gamma_1\cdots\gamma_m\right|^{-1/\rho'}\left|\theta_1\cdots\theta_m\right|^{1/(2\rho')}). \end{aligned}$$

(6) In Subsections 4.5 it suffices now to assume that $[\mathbb{K}:\mathbb{Q}] \geqslant 2$. To explain this point, recall that the assumption $[\mathbb{K}:\mathbb{Q}] \geqslant 3$ was required only when $\mathbb{K} = \mathbb{K}_0$, to guarantee the existence of i_1 and i_2 such that among the numbers (62) there are at least three distinct. In the case of (α, β)-symmetry, it is enough to have $[\mathbb{K}_0:\mathbb{Q}] \geqslant 2$, because for any two distinct i_1 and i_2, there at least three distinct among the numbers (62). (Otherwise it would be either $\alpha_{i_1} = \beta_{i_1}$ and $\alpha_{i_2} = \beta_{i_2}$, or $\alpha_{i_1} = \beta_{i_2}$ and $\alpha_{i_2} = \beta_{i_1}$. In both the cases $\alpha_{i_1} + \alpha_{i_2} = \beta_{i_1} + \beta_{i_2}$ and $\alpha_{i_1}\alpha_{i_2} = \beta_{i_1}\beta_{i_2}$, which means that $\sigma_{i_1} = \sigma_{i_2}$.)

(7) Modify ϑ_0 (see (68)) as follows: $\vartheta_0 = (\gamma_{i_2}^{2\rho_{i_1}}\theta_{i_1}^{\rho_{i_2}})/(\gamma_{i_1}^{2\rho_{i_2}}\theta_{i_2}^{\rho_{i_1}})$.

(8) Replace c_{12} by $2c_{12}$ in (70), (71), (73), (75) and everywhere in Appendix D.

(9) Rewrite (94) as

$$\omega_i := \pm\gamma_i^{-1}\left(\theta_i\eta_{i1}^{b_1}\cdots\eta_{ir}^{b_r}\right)^{1/2} - \gamma_i'. \tag{98}$$

(Now there are two possibilities for ω_i, both being to be considered.)

(10) In Step 1 of the algorithm, replace the reference to Subsection 4.1 by Subsection 5.2.

B. On the number of possibilities for the vector $\boldsymbol{k}(x)$

When the number of $\mu \in \mathrm{M}$ such that $\mathbb{K}_0(\mu^{1/p}) \cong \mathbb{K}$ (or $\mathbb{K}_0(\mu^{1/p} + \mu^{-1/p}) \cong \mathbb{K}$ in the case of (α, β)-symmetry) is not too large, one can reduce the number of possible $\boldsymbol{k}(x)$. For brevity, we consider only the general case.

Fix $\mu \in \mathrm{M}$ such that $\mathbb{K}_0(\mu^{1/p}) \cong \mathbb{K}$. Then $\mathbb{K}_0(\zeta^\kappa \mu^{1/p}) = \mathbb{K}$ for some $\kappa \in \mathcal{P}$. Put $\mu_i = \sigma_i(\mu)$ and define $l_i \in \mathcal{P}$ from the equality $\sigma_i(\zeta^\kappa \mu^{1/p}) = \zeta^{l_i} {\mu_i}^{1/p}$.

Consider $x \in \mathrm{Sol}(\mathbb{K})$ such that

$$\zeta^k \left(\frac{x-\alpha}{x-\beta}\right)^{1/p} \mu^{-1/p} \in \mathbb{K}_0 \quad \text{for some } k \in \mathcal{P}. \tag{99}$$

It follows that

$$\zeta^{k(x)} \left(\frac{x-\alpha}{x-\beta}\right)^{1/p} \zeta^{-\kappa} \mu^{-1/p} \in \mathbb{K}_0. \tag{100}$$

Indeed, since both $\zeta^{k(x)}(x-\alpha/x-\beta)^{1/p}$ and $\zeta^\kappa \mu^{1/p}$ belong to $\mathbb{K}$, we have

$$\zeta^{k(x)} \left(\frac{x-\alpha}{x-\beta}\right)^{1/p} \zeta^{-\kappa} \mu^{-1/p} \in \mathbb{K}. \tag{101}$$

Therefore $\zeta^{k-k(x)+\kappa} \in \mathbb{K}$, where k is defined from (99). It follows that the degree of $\zeta^{k-k(x)+\kappa}$ over $\mathbb{K}_0$ divides p. Since it also divides $p-1$, the degree is 1, that is $\zeta^{k-k(x)+\kappa} \in \mathbb{K}_0$. Together with (99) this proves (100).

