MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 210
APRIL 1995, PAGES 819–840

THE SOLUTION OF TRIANGULARLY CONNECTED DECOMPOSABLE FORM EQUATIONS

N. P. SMART

ABSTRACT. An algorithm is given to solve the equations of the title. It generalizes an earlier algorithm to solve discriminant form equations. An application is given to finding curves of genus 2 with good reduction outside a given finite set of primes and Weierstrass points in given number fields.

In this paper we generalize the methods for Thue and Thue-Mahler equations given by Tzanakis and de Weger, [23, 24, 25] (see also [1, 17, 28]), and the method for discriminant form equations given in [22] (see also [4, 5, 6]). All of the above-mentioned equations are examples of Triangularly Connected Decomposable Forms (TCDFs for short). These were first studied by Győry, whose treatment relies on the finiteness results he established for linear equations in S-units, [8]. In [8] an explicit bound was given on the solutions of equations of the type

$$\alpha_1 x_1 + \alpha_2 x_2 + 1 = 0,$$

where we are given α_1 and $\alpha_2 \in K$, a given number field, and we wish to find x_1 and x_2 in S-units of K. This result makes it possible, at least in principle, to determine all solutions. However, the bound is too large for practical use. I give an algorithm to solve such S-unit equations using the reduction techniques developed in [27]. Unlike the Thue-Mahler equation case, we have to consider linear forms with nonzero real and imaginary parts. This leads to a slightly different reduction technique than that used in [25].

Győry, [7, 9, 11], used the above result to establish finiteness results on the solutions of TCDF equations by giving explicit upper bounds for the solutions. These bounds are also too large for practical use. I give a method to solve such TCDF equations using the above-mentioned algorithm for S-unit equations. But one need not stop here, since Győry, [12] (see also [3]), extended the type of TCDFs that can be considered. But I shall not deal with these more general equations here, except to note that they are closely related to Győry's work on graphs of sets of algebraic integers, see [10].

The work in this paper was started in the author's thesis, [21]. However, in this paper I take the opportunity to improve the method and correct some mistakes that appeared in the thesis. I would like to thank SERC for funding my Ph.D. work and the Wingate Foundation and the Royal Society for funding my

Received by the editor November 18, 1992 and, in revised form, December 2, 1993.
1991 *Mathematics Subject Classification.* Primary 11Y50; Secondary 11D41.

post-Ph.D. work. I also wish to thank the Universities of Kent and Rotterdam for their hospitality and the use of their computing facilities, and the referee for many helpful suggestions and improvements.

As usual, $c_1, c_2, \ldots$ will denote positive real constants which are effectively computable, the notation $c_i(j)$ will mean that c_i possibly takes a different value for every value of the parameter j, i.e., c_i is an array of constants.

1. Triangularly connected linear forms

Let $\mathbb{L}$ be a set of m linear forms, $m \geq 3$, in v variables with coefficients in the ring of integers of some number field K of degree n, i.e.,

$$L_j(\underline{x}) = \sum_{i=1}^{v} l_{i,j} x_i \ , \qquad l_{i,j} \in \mathbb{Z}_K \ , \ 1 \leq j \leq m.$$

Such a system is called triangularly connected, cf. [13, p. 312], if for all i, j, such that $i \neq j$ and $1 \leq i, j \leq m$, there is a sequence, $L_i = L_{i_1}, L_{i_2}, \ldots, L_{i_w} = L_j$, in $\mathbb{L}$, such that for each u, with $1 \leq u \leq w-1$, there exist nonzero $\alpha_i \in \mathbb{Z}_K$ for $i = 1, 2, 3$ (depending on u), such that

$$\alpha_1 L_{i_u} + \alpha_2 L_{i_{u+1}} + \alpha_3 L_{i_{u,u+1}} = 0$$

with $L_{i_{u,u+1}} \in \mathbb{L}$.

To see why we call this triangularly connected, let $G_{\mathbb{L}}$ be the hypergraph with vertices $L_i \in \mathbb{L}$. Now, for three such vertices, say L_1, L_2, L_3, we connect the vertices with an edge (triangle) if and only if

$$\alpha_1 L_1 + \alpha_2 L_2 + \alpha_3 L_3 = 0$$

has a solution $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}_K$, with $\alpha_i \neq 0$ for $i = 1, 2, 3$. So the hypergraph consists entirely of triangles and $\mathbb{L}$ is triangularly connected if and only if $G_{\mathbb{L}}$ is a connected hypergraph.

2. Triangularly connected decomposable form equations

Let $F(\underline{x})$ be a decomposable form of degree m in v variables, with coefficients in $\mathbb{Z}$, and with decomposition

$$F(\underline{x}) = a_0 L_1'(\underline{x}) \cdots L_m'(\underline{x}),$$

where $a_0 \neq 0$ is a rational integer and $L_i'(\underline{x})$ are linear forms with coefficients in a galois extension K of $\mathbb{Q}$ of degree n, given by

$$L_j'(\underline{x}) = x_1 + l_{2,j}' x_2 + \cdots + l_{v,j}' x_v \ , \qquad j = 1, \ldots, m,$$

where $l_{i,j}' \in K$. Write $l_{i,j} = a_0 l_{i,j}'$ for $i \geq 2$ and $l_{1,j} = a_0$. Then $l_{i,j} \in \mathbb{Z}_K$ for all i, j, and set

$$f(\underline{x}) = a_0^{m-1} F(\underline{x}) = \prod_{j=1}^{m} L_j(\underline{x}),$$

where

$$L_j(\underline{x}) = \sum_{i=1}^{v} l_{i,j} x_i \ , \qquad j = 1, \ldots, m.$$

The form $f(\underline{x})$ will be called triangularly connected if the set $\mathbb{L} = \{L_j(\underline{x})\}$ is triangularly connected. We wish to solve the equation $F(\underline{x}) = Ap_1^{z_1} \cdots p_t^{z_t}$ in $\underline{x} \in \mathbb{Z}^v$ and nonnegative integers $z_1, \ldots, z_t$, subject to $\gcd(\underline{x}) = 1$, where A is a given nonzero integer and $\{p_1, \ldots, p_t\}$ are given distinct rational primes. This is equivalent to solving the equation

$$f(\underline{x}) = a_0^{m-1} A p_1^{z_1} \cdots p_t^{z_t}. \tag{1}$$

Further, we shall assume

1. $f(\underline{x})$ is a TCDF;
2. There is no $\underline{x} \in \mathbb{Z}^v$, with $\underline{x} \neq \underline{0}$, such that $L_j(\underline{x}) = 0$ for all j.

Assumption 2 means that the matrix

$$\begin{pmatrix} l_{1,1} & \cdots & l_{v,1} \\ \vdots & & \vdots \\ l_{1,m} & \cdots & l_{v,m} \end{pmatrix}$$

has column rank v over $\mathbb{Q}$. This in turn means that we must have $v \leq mn$, see [13].

We define a prime of K to be an equivalence class of nontrivial valuations on K. The infinite primes, S_∞, are those containing archimedian valuations. An infinite prime will be called real (resp. complex) if it corresponds to a real (resp. complex) embedding of K. The number of real embeddings will be denoted by r_1 and the number of nonconjugate complex embeddings will be denoted by r_2. Let S_f be a finite set of finite primes of K. Then we define S to be the set $S_f \cup S_\infty$.

Let s denote the number of elements of S_f and r be the usual Dirichlet rank (so $\#S_\infty = r + 1 = r_1 + r_2$). Because the sets of prime ideals and finite primes are equivalent, we shall also refer to S_f as a set of prime ideals. We place an order on S in the following way: for $\alpha \in K$ and $\wp_i \in S$

$$|\alpha|_{\wp_i} = \begin{cases} p_i^{-f_i \operatorname{ord}_{\wp_i}(\alpha)}, & 1 \leq i \leq s, \ \wp_i \in S_f, \\ |\alpha^{(i-s)}|, & s+1 \leq i \leq s + r_1, \\ |\alpha^{(i-s)}|^2, & \text{otherwise}, \end{cases}$$

where the $\alpha^{(i)}$ of K are ordered in the usual way, see [25, p. 225], and p_i, f_i denote the rational prime lying below $\wp_i$ and its residual degree, respectively. The ramification index of $\wp_i$ will be denoted by e_i. The S-units of K are the finitely generated group

$$U_S = \{\alpha \in K : |\alpha|_\wp = 1 \text{ for all } \wp \notin S\}.$$

Let Log denote the usual map $U_S \longrightarrow \mathbb{R}^{r+s}$ and h_K the class number of K.

Let $\underline{x}$ be a solution of equation (1) with $\gcd(\underline{x}) = 1$. For $1 \leq j \leq m$ set $\beta_j = L_j(\underline{x})$. Now, if S_f denotes the set of prime ideals of K dividing $(a_0 A p_1 \cdots p_t)$, then we see that $\beta_j \in U_S$. In particular, we see that if (L_1, L_2, L_3), say, denotes any triangle of the hypergraph, then

$$\frac{\alpha_1 \beta_1}{\alpha_3 \beta_3} + \frac{\alpha_2 \beta_2}{\alpha_3 \beta_3} + 1 = 0$$

is an S-unit equation. In later sections I will show how to solve such an S-unit equation. First note that we have one S-unit equation for each triangle in the hypergraph. However, using the action of the galois group of K over $\mathbb{Q}$, remembering that K is a galois extension, we can reduce the number of S-unit equations that need to be considered.

Let $G = \mathrm{Gal}(K/\mathbb{Q})$ and let $\mathscr{C}$ be a subhypergraph of $G_{\mathbb{L}}$. The group G naturally generates a subhypergraph, $\mathscr{C}^G$, of $G_{\mathbb{L}}$ from $\mathscr{C}$, where $\mathscr{C}^G$ has vertices given by $\sigma(L_i)$, where $\sigma \in G$ and $L_i \in \mathscr{C}$, if $\sigma(L_i) \in G_{\mathbb{L}}$. The edges of $\mathscr{C}^G$ are those triangles in $G_{\mathbb{L}}$ which have all their vertices in $\mathscr{C}^G$. Thus, we have $\mathscr{C} \subset \mathscr{C}^G \subset G_{\mathbb{L}}$. To solve our TCDF, we only need to solve the S-unit equations represented by $\mathscr{C}$ (rather than $G_{\mathbb{L}}$) for a $\mathscr{C}$ such that

1. $\mathscr{C}^G$ is a connected hypergraph;
2. $\mathscr{C}^G$ contains all vertices of $G_{\mathbb{L}}$.

3. Solving an S-unit equation

We now derive an effective bound for the solutions of S-unit equations. In [8], an explicit bound was given for the solutions. In the proof, some explicit estimates for linear forms in logarithms were involved. In our proof below we give a modified version of the proof of [8] and replace the estimates mentioned above by recent improved ones due to Yu [29] and Baker and Wüstholz [2].

Let $\beta_{i,j} \in U_S$ for $1 \leq i \leq t_j$ and $j = 1, 2$ such that $\mathrm{Log}(\beta_{1,j}), \ldots, \mathrm{Log}(\beta_{t_j,j})$ are linearly independent, hence $t_j \leq r+s$. Now set

$$\tau_i = \prod_{j=1}^{t_i} \beta_{j,i}^{a_{j,i}}, \qquad a_{j,i} \in \mathbb{Z}, \quad i = 1, 2.$$

We wish to solve the equation

$$\alpha_1\tau_1 + \alpha_2\tau_2 + 1 = 0, \tag{2}$$

where $\alpha_1, \alpha_2 \in \mathscr{A}$, a finite set of elements of K. In our case we have $\beta_{i,1} = \beta_{i,2}$ for $i = 1, \ldots, t_1$, where $t_1 = t_2 = r+s$ and $\beta_{1,1}, \ldots, \beta_{r+s,1}$ are generators of the nontorsion part of U_S. Such generators are easily constructed. It may be possible to restrict the τ_i to a subgroup of U_S in some examples, for instance by considering the factorization of the form $f(\underline{x})$ over $\mathbb{Z}$. So we shall consider the more general S-unit equation, (2).

Set $H = \max(|a_{i,j}|)$, where the maximum is taken over $1 \leq i \leq t_j$ and $1 \leq j \leq 2$. Our aim in this section is to find a large bound on H. Choose g, h, b such that $b = 1, 2$ and $1 \leq g, h \leq r+s+1$ such that $H = |a_{k,b}|$ for some k and

$$|\log|\tau_b|_{\wp_g}| = \max_{\wp_i \in S} |\log|\tau_b|_{\wp_i}|, \qquad |\tau_b|_{\wp_h} = \min_{\wp_i \in S} |\tau_b|_{\wp_i}.$$

We do not know at this stage what the values of b and h actually are, so we need to perform our calculations for each possibility. It will turn out that the value of g is immaterial.