PROPOSITION B.1. *Suppose that* $\sigma_i|_{\mathbb{K}_0} = \sigma_{i'}|_{\mathbb{K}_0}$, *that is* $\alpha_i = \alpha_{i'}$ *and* $\beta_i = \beta_{i'}$. *Then for any* $x \in \mathrm{Sol}(\mathbb{K})$ *with the property* (99) *we have*

$$k_i(x) - k_{i'}(x) \equiv l_i - l_{i'} \pmod{p}. \tag{102}$$

Proof. Put

$$\lambda = \zeta^{k(x)} \left(\frac{x-\alpha}{x-\beta}\right)^{1/p} \zeta^{-\kappa} \mu^{-1/p}, \qquad \lambda_i = \sigma_i(\lambda).$$

Since λ and μ belong to $\mathbb{K}_0$, we have $\lambda_i = \lambda_{i'}$ and $\mu_i = \mu_{i'}$. Therefore

$$\begin{aligned}
\zeta^{k_i(x)} \left(\frac{x-\alpha_i}{x-\beta_i}\right)^{1/p} &= \zeta^{l_i} \mu_i^{1/p} \lambda_i \\
&= \zeta^{l_i - l_{i'}} \zeta^{l_{i'}} \mu_{i'}^{1/p} \lambda_{i'} \\
&= \zeta^{l_i - l_{i'}} \zeta^{k_{i'}(x)} \left(\frac{x-\alpha_{i'}}{x-\beta_{i'}}\right)^{1/p} \\
&= \zeta^{l_i - l_{i'}} \zeta^{k_{i'}(x)} \left(\frac{x-\alpha_i}{x-\beta_i}\right)^{1/p},
\end{aligned}$$

which proves the proposition.

Given a value of $k_i(x)$ for some i, the condition (102) defines uniquely $k_{i'}(x)$ for the p values of i' satisfying $\sigma_i|_{\mathbb{K}_0} = \sigma_{i'}|_{\mathbb{K}_0}$. Together with (19) and (20) this leaves p^{t_0} possibilities for $\boldsymbol{k}(x)$, where $2t_0$ is the number of complex embeddings of $\mathbb{K}_0$. Therefore there are at most

$$p^{t_0}|\{\mu \in \mathrm{M} : \mathbb{K}_0(\mu^{1/p}) \cong \mathbb{K}\}|, \tag{103}$$

possibilities for $\boldsymbol{k}(x)$. In some cases this number can be smaller than $(2^{p-1/2}(p-1/2)!)^{s_0}(p!)^{t_0}$.

C. Solving the Equation $\Phi(x) = 1$

In Subsection 4.5 the equation $\Phi(x) = 1$ had to be solved (in the case of (α, β)-symmetry it should be replaced by $\Phi(x) = \pm 1$.) In the case $[\mathbb{K} : \mathbb{K}_0] = p \geqslant 3$ both k_{i_1} and k_{i_2} are nonzero. Therefore $\rho_{i_1} = \rho_{i_2} = 1$, and the equation $\Phi(x) = \pm 1$ can be rewritten as

$$\zeta_{i_1}(1-\alpha_{i_1}x^{-1})^{1/p} - (1-\beta_{i_1}x^{-1})^{1/p} = \mathrm{const} \cdot (\zeta_{i_2}(1-\alpha_{i_1}x^{-1})^{1/p} - (1-\beta_{i_1}x^{-1})^{1/p}),$$

which can be easily reduced to a linear equation in x.

In the case $\mathbb{K} = \mathbb{K}_0$ we need the following lemma, which is an immediate consequence of Kummer's theory [12, Ch. 6, Th. 8.1] over the field $\mathbb{C}(T)$.

LEMMA C.1. *Let $\varsigma_1, \ldots, \varsigma_\nu$ be distinct nonzero complex numbers and*

$$F(T, T_1, \ldots, T_\nu) \in \mathbb{C}[T, T_1, \ldots, T_\nu],$$

a nonzero polynomial such that

$$F\left(T, (1-\varsigma_1 T)^{1/p}, \ldots, (1-\varsigma_\nu T)^{1/p}\right) \equiv 0.$$

Then $\deg_{T_i} F \geqslant p$ *for* $1 \leqslant i \leqslant \nu$.