For $i = 1, 2$ let $U = \{u_1, \ldots, u_{t_i}\}$ be a subset of distinct elements of $\{1, \ldots, r+s+1\}$ such that the matrix

$$C_{i,U} = \begin{pmatrix} \log|\beta_{1,i}|_{\wp_{u_1}} & \cdots & \log|\beta_{t_i,i}|_{\wp_{u_1}} \\ \vdots & & \vdots \\ \log|\beta_{1,i}|_{\wp_{u_{t_i}}} & \cdots & \log|\beta_{t_i,i}|_{\wp_{u_{t_i}}} \end{pmatrix} \in \mathbb{R}^{t_i \times t_i}$$

is invertible. Now by our assumption that $\mathrm{Log}(\beta_{1,i}), \ldots, \mathrm{Log}(\beta_{t_i,i})$ are linearly independent such U do exist. Set $c_1 = \max(\|C_{i,U}^{-1}\|_\infty)$, where the maximum is taken over $i = 1, 2$ and all U satisfying the above condition. Note, for a matrix A, that $\|A\|_\infty$ denotes the infinity norm of the matrix, see [14, §5.6].

Lemma 1. *We have*

$$H \leq c_1 |\log|\tau_b|_{\wp_g}|.$$

Proof. We have that for some U,

$$\begin{pmatrix} a_{1,b} \\ \vdots \\ a_{t_b,b} \end{pmatrix} = C_{b,U}^{-1} \begin{pmatrix} \log|\tau_b|_{\wp_{u_1}} \\ \vdots \\ \log|\tau_b|_{\wp_{u_{t_b}}} \end{pmatrix}.$$

So

$$H \leq \|C_{b,U}^{-1}\|_\infty \max_{u_i \in U}(|\log|\tau_b|_{\wp_{u_i}}|) \leq c_1 |\log|\tau_b|_{\wp_g}|. \quad \square$$

Let $c_2 = 1/c_1$ and choose c_3 such that $0 < c_3 < c_2/(r+s)$. A good choice of c_3 is $0.99c_2/(r+s)$, assuming $r+s$ is not too large (say < 50). It can be seen from what follows that the larger c_3 is, the better the final bounds will be after our reduction steps. With present computing power an equation with $r+s > 15$ would seem to be impractical, so we always make the above choice of c_3.

Lemma 2. *We have*

$$|\tau_b|_{\wp_h} \leq e^{-c_3 H}.$$

Proof. Assume that $|\tau_b|_{\wp_h} > e^{-c_3 H}$. Then, by Lemma 1, we have two cases to consider.

Case 1. $|\tau_b|_{\wp_g} \geq e^{c_2 H}$. We have that

$$\prod_{i=1}^{r+s+1} |\tau_b|_{\wp_i} = 1,$$

and so

$$e^{c_2 H} \leq |\tau_b|_{\wp_g} = \prod_{i=1, i \neq g}^{r+s+1} |\tau_b|_{\wp_i}^{-1} < e^{(r+s)c_3 H}.$$

Therefore, $H < 0$, as $c_2 > (r+s)c_3$, which is impossible.

Case 2. $|\tau_b|_{\wp_g} \leq e^{-c_2 H}$. We have

$$e^{-c_2 H} \geq |\tau_b|_{\wp_g} \geq |\tau_b|_{\wp_h} > e^{-c_3 H}.$$

So $H < 0$, as $c_2 > c_3$, which is again impossible. $\square$

Now for $1 \leq i \leq r+s+1$ set

$$c_4(i) = \max_{\alpha \in \mathscr{A}} |\alpha|_{\wp_i}.$$

Set $d = 3 - b$, remembering that $b = 1$ or 2, and $\Lambda_b = \alpha_b \tau_b = -\alpha_d \tau_d - 1$. Note, by Lemma 2, $|\Lambda_b|_{\wp_h} \leq c_4(h) e^{-c_3 H}$. We now bound H in the case that $1 \leq h \leq s$.

Lemma 3. *There exists an effectively computable number K_0 such that if $1 \leq h \leq s$, then $H < K_0$.*

Proof. We have

$$p_h^{-f_h \operatorname{ord}_{\wp_h}(\Lambda_b)} \leq c_4(h) e^{-c_3 H},$$

and so

$$\operatorname{ord}_{\wp_h}(\Lambda_b) \geq (c_3 H - \log c_4(h))/(f_h \log p_h) = e_h(c_5(h)H - c_6(h)),$$

where e_h is the ramification index of $\wp_h$. Assume $H > c_6(h)/c_5(h) = c_7(h)$. Then we have $\operatorname{ord}_{\wp_h}(\Lambda_b) > 0$, and so $\operatorname{ord}_{\wp_h}(\alpha_d \tau_d) = 0$. We can find $\mu_i \in K$, $0 \leq i \leq s_d$, such that $\operatorname{ord}_{\wp_h}(\mu_i) = 0$ and

$$\alpha_d \tau_d = \mu_0 \prod_{i=1}^{s_d} \mu_i^{b_{i,d}},$$

where $s_d = t_d$ or $t_d - 1$ for some variables, $b_{i,d}$, which satisfy $|b_{i,d}| \leq H$. Hence by Yu's Theorem [29], we can find constants $c_8(h)$, $c_9(h)$ such that

$$\operatorname{ord}_{\wp_h}\left(\mu_0 \prod_{1}^{s_d} \mu_i^{b_{i,d}} - 1\right) \leq c_8(h) \log H + c_9(h).$$

Then we have, by a lemma of Pethő and de Weger, [19, Lemma 2.2],

$$H \leq \frac{2}{e_h c_5(h)} \left(e_h c_6(h) + c_9(h) + c_8(h) \log\left(\frac{c_8(h)}{e_h c_5(h)}\right)\right) = c_{10}(h).$$

We set

$$K_0 = \max_{1 \leq h \leq s} (c_{10}(h), c_7(h)). \quad \square$$

The μ_i's that appear in the above proof will need to be found for the p-adic reduction step. I shall now describe their construction. Let $n_j = \operatorname{ord}_{\wp_h}(\beta_{j,d})$ for $j = 1, .., t_d$, and $n_0 = \operatorname{ord}_{\wp_h}(\alpha_d)$. If $n_i = 0$ for all i, then we can take $\mu_i = \beta_{i,d}$ and $s_d = t_d$, so we shall assume otherwise. Now choose $k \neq 0$ such that $n_k \neq 0$ and

$$|n_k| = \min_{1 \leq i \leq t_d,\, n_i \neq 0} |n_i|.$$

The condition $\operatorname{ord}_{\wp_h}(\alpha_d \tau_d) = 0$ means that we have the equation

$$n_0 + \sum_{i=1}^{t_d} n_i a_{i,d} = 0.$$

Then set $\mu_k = 1$, and for $j \neq 0$ or k set $\mu_j = \beta_{j,d}^{n_k}\beta_{k,d}^{-n_j}$. Define r_i and $b_{i,d}$ by $a_{i,d} = n_k b_{i,d} + r_i$ with $0 \leq r_i < |n_k|$, and

$$\sigma = -\left(n_0 + \sum_{i=1, i\neq k}^{t_d} n_i r_i\right), \qquad \mu_0 = \alpha_0 \left(\prod_{i=1, i\neq k}^{t_d} \beta_{i,d}^{r_i}\right) \beta_{k,d}^{\sigma/n_k}.$$

We must have $\sigma \equiv 0 \pmod{n_k}$, hence $\mu_0 \in K$. We note that as $\mu_k = 1$, we have reduced the number of variables by 1. So we relabel the μ_i's and set $s_d = t_d - 1$. Note that we shall have a different μ_0 for each possible set $\{r_1, \ldots, r_{t_d}\}$ satisfying $\sigma \equiv 0 \pmod{n_k}$.

From the above proof it can be seen that one has a trivial bound on H in a very special case.

Corollary 1. *If* $\operatorname{ord}_{\wp_h}(\alpha_1\tau_1) = \operatorname{ord}_{\wp_h}(\alpha_2\tau_2)$, *then* $H \leq c_7(h)$.

In our example we shall later employ this result to remove the need for any p-adic linear forms in logarithms.

We now bound H in the case that $s + 1 \leq h \leq r + s + 1$.

Lemma 4. *There exists an effectively computable number* K_1 *such that, if* $s + 1 \leq h \leq r + s + 1$, *then* $H < K_1$.

Proof. Let $k = h - s$ and define

$$(c_{11}(k), c_{12}(k), c_{13}(k)) = \begin{cases} (\log(4c_4(h))/c_3,\ 2c_4(h),\ c_3) & \text{if } \wp_h \text{ is real,} \\ (2\log(4\sqrt{c_4(h)})/c_3,\ 2\sqrt{c_4(h)},\ c_3/2) & \text{if } \wp_h \text{ is complex.} \end{cases}$$

Now if $H \geq c_{11}(k)$, then $|\Lambda_d^{(k)} - 1| \leq 1/4$, and so

$$|\log \Lambda_d^{(k)}| \leq c_{12}(k) e^{-c_{13}(k)H}.$$

The left-hand side of this last inequality is equal to

$$\left|\log(\alpha_d^{(k)}) + \sum_{i=1}^{t_d} a_{i,d} \log(\beta_{i,d}^{(k)}) + a_{0,d} 2\pi\sqrt{-1}\right|,$$

where $|a_{0,d}| \leq (t_d + 1)H$. We now apply the theorem of Baker and Wüstholz [2] to find a constant $c_{14}(k)$ such that $|\log \Lambda_d^{(k)}| > \exp(-c_{14}(k)\log(H(t_d + 1)))$. So $-c_{14}(k)\log(H(t_d + 1)) < -c_{13}(k)H + \log c_{12}(k)$. In other words,

$$H < \frac{1}{c_{13}(k)} (\log(c_{12}(k)) + c_{14}(k)\log(H(t_d + 1))).$$

Hence, again by the lemma of Pethő and de Weger,

$$H < \frac{2}{c_{13}(k)} \left(\log(c_{12}(k)) + c_{14}(k)\log\left(\frac{(t_d + 1)c_{14}(k)}{c_{13}(k)}\right)\right) = c_{15}(k).$$

We finally set

$$K_1 = \max_k (c_{11}(k), c_{15}(k)). \quad \square$$

So in all cases we have a bound on H.

4. The reduction of the bounds

In this section I show how to reduce the bounds. The p-adic reduction step is a slight modification on Evertse's trick, given in [25], which uses an idea given in [27, p. 19]. The complex reduction step uses a similar idea, see [27, p. 16], to remove the need for the use of the complex L^3 reduction algorithm that was used in [21]. Both reduction steps use the real L^3 reduction algorithm on lattices generated by integer matrices. So instead of using the algorithm given in [16], we use the fraction-free algorithm given in [26]. If $\Im$ is a lattice in $\mathbb{R}^n$ and $\underline{y} \in \mathbb{R}^n$, then we define $\ell(\Im, \underline{y})$ by

$$\ell(\Im, \underline{y}) = \begin{cases} \min_{\underline{x} \in \Im, \underline{x} \neq \underline{0}} \|\underline{x}\| & \text{if } \underline{y} = \underline{0}, \\ \min_{\underline{x} \in \Im} \|\underline{x} - \underline{y}\| & \text{otherwise.} \end{cases}$$

For properties of L^3 bases I refer the reader to the discussion in [27].

p-adic reduction step. Assume that $1 \leq h \leq s$; then $\operatorname{ord}_{p_h}(\Lambda_b) \geq c_5(h)H - c_6(h)$. Now, as in the proof of Lemma 3, if $H > (1 + c_6(h))/c_5(h) = c_{16}(h) > c_7(h)$, then

$$\Lambda_b = \mu_0 \prod_1^{s_d} \mu_i^{b_{i,d}} - 1,$$

where $\operatorname{ord}_{\wp_h}(\mu_i) = 0$ for all i. As $H > c_{16}(h)$, we have $\operatorname{ord}_{p_h}(\Delta_b) \geq 1$. So

$$\operatorname{ord}_{p_h}(\Delta_b) = \operatorname{ord}_{p_h}(\log_{p_h}(\Lambda_b + 1)) = \operatorname{ord}_{p_h}(\Lambda_b) \geq c_5(h)H - c_6(h),$$

where

$$\Delta_b = \log_{p_h} \mu_0 + \sum_{i=1}^{s_d} b_{i,d} \log_{p_h} \mu_i \in K_{\wp_h}.$$

Let $n_h = [K_{\wp_h} : \mathbb{Q}_{p_h}]$ and $K_{\wp_h} = \mathbb{Q}_{p_h}(\phi_h)$; then

$$\Delta_b = \sum_{i=0}^{n_h - 1} \Delta_{b,i} \phi_h^i,$$

where

$$\Delta_{b,i} = \alpha_{0,i} + \sum_{j=1}^{s_d} b_{j,d} \alpha_{j,i}, \qquad \alpha_{j,i} \in \mathbb{Q}_{p_h}, \quad 0 \leq i \leq n_h - 1.$$