Using this lemma we can prove that the function $\Phi(x)$ is non-constant. Indeed, if $\Phi(x)$ were a constant, then, depending on whether ρ_{i_1} and ρ_{i_2} are equal or distinct, we would have obtained one of the following identities: either

$$\zeta_{i_1}(1-\alpha_{i_1}x^{-1})^{1/p} - (1-\beta_{i_1}x^{-1})^{1/p} = \mathrm{const}(\zeta_{i_2}(1-\alpha_{i_2}x^{-1})^{1/p} - (1-\beta_{i_2}x^{-1})^{1/p}), \tag{104}$$

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

or

$$x(\zeta_{i_1}(1-\alpha_{i_1}x^{-1})^{1/p}-(1-\beta_{i_1}x^{-1})^{1/p})$$
$$\times(\zeta_{i_2}(1-\alpha_{i_2}x^{-1})^{1/p}-(1-\beta_{i_2}x^{-1})^{1/p})^{p-1}=ct. \tag{105}$$

(We used (48), which holds for sufficiently large x, and in the case of distinct ρ_{i_1} and ρ_{i_2} we assumed that $\rho_{i_1}=1$ and $\rho_{i_2}=1-p$.) Since among the radicals there are at least three distinct, both (104) and (105) contradict to the assertion of Lemma C.1. Therefore $\Phi(x)$ is non-constant.

We solve the equation $\Phi(x)=1$ in the following way. Let $\mathcal{K}$ be the field generated over $\mathbb{C}(x)$ by the radicals involved in $\Phi(x)$. Then $\mathcal{N}_{\mathcal{K}/\mathbb{C}(x)}(\Phi(x)-1)$is rational function in x, and we write it as $P(x)/Q(x)$. Since $\Phi(x)$ is non-constant, the polynomial $P(x)$ is nonzero, and all the solutions of $\Phi(x)=1$ are among the roots of $P(x)$.

Thus, finding integral solutions of the algebraic Equation (64) reduces to finding integral roots of a polynomial $P(x)$. In practice, the coefficients of $P(x)$ are known approximately, and we had to estimate the precision of the roots. (Since we were interested only in integral roots, we did not need very high precision.) The following lemma was used for estimating the precision.

LEMMA C.2. *Let $P(x)=a_0x^N+a_1x^{N-1}+\cdots+a_N$ and $Q(x)=b_0x^N+b_1x^{N-1}+\cdots+b_N$ be polynomials with complex coefficients. Let ε be a positive number with the following property:*

$(*)$ *for any two roots z and z' of Q one has either $|z-z'|\leqslant\varepsilon/2$ or $|z-z'|\geqslant 2\varepsilon$. Put*

$$\delta=\delta(\varepsilon)=\min_{1\leqslant i\leqslant N}\frac{|b_0|\prod_{j=1}^{N}||z_j-z_i|-\varepsilon|}{\sum_{j=0}^{N}(|z_i|+\varepsilon)^j}, \tag{106}$$

where $z_1,\ldots,z_N$ are the roots of Q counted with multiplicities. Assume that

$$|a_i-b_i|<\delta \quad (0\leqslant i\leqslant N).$$

Then for any root z of P there is a root z' of Q such that $|z-z'|<\varepsilon$.

(It will follow from the proof that there is a one-to-one correspondence $z\leftrightarrow z'$ between the roots of P and the roots of Q such that $|z-z'|<\varepsilon$ for every pair of corresponding roots.)

Proof. Define an equivalence relation on the set of roots of Q by $z\sim z'$ when $|z-z'|\leqslant\varepsilon/2$ (transitivity follows from $(*)$). Let $m_1,\ldots,m_k$ be the cardinalities of the the equivalence classes (so that $m_1+\cdots+m_k=N$), and assume that the roots are numbered so that $z_1,\ldots,z_k$ are respective representatives of the classes. In particular

$$|z_i-z_j|\geqslant 2\varepsilon \quad (1\leqslant i<j\leqslant k). \tag{107}$$

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

Fix i with $1 \leqslant i \leqslant k$. Then Q has m_i roots in the disc $\Delta_i := \{z \in \mathbb{C} : |z - z_i| < \varepsilon\}$.