By Evertse's trick, [25, p. 257], it follows that, for all i,

$$\operatorname{ord}_{p_h}(\Delta_{b,i}) \geq c_5(h)H - c_6(h) - \frac{1}{2} D_{p_h}(\phi_h),$$

where $D_{p_h}(\phi_h) = \operatorname{ord}_{p_h}(\operatorname{Disc}(\phi_h))$. Choose $\lambda \in \mathbb{Q}_{p_h}$ such that

$$\operatorname{ord}_{p_h}(\lambda) = \min_{1 \leq i \leq s_d} \left(\min_{0 \leq j \leq n_h - 1} (\operatorname{ord}_{p_h}(\alpha_{i,j})) \right) = c_{17}(h).$$

Note. If $c_{17}(h) \geq \operatorname{ord}_{p_h}(\alpha_{0,i})$ for some i, then

$$H \leq \frac{1}{c_5(h)}\left(c_{17}(h) + c_6(h) + \frac{1}{2}D_{p_h}(\phi_h)\right).$$

So we shall assume that $c_{17}(h) < \min(\operatorname{ord}_{p_h}(\alpha_{0,i}))$. Then

$$\operatorname{ord}_{p_h}(\Delta_{b,i}/\lambda) \geq c_5(h)H - c_6(h) - \frac{1}{2}D_{p_h}(\phi_h) - c_{17}(h) = c_5(h)H - c_{18}(h),$$

and we set

$$\Delta_{b,i}/\lambda = \kappa_{0,i} + \sum_{j=1}^{s_d} b_{j,d}\kappa_{j,i}, \qquad \kappa_{j,i} \in \mathbb{Z}_{p_h},\ 0 \leq i \leq n_h - 1.$$

Choose u such that $p_h^u \approx K_0^{(1+s_d)/n_h}$. For $\alpha \in \mathbb{Z}_{p_h}$, let $\alpha^{(u)}$ denote the unique rational integer such that $0 \leq \alpha^{(u)} \leq p_h^u - 1$ and $\alpha \equiv \alpha^{(u)} \pmod{p_h^u}$. Then set

$$\mathscr{B} = \begin{pmatrix} 1 & & & & 0 & \\ & \ddots & & & & \\ 0 & & 1 & & & \\ \kappa_{1,0}^{(u)} & \cdots & \kappa_{s_d,0}^{(u)} & p_h^u & & 0 \\ \vdots & & \vdots & & \ddots & \\ \kappa_{1,n_h-1}^{(u)} & \cdots & \kappa_{s_d,n_h-1}^{(u)} & 0 & & p_h^u \end{pmatrix} \in \mathbb{Z}^{(s_d+n_h)\times(s_d+n_h)},$$

$$\underline{y} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -\kappa_{0,0}^{(u)} \\ \vdots \\ -\kappa_{0,n_h-1}^{(u)} \end{pmatrix} \in \mathbb{Z}^{s_d+n_h}.$$

Let $\mathfrak{I}$ denote the lattice generated over $\mathbb{Z}$ by the columns of $\mathscr{B}$. Now Lemmas 3.4, 3.5, and 3.6 of [27] give us a lower bound on $\ell(\mathfrak{I}, \underline{y})$, and using the next lemma, we can probably reduce our bound for H.

Lemma 5. *If* $\ell(\mathfrak{I}, \underline{y}) > \sqrt{s_d}K_0$, *then* $H < (u + c_{18}(h))/c_5(h)$.

Proof. Assume $H \geq (u + c_{18}(h))/c_5(h)$; then $c_5(h)H - c_{18}(h) \geq u$, i.e., $\operatorname{ord}_{p_h}(\Delta_{b,i}/\lambda) \geq u$ for all $i = 0, \ldots, n_h - 1$. Then

$$\operatorname{ord}_{p_h}\left(\kappa_{0,i}^{(u)} + \sum_{j=1}^{s_d} b_{j,d}\kappa_{j,i}^{(u)}\right) \geq u.$$

So, for all i,

$$z_i = \frac{\kappa_{0,i}^{(u)} + \sum_{j=1}^{s_d} b_{j,d}\kappa_{j,i}^{(u)}}{p_h^u} \in \mathbb{Z}.$$

Therefore, we can consider the lattice point

$$\underline{x} = \mathscr{B} \begin{pmatrix} b_{1,d} \\ \vdots \\ b_{s_d,d} \\ -z_0 \\ \vdots \\ -z_{n_h-1} \end{pmatrix} = \begin{pmatrix} b_{1,d} \\ \vdots \\ b_{s_d,d} \\ -\kappa_{0,0}^{(u)} \\ \vdots \\ -\kappa_{0,n_h-1}^{(u)} \end{pmatrix}.$$

Hence,

$$\underline{x} - \underline{y} = \begin{pmatrix} b_{1,d} \\ \vdots \\ b_{s_d,d} \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

i.e.,

$$\ell(\Im, \underline{y})^2 \leq \sum_{i=1}^{s_d} b_{j,d}^2 \leq s_d K_0^2. \quad \square$$

Note that in this p-adic method the value of u can be chosen to be smaller than that in the original version given in [25]. This means the p-adic logarithms do not have to be calculated to such a high accuracy as with previous methods. If our choice of u does not result in a new upper bound, we choose a larger u and repeat the process. Once a new upper bound has been found, we then choose a smaller u to try and reduce this new bound.

Complex reduction step. Assume that $s+1 \leq h \leq r+s+1$. Let $k = h - s$ and

$$\Lambda = \log(\alpha_d^{(k)}) + \sum_{i=1}^{t_d} a_{i,d} \log(\beta_{i,d}^{(k)}) + a_{0,d} 2\pi\sqrt{-1}.$$

By Lemma 4 we have the bounds $|a_{i,d}| \leq K_1$ and $|a_{0,d}| \leq (t_d+1)K_1$. Now if $H \geq c_{11}(k)$, then

$$|\Lambda| \leq c_{12}(k) e^{-c_{13}(k)H}.$$

Our objective is to find a new bound, K_1, which is lower than our original bound given by Lemma 4. Previously, we would have used the complex L^3 algorithm developed in [21]. We now show that this is unnecessary.

Write Λ as $\Lambda = \kappa_0 + \sum_{i=1}^{t_d} a_{i,d}\kappa_i + a_{0,d} 2\pi\sqrt{-1}$. There are three cases to consider.

Case 1. Totally Real, i.e., for all i, $\kappa_i \in \mathbb{R}$.

Case 2. Pure Imaginary, i.e., for all i, $\sqrt{-1}\kappa_i \in \mathbb{R}$.

Case 3. Mixed Case otherwise.

Cases 1 and 2 are dealt with in [23]; therefore, we shall only consider here Case 3.

Case 3. Choose a constant C such that $C \approx K_1^{(t_d+1)/2}$ and relabel $\{\kappa_1, \ldots, \kappa_{t_d}\}$ such that $\mathrm{Re}(\kappa_{t_d}) \neq 0$. Then define $\Im$ to be the lattice generated by the columns of the matrix

$$\mathscr{B} = \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ 0 & & 1 & & \\ [C\ \mathrm{Re}(\kappa_1)] & \ldots & \ldots & [C\ \mathrm{Re}(\kappa_{t_d})] & 0 \\ [C\ \mathrm{Im}(\kappa_1)] & \ldots & \ldots & [C\ \mathrm{Im}(\kappa_{t_d})] & [C2\pi] \end{pmatrix} \in \mathbb{Z}^{(t_d+1)\times(t_d+1)}.$$

Let

$$\underline{y} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -[C\ \mathrm{Re}(\kappa_0)] \\ -[C\ \mathrm{Im}(\kappa_0)] \end{pmatrix} \in \mathbb{Z}^{t_d+1},$$

where $[\cdot]$ denotes rounding to the nearest integer. We find a lower bound K_2 on $\ell(\Im, \underline{y})$ by Lemmas 3.4, 3.5, and 3.6 of [27], and define S and T as follows:

$$S = \sqrt{K_2^2 - (t_d - 1)K_1^2}\,, \qquad T = (1 + (2t_d + 1)K_1)/\sqrt{2}.$$

Lemma 6. *If* $K_2^2 \geq T^2 + (t_d - 1)K_1^2$, *then*

$$H \leq \frac{1}{c_{13}(k)} (\log(Cc_{12}(k)) - \log(S - T)).$$

Proof. Define Φ_1, Φ_2 as follows:

$$\Phi_1 = [C\ \mathrm{Re}(\kappa_0)] + \sum_{i=1}^{t_d} a_{i,d}[C\ \mathrm{Re}(\kappa_i)],$$

$$\Phi_2 = [C\ \mathrm{Im}(\kappa_0)] + \sum_{i=1}^{t_d} a_{i,d}[C\ \mathrm{Im}(\kappa_i)] + a_{0,d}[C2\pi].$$

Notice that $|\Phi_1 + \sqrt{-1}\Phi_2 - C\Lambda| \leq T$; therefore,

$$|\Phi_1 + \sqrt{-1}\Phi_2| \leq T + Cc_{12}(k)e^{-c_{13}(k)H}.$$

Now consider the lattice point $\underline{x} = \mathscr{B}\underline{z}$, where

$$\underline{z} = \begin{pmatrix} a_{1,d} \\ \vdots \\ a_{t_d,d} \\ a_{0,d} \end{pmatrix}, \quad \text{so} \quad \underline{x} - \underline{y} = \begin{pmatrix} a_{1,d} \\ \vdots \\ a_{t_{d-1},d} \\ \Phi_1 \\ \Phi_2 \end{pmatrix}.$$

Therefore,

$$\ell(\Im, \underline{y})^2 \leq \sum_{i=1}^{t_d-1} a_{i,d}^2 + \Phi_1^2 + \Phi_2^2 \leq (t_d - 1)K_1^2 + |\Phi_1 + \sqrt{-1}\Phi_2|^2$$
$$\leq (t_d - 1)K_1^2 + \left(T + Cc_{12}(k)e^{c_{13}(k)H}\right)^2.$$

Note by assumption that $S \in \mathbb{R}$, so we have $S - T \leq Cc_{12}(k)e^{c_{13}(k)H}$, and hence the inequality for H follows. □

We expect this result to reduce our upper bound for H, as we believe the logarithms of algebraic numbers to behave as random complex numbers. Therefore we expect to reduce the bound. All experience shows (see [5, 22, 23, 24]) that this is indeed the case. As in the p-adic case, if we do not reduce our upper bound, then we choose a larger C and repeat the process.

5. Locating the solutions

When solving an exponential diophantine equation, we often need to sieve the solutions, that is, find a set of congruence conditions on the exponents involved. In our case we have

$$\alpha_1 \beta_{1,1}^{a_{1,1}} \cdots \beta_{t_1,1}^{a_{t_1,1}} + \alpha_2 \beta_{1,2}^{a_{1,2}} \cdots \beta_{t_2,2}^{a_{t_2,2}} + 1 = 0, \tag{3}$$

where the $\beta_{i,j} \in \mathbb{Z}_K$ are given, the α_j come from a finite set $\mathscr{A}$ and the $a_{i,j} \in \mathbb{Z}$ need to be found for $1 \leq i \leq t_j$ and $j = 1, 2$. We may have some additional information in the form of linear equations amongst the $a_{i,j}$'s which need to be satisfied. In this case sieving the equation means finding congruence conditions on the $a_{i,j}$'s. The idea of sieving an equation to locate the solutions goes back to [24]. The S-unit equations that were considered in that paper were very simple to sieve, as they had $t_1 = t_2$ and $a_{i,1} = a_{i,2}$ for all i. For the more general S-unit equation one has to be more careful when organizing the sieving process, because there are many more cases to consider. Unlike [25], we find it more efficient to find the $a_{i,j}$'s up to congruence rather than enumerate all $a_{i,j}$'s up to our previously given upper bounds and then sieve all these cases. As the modulus for our congruences becomes larger, one can make use of the previously given upper bound to speed up the process. Often, however, a parallel computer is required. We explain how to organize the computations below.

We now choose a rational prime p such that the minimal polynomial of a generator of the field K splits completely in $\mathbb{F}_p$, p does not divide the discriminant of the polynomial and p does not lie below a prime of S_f. Also p should be chosen such that the α_i's have a well-defined image in $\mathbb{F}_p$ for $i = 1, 2$, as explained below. This is to force the $\beta_{i,j}$'s to have small order when working modulo p. As K is a galois field, we expect, see [15, §8.4], that on average $1/n$ primes split completely in the field K. So, although one cannot guarantee that such small primes, say $p \leq 300$, exist, we expect that they do. Experience shows this indeed to be the case. We then solve equation (3) modulo p by working over the field $\mathbb{F}_p$ and enumerating all possibilities for the $a_{i,j}$ modulo $p - 1$.