For any z on the circle $\Gamma_i := \{z \in \mathbb{C} : |z - z_i| = \varepsilon\}$ one has

$$|Q(z)| = |b_0(z - z_1) \dots (z - z_N)| \geqslant |b_0| \prod_{j=1}^{N} ||z_j - z_i| - \varepsilon|.$$

Hence, for any $z \in \Gamma_i$

$$|P(z) - Q(z)| < \delta \sum_{j=0}^{N} (|z_i| + \varepsilon)^j \leqslant |Q(z)|.$$

By the theorem of Rouché, P also has m_i roots in Δ_i.

By (107), the discs Δ_i are pairwise disjoint. Since $m_1 + \dots + m_k = N$, every root of P belongs to one of Δ_i. The lemma is proved.

We apply this lemma as follows. Assume we have to find all integral roots of a polynomial $P(x)$, but instead of P, we have only an approximation $Q(x)$, with a known precision δ_0 (that is, $\max_{i=0,\dots,N} |a_i - b_i| \leqslant \delta_0$). Having computed the roots of $Q(x)$, one can easily decide which integers are 'very close' to a root of $Q(x)$. This integers (we call them *suspicious*) are probable roots of $P(x)$.

To see that $P(x)$ has no integral roots other than suspicious, we do as follows. For any $z \in C$ denote by $\rho(z)$ the distance to the nearest non-suspicious integer, and put $\varepsilon_0 = 0.1 \min(\rho(z_1), \dots, \rho(z_N))$. If ε_0 meets the condition (∗), we put $\varepsilon = \varepsilon_0$; otherwise put $\varepsilon_1 = 0.1 \min_{|z - z'| \geqslant \varepsilon_0} |z - z'|$, where z and z' independently run the set of all roots of Q. If ε_1 meets the condition (∗), we put $\varepsilon = \varepsilon_1$; otherwise put $\varepsilon_2 = 0.1 \min_{|z - z'| \geqslant \varepsilon_1} |z - z'|$, etc.; in practice, we always found a suitable ε after two–three iterations. When ε is found, compute δ; if $\delta > \delta_0$ then $P(x)$ indeed has no integral roots other than suspicious. If $\delta \leqslant \delta_0$ (which never happened in our practice) then one has to recompute Q with higher precision.

D. The totally rational case

In this appendix we give a detailed treatment of the totally rational case, see Subsection 4.6.1.

We have

$$\delta_{j_1}^{-1} \delta_j = q_j / q, \quad \delta_{j_1}^{-1} \left(\delta_j \lambda_{j_1} - \delta_{j_1} \lambda_j\right) = q_j' / q \quad (1 \leqslant j \leqslant r), \tag{108}$$

where q is a positive integer, q_j, q_j' integers, and $\gcd(q_1, \dots, q_r, q) = 1$. (To simplify the notation, we do not exclude $j = j_1$, in which case $q_j = q$ and $q_j' = 0$.) As in the semirational case, we expect that the integers q_j, q_j' and q are 'small'.

Replacing in (77) index j_2 by j, and using (108), we obtain

$$|q b_j(x) - q_j b_{j_1}(x) + q_j'| \leqslant 2 q c_{10} |x|^{-1} \quad (1 \leqslant j \leqslant r). \tag{109}$$

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

If $|x| > X_7 : \max(X_3, 4qc_{10})$ then (109) turns to

$$qb_j(x) - q_j b_{j_1}(x) + q'_j = 0 \quad (1 \leqslant j \leqslant r). \tag{110}$$

If $\gcd(q, q_j)$ does not divide q'_j for some j then there are no solutions x with $|x| > X_7$. Otherwise, one easily finds integers $b_1, \ldots, b_r$ such that

$$qb_j - q_j b_{j_1} + q'_j = 0 \quad (1 \leqslant j \leqslant r). \tag{111}$$

Then

$$b_j(x) = b_j + q_j b(x) \quad (1 \leqslant j \leqslant r), \tag{112}$$

where $b(x) \in \mathbb{Z}$. Substituting this to (67), we obtain

$$\Phi(x) = \vartheta'_0 \vartheta^{b(x)}, \tag{113}$$

where

$$\vartheta'_0 = \vartheta_0 \vartheta_1^{b_1} \cdots \vartheta_r^{b_r}, \quad \vartheta = \vartheta_1^{q_1} \cdots \vartheta_r^{q_r}.$$

The further arguments splits into five cases.

(1) $|\vartheta| \neq 1$

In this case (113), together with (66), yields

$$|\log|\vartheta'_0| + b(x)\log|\vartheta|| \leqslant c_{12}|x|^{-1}. \tag{114}$$

Hence $b(x)$ is the nearest integer to $-\log|\vartheta'_0|/\log|\vartheta|$ whenever $|x| > X_8 := \max(X_7, 2c_{12})$.

(2) $|\vartheta| = 1$, but $|\vartheta'_0| \neq 1$

We again have (114), which now reduces to

$$|\log|\vartheta'_0|| \leqslant c_{12}|x|^{-1}. \tag{115}$$

Thus, $|x| \leqslant X_8 := \max(X_7, c_{12}|\log|\vartheta'_0||^{-1})$.

(3) $|\vartheta| = |\vartheta'_0| = 1$, *but ϑ is not a root of unity*

Again using (113) and (66), we obtain

$$\|(2\pi)^{-1}\arg\vartheta'_0 + (2\pi)^{-1}\arg\vartheta b(x)\| \leqslant (2\pi)^{-1}c_{12}|x|^{-1}, \tag{116}$$

and we continue as in the irrational (respectively, semirational) case if 2π, $\arg\vartheta$ and $\arg\vartheta'_0$ are linearly independent (respectively, linearly dependent) over $\mathbb{Z}$.

(4) *ϑ is a primitive Nth root of unity and $|\vartheta'_0| = 1$, but ϑ'_0 is not an Nth root of unity*

We have

$$\|N(2\pi)^{-1}\arg\vartheta_0'\| \leqslant N(2\pi)^{-1}c_{12}|x|^{-1}, \tag{117}$$

and since the left-hand side is nonzero, we obtain

$$|x| \leqslant X_8 := \max(X_7, N(2\pi)^{-1}c_{12}\|N(2\pi)^{-1}\arg\vartheta_0'\|^{-1}).$$

(5) *ϑ is a primitive Nth root of unity and ϑ_0' is an Nth root of unity*
In this case $\Phi(x)$ is also an Nth root of unity. Since $\Phi(x) \neq 1$, we obtain $|\log\Phi(x)| \geqslant 2\pi/N$. Hence $|x| \leqslant X_8 := \max(X_7, N(2\pi)^{-1}c_{12})$.

E. THE HYPERELLIPTIC EQUATION

In this appendix we briefly explain how our method can be adapted for solving the *hyperelliptic equation* $y^2 = f(x)$, where $f(x)$ is a separable polynomial of degree at least 3. (Probably, it would be more correct to call it *elliptic equation* when $\deg f \leqslant 4$; for brevity, we extend the term *hyperelliptic* also to this case.) What follows is merely a short draft, and many details are left out. In particular, we make no use in possible symmetry of the roots. For examples and generalization of (α, β)-symmetry to that case, see [11].

Again, fix two distinct roots α and β of $f(x)$, and assume first that $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] \geqslant 3$. It is easy to see that in this case the method of Section 4 extends also to $p = 2$. Indeed, the assumption $p \geqslant 3$ was made in Section 4 only twice: in Proposition 4.2.1, and in Subsection 4.5. We leave to the reader the reformulation of Proposition 4.2.1 for $p = 2$. As for Subsection 4.5, it is indeed impossible to satisfy (60)–(61) when $p = 2$. However, since $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] \geqslant 3$, we can always find i_1 and i_2 such that among the numbers (62) there are at least three distinct, which allows one to compute the Baker's bound.

It remains to consider the case $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] \leqslant 2$. Fix one more root γ, distinct from α and β. We may assume that $[\mathbb{Q}(\alpha,\gamma):\mathbb{Q}] \leqslant 2$ and $[\mathbb{Q}(\gamma,\beta):\mathbb{Q}] \leqslant 2$; otherwise, redefining the roots, we return to the case $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] \geqslant 3$.

It follows that $[\mathbb{Q}(\alpha,\beta,\gamma):\mathbb{Q}] \leqslant 2$. Redefining the roots, we can additionally assume that

(i) either $\alpha,\beta,\gamma \in \mathbb{Q}$,
(ii) or α and β are quadratic conjugates over $\mathbb{Q}$, and $\gamma \in \mathbb{Q}(\alpha)$.