Once this initial sieve has been performed, the given solutions can be sieved again by another prime until one has enough congruence conditions to easily locate all the actual solutions of equation (3). Note the smallest prime should be used first, as this is the time-critical step. This is contrary to the advice given in [25], and is dictated by the larger number of cases that we have to consider. After the first prime, the $a_{i,j}$'s will be determined modulo $p_1 - 1$. After the second prime, they will be determined modulo the least common multiple of $p_1 - 1$ and $p_2 - 1$, and so on.

I now explain how one should organize finding the solutions for the smallest prime. Now for each conjugate of the field K, there is a completion of K with respect to the prime p; the primes p have been chosen so that this completion always lies in $\mathbb{Q}_p$. Hence, we have n images of U_S in $\mathbb{F}_p$ given by the roots of the minimal polynomial modulo p. With these roots it is easy to calculate the numbers $\beta_{i,j}$ modulo p for each such image. We then have n equations of the type (3) to solve modulo p.

Now each $\beta_{i,j}$ has an order in each image, say $o_{i,j,k}$, $1 \leq k \leq n$. Reordering the roots if necessary, we can assume that

$$\prod_{i,j} o_{i,j,k} \leq \prod_{i,j} o_{i,j,k+1}, \qquad 1 \leq k \leq n-1.$$

So searching in the box corresponding to the first root will be fast in comparison to searching in the other boxes. Hence, we solve the equations in the order given by the above ordering of the roots, i.e., by simply testing each possible congruence modulo p. We also take into account any linear equations that may exist amongst the exponential variables. It transpires that the search for the solutions with respect to the second root is now the most expensive in terms of CPU-time.

If required, the system can be parallelized as follows: The first process solves the equation with respect to the first prime and the first root, with respect to the ordering above. The solutions of this are then farmed to workers who solve the equation with respect to the first prime and the other $n - 1$ roots. The results from the workers are then harvested and passed to the next process. The $a_{i,j}$'s determined up to congruence are then passed down a chain which solves the equation modulo other primes, thus giving higher modulo congruences on the $a_{i,j}$'s via the Chinese remainder theorem. These last processes will hardly have any data sent to them, so this last part of the chain should have one prime on each process. The results give the congruence conditions on the solutions $a_{i,j}$.

This method should also be used when using a serial computer, as it leads to significant improvements in CPU-time when compared to the original brute-force approach.

6. Connecting the solutions together

Having given a method to derive upper bounds on the variables in an S-unit equation, and shown how to reduce them, we now use this to solve our TCDF equation. We shall use some arguments from the proof of Theorem 1 of [9] (see also [7] and [11]), where an explicit upper bound is given for the solutions of equation (1). For each set of solutions of the S-unit equations represented

by $\mathscr{C}$, we use the action of G to produce a set of solutions of a connected set of S-unit equations.

Before proceeding further, we need to calculate a constant for use later on. Choose $I = \{i_1, \ldots, i_v\}$ and $J = \{j_1, \ldots, j_v\}$, with $1 \leq i_k \leq m$ and $1 \leq j_k \leq n$, such that the matrix

$$A_{I,J} = \begin{pmatrix} l_{1,i_1}^{(j_1)} & \cdots & l_{v,i_1}^{(j_1)} \\ \vdots & & \vdots \\ l_{1,i_v}^{(j_v)} & \cdots & l_{v,i_v}^{(j_v)} \end{pmatrix}$$

is invertible. By Assumption 2 such I and J must exist. We have, obviously, $\det(A_{I,J}) \in \mathbb{Z}_K$. So set

$$c_{19} = |N_{K/\mathbb{Q}}(\det(A_{I,J}))|.$$

We then have the following result:

Lemma 7. *Let $\chi \in \mathbb{Z}$ and $\xi_j \in \mathbb{Z}_K$ be such that $L_j(\underline{x}) = \chi\xi_j$; then we have $|\chi|^n \leq c_{19}$.*

Proof. With the choice of I and J above we have $A_{I,J}\underline{x} = \chi\underline{b}$, where $\underline{b} = (\xi_{i_1}^{(j_1)}, \ldots, \xi_{i_v}^{(j_v)})^t$. Now by Cramer's rule,

$$x_i = \chi \det(A_{I,J}^{(i)})/\det(A_{I,J}),$$

where $A_{I,J}^{(i)}$ is the matrix obtained from $A_{I,J}$ by replacing column i of $A_{I,J}$ by the vector $\underline{b}$. Let $y_i = \det(A_{I,J}^{(i)})$ and $y = \det(A_{I,J})$; then $y_i, y \in \mathbb{Z}_K$ and $x_i = \chi y_i/y$. This implies that

$$(\chi) \cdot (y_1, \ldots, y_v) = (x_1, \ldots, x_v) \cdot (y) = (y),$$

and so $|N_{K/\mathbb{Q}}(\chi)| \leq |N_{K/\mathbb{Q}}(y)| = c_{19}$. □

By Assumption 1, for each j, $1 \leq j \leq m$, there exists a sequence

$$L_2 = L_{i_1}, \ldots, L_{i_w} = L_j$$

such that for all u, $1 \leq u \leq w-1$, there exists $\alpha_{i_u}, \alpha_{i_{u+1}}, \alpha_{i_u,u+1}$ such that

$$\alpha_{i_u}L_{i_u} + \alpha_{i_{u+1}}L_{i_{u+1}} + \alpha_{i_u,u+1}L_{i_u,u+1} = 0.$$

If we let κ_i denote our solutions for the L_i above, then

$$\begin{aligned} L_1 &= \sigma'\kappa_1, \qquad L_2 = \sigma'\kappa_2, \\ L_{i_u} &= \sigma_u'\kappa_{u,i_u}, \quad L_{i_{u+1}} = \sigma_u'\kappa_{u,i_{u+1}}, \end{aligned}$$

where σ' and σ_u' are unknown S-units. We then find that for all j, $1 \leq j \leq m$,

$$L_j = L_{i_w} = \kappa_{w-1,i_w}L_{i_{w-1}}/\kappa_{w-1,i_{w-1}} = \cdots = \sigma'\phi_j/\psi_j = \sigma'\lambda_j,$$

where

$$\phi_j = \kappa_2 \prod_{u=1}^{w-1} \kappa_{u,i_{u+1}}, \qquad \psi_j = \prod_{u=1}^{w-1} \kappa_{u,i_u}.$$