Case (i) is very simple: it can be reduced to two simultaneous Pell equations, see for instance [33]. In case (ii) put $\mathbb{K}_0 = \mathbb{Q}(\alpha)$, and say that a number field $\mathbb{K}$ is admissible for a solution x if $\mathbb{K} = \mathbb{K}_0((x-\alpha/x-\gamma)^{1/2})$. One easily constructs a complete system of admissible fields, which would consist of $\mathbb{K}_0$ and a finite amount of its quadratic extensions.

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

Now fix an admissible field $\mathbb{K}$ and put $\varphi(x) = (x-\gamma)((x-\alpha/x-\gamma)^{1/2}+1)^2$. Then we again have (34), where $\theta(x)$ belongs to a finite effectively constructible set.

If $\mathbb{K} = \mathbb{K}_0$ then we have finitely many possible values for $\varphi(x)\sigma(\varphi(x))$, where σ is the non-trivial automorphism of $\mathbb{K}_0$. However, $\sigma((x-\alpha/x-\gamma)^{1/2}) = \pm(x-\beta/x-\gamma')^{1/2}$, where $\gamma' = \sigma(\gamma)$. Using Kummer's theory, as in Appendix C, we observe that

$$\varphi(x)\sigma(\varphi(x)) = (x-\gamma)\left(\left(\frac{x-\alpha}{x-\gamma}\right)^{1/2}+1\right)^2 (x-\gamma')\left(\pm\left(\frac{x-\beta}{x-\gamma'}\right)^{1/2}+1\right)^2$$

is a non-constant function of x, which allows one to compute the set $\mathrm{Sol}(\mathbb{K}_0)$.

If $[\mathbb{K}:\mathbb{K}_0] = 2$, then, putting

$$\Phi(x) = \frac{(x-\gamma)\left(\left(\frac{x-\alpha}{x-\gamma}\right)^{1/2}+1\right)^2}{(x-\gamma')\left(\left(\frac{x-\beta}{x-\gamma'}\right)^{1/2}+1\right)^2},$$

one can compute the Baker's bound and proceed further as in Section 4. See [31, 32] for a similar algorithm in the case deg $f = 3$.

Acknowledgements

The main part of this paper was written during the first named author's postdoctoral stage at the Max-Planck-Institut für Mathematik, Bonn. At different stages of preparation of this paper he was also supported by the Bourse Chateaubriand du Gouvernement Français, Karl-Franzens-Universität Graz, and Instituto de Matemática Pura e Aplicada. He is grateful to Professor J.-M. Deshouillers at Bordeaux, Professor F. Hirzebruch at Bonn, Professor F. Halter-Koch at Graz, and Professor J. Palis at Rio de Janeiro for their generous hospitality.

We would like to thank Henri Cohen, Xavier Roblot, Nikos Tzanakis, Benne de Weger, and Don Zagier for interesting discussions and suggestions.

The last but not least, we are pleased to thank the referee for a number of very valuable comments, in particular concerning Proposition 3.1.

References

1. Baker, A.: Linear forms in the logarithms of algebraic numbers I, *Mathematica* 13 (1966), 204–216; II, ibid. 14 (1967), 102–107; III, ibid. 14 (1967), 220–228; IV, ibid. 15 (1968), 204–216.
2. Baker, A.: Bounds for the solutions of the hyperelliptic equations, *Proc. Camb. Phil. Soc.* 65 (1969), 439–444.
3. Baker, A. and Davenport, H.: The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quat. J. Math. Oxford (2)* 20 (1969), 129–137.
4. Baker, A. and Wüstholz, G.: Logarithmic forms and group varieties, *J. Reine Angew. Math.* 442 (1993), 19–62.

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

5. Bilu, Yu.: Effective analysis of integral points on algebraic curves, *Israel J. of Math.* 90 (1995), 235–252.
6. Bilu, Yu.: Solving superelliptic Diophantine equations by the method of Gelfond–Baker, preprint 94–109, Mathématiques Stochastiques, Univ. Bordeaux 2, 1994.
7. Bilu, Yu.: Quantitative Siegel's theorem for Galois coverings, *Compositio Math.* 106 (1997), 125–158.
8. Bilu, Yu. and Hanrot, G.: Solving Thue equations of high degree, *J. Number Th.* 60 (1996), 373–392.
9. Brindza, B.: On S-integral solutions of the equation $y^m = f(x)$, *Acta Math. Hungar.* 44 (1984), 133–139.
10. Cohen, H.: *A Course in Computational Algebraic Number Theory,* Graduate Texts in Math. 138, Springer, 1993.
11. Hanrot, G.: *Résolution effective d'équations diophantiennes: algorithmes et applications*, Thèse, Université Bordeaux 1, 1997.
12. Lang, S.: *Algebra,* Third Edition, Addison-Wesley, 1993.
13. Lenstra, A. K., Lenstra jr., H. W. and Lovász, L.: Factoring polynomials with rational coefficients, *Math. Ann.* 261 (1982), 515–534.
14. Mignotte, M. and Pethö, A.: Sur les carrés dans certaines suites de Lucas, *J. Th. Nombr. Bordeaux* 5 (1993), 333–341.
15. Mignotte, M. and Pethö, A.: On the system of diophantine equations $x^2 - 6y^2 = -5$ and $x = 2z^2 - 1$, *Math. Scand.* 76 (1995), 50–60.
16. Mignotte, M. and de Weger, B. M. M.: On the Diophantine equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$, *Glasgow Math. J.* 38 (1996).
17. Pethö, A.: Computational methods for the resolution of Diophantine equations, *in* R. A. Mollin (ed.), *Number Theory: Proc. First Conf. Can. Number Th. Ass., Banff, 1988,* de Gruyter, 1990, 477–492.
18. Pethö, A.: de Weger, B, M, M.: Products of prime powers in binary recurrence sequences Part I: The hyperbolic case, with an application to the generalized Ramanujan–Nagell equation, *Math. Comp.* 47 (1987), 713–727.
19. Pohst, M. E.: *Computational Algebraic Number Theory,* DMV Seminar, Vol. 21, Birkhäuser, Basel, 1993.
20. Pohst, M. E. amd Zassenhaus, H.: *Algorithmic Algebraic Number Theory,* Cambridge Univ. Press, 1989.
21. Poulakis, D.: Solutions entières de l'équation $Y^m = f(x)$. *Sém. Th. Nombr. Bordeaux* 3 (1991), 187–199.
22. Shorey, T. N. and Tijdeman, R.: *Exponential Diophantine equations,* Cambridge Univ. Press, Cambridge, 1986.
23. Smart, N.: The solution of triangularly connected decomposable form equation, *Math. Comp.* 64 (1995), 819–840.
24. Sprindžuk, V. G.: The arithmetic structure of integral polynomials and class numbers (Russian), *Trudy Mat. Inst. Steklov* 143 (1977), 152–174; English transl.: *Proc. Steklov Inst. Math*. 1980, issue 1, 163–186.
25. Sprindžuk, V. G.: *Classical Diophantine Equations in Two Unknowns* (Russian), Nauka, Moscow, 1982; English trans.: Lecture Notes in Math. 1559, Springer, 1994.
26. Trelina, L. A.: On S-integral solutions of the hyperelliptic equation (Russian), *Dokl. Akad. Nauk BSSR* 22 (1978), 881–884.
27. Tzanakis, N. and de Weger, B. M. M.: On the practical solution of the Thue equation, *J. Number Th.* 31 (1989), 99–132.
28. Tzanakis, N. and de Weger, B. M. M.: How to explicitly solve a Thue–Mahler equation, *Compositio Math.* 84 (1992), 223–288.
29. Voutier, P. M.: An upper bound for the size of integral solutions to $Y^m = f(X)$, *J. Number Theory* 53 (1995), 247–271.
30. de Weger, B. M. M.: Solving exponential diophantine equations using lattice basis reduction algorithms, *J. Number Th.* 26 (1987), 325–367.

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press

31. de Weger, B. M. M.: Integral and S-integral solutions of a Weierstrass equation, report 9452/B, Econometric Inst., Erasmus Univ., Rotterdam, 1994.
32. de Weger, B. M. M.: Solving elliptic Diophantine equations by Bilu's method, report 9469/B, Econometric Inst., Erasmus Univ., Rotterdam, 1994.
33. Zagier, D.: Large integral points on elliptic curves, *Math. Comp.* 48 (1987), 425–436.

https://doi.org/10.1023/A:1000305028888 Published online by Cambridge University Press