Let $\pi_1, \ldots, \pi_s$ be elements of K such that $(\pi_i) = \wp_i^{h_K}$, where $\wp_i$ are prime ideals dividing $(a_0 A p_1 \cdots p_t)$. Let

$$\Delta = \left\{ \delta : \begin{array}{c} (\delta) = \wp_1^{a_1} \cdots \wp_s^{a_s} : 0 \le a_i < h_K, \\ \delta_1, \delta_2 \in \Delta \text{ implies } \delta_1 \text{ and } \delta_2 \text{ are not associates.} \end{array} \right\}.$$

For $\epsilon \in U_K$ and $\delta \in \Delta$ we have

$$\sigma' = \epsilon \delta \pi_1^{a_1'} \cdots \pi_s^{a_s'}.$$

Now for each $\delta \in \Delta$ repeat the following:

For $1 \le k \le s$ choose b_k to be the smallest integer such that for all i, $1 \le i \le m$,

$$b_k h_K \ge -\operatorname{ord}_{\wp_k}(\delta \lambda_i).$$

If $b_k > a_k'$, then, for some j, we have

$$\begin{aligned} \operatorname{ord}_{\wp_k}(\sigma' \lambda_j) &= h_K a_k' + \operatorname{ord}_{\wp_k}(\delta \lambda_j) \\ &\le h_K(b_k - 1) + \operatorname{ord}_{\wp_k}(\delta \lambda_j) < 0, \end{aligned}$$

so $L_j \notin \mathbb{Z}_K$ which is a contradiction. So we must have $b_k \le a_k'$. Set $a_k = a_k' - b_k \ge 0$ and then

$$\delta_j = \pi_1^{b_1} \cdots \pi_s^{b_s} \delta \lambda_j, \qquad \sigma = \epsilon \pi_1^{a_1} \cdots \pi_s^{a_s},$$

where $\epsilon \in U_K$. So $\delta_j \in \mathbb{Z}_K$ and $L_j = \sigma \delta_j$ for $j = 1, \ldots, m$.

7. Bounding the a_i's

Let p_i denote the primes of $\mathbb{Z}$, $1 \le i \le u$, which divide $(a_0 A p_1 \cdots p_t)$, therefore, in particular $u \ge t$. Then for some $g_1, \ldots, g_u \in \mathbb{N}$

$$\left(\prod_{i=1}^{m} L_i \right) = \left(\sigma^m \prod_{i=1}^{m} \delta_i \right) = p_1^{g_1} \cdots p_u^{g_u}.$$

Fix k such that $1 \le k \le u$, and let $\wp$ denote an arbitrary prime ideal of K lying above p_k. If $\wp^{e_k} \| p_k$, then e_k does not depend on the choice of $\wp$ since $K/\mathbb{Q}$ is a galois extension.

Let d_k be the greatest rational integer for which

$$g_k e_k - \operatorname{ord}_{\wp} \left(\prod_{i=1}^{m} \delta_i \right) \ge m d_k e_k \tag{4}$$

holds for each $\wp$ with $\wp | p_k$. Note that it is easy to see that $d_k \ge 0$. Now by definition there exists a $\wp$ lying above p_k such that

$$m(d_k + 1) e_k > g_k e_k - \operatorname{ord}_{\wp} \left(\prod_{i=1}^{m} \delta_i \right). \tag{5}$$

By (4) we see that $g_k e_k - m d_k e_k \ge 0$, and by (5) we have

$$0 \le g_k e_k - m d_k e_k < m e_k + \operatorname{ord}_{\wp} \left(\prod_{i=1}^{m} \delta_i \right).$$

Note that for an arbitrary ideal $\wp$ lying above p_k, with $\wp|(\pi_q)$,

$$a_q m h_K + \mathrm{ord}_\wp\left(\prod_{i=1}^{m}\delta_i\right) = g_k e_k. \tag{6}$$

If $p_k \notin \{p_1, \ldots, p_t\}$, then g_k is fixed and we have determined a_q; otherwise, we have $0 \leq a_q \leq e_k(1+d_k)/h_K$. So if we can bound d_k, then we can bound a_q.

Now let $\chi \in \mathbb{Z}$ be such that $\chi = p_1^{d_1}\cdots p_u^{d_u}$ and choose ξ such that $\chi\xi = \pi_1^{a_1}\cdots\pi_s^{a_s}$. It follows that

$$\mathrm{ord}_\wp(\chi\xi) = h_K a_q = e_k d_k + \mathrm{ord}_\wp(\xi).$$

So, from equations (4) and (6), we deduce that ξ is an algebraic integer. Write $\xi_j = \epsilon\xi\delta_j$; then $L_j(\underline{x}) = \chi\xi_j$. Then we apply Lemma 7 to find $|\chi|^n \leq c_{19}$. Hence, if we set $c_{20} = \log c_{19}/n$, then

$$d_k \leq c_{20}/\log p_k.$$

8. Finding the solutions

Therefore, we have a finite set of cases,

$$L_j = \epsilon\pi_1^{a_1}\cdots\pi_s^{a_s}\delta_j,$$

with the a_i and δ_j given, and we have the equation

$$\epsilon^m\pi_1^{ma_1}\cdots\pi_s^{ma_s}\prod_{i=1}^{m}\delta_j = a_0^{m-1}Ap_1^{z_1}\cdots p_t^{z_t}.$$

Now, take ord_{p_i} of both sides to completely determine the z_i.

If K has fundamental units $\eta_1, \ldots, \eta_r$, then ϵ is of the form

$$\epsilon = \xi\eta_1^{v_1}\cdots\eta_r^{v_r}, \qquad \xi \in \mathrm{Tors}(U_K).$$

So we have, for some given $\phi \in U_K$,

$$\left(\xi\eta_1^{v_1}\cdots\eta_r^{v_r}\right)^m = \phi. \tag{7}$$

This gives us the matrix equation

$$\begin{pmatrix} \log|\eta_1^{(1)}| & \cdots & \log|\eta_r^{(1)}| \\ \vdots & & \vdots \\ \log|\eta_1^{(r+1)}| & \cdots & \log|\eta_r^{(r+1)}| \end{pmatrix}\begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix} = \frac{1}{m}\begin{pmatrix} \log|\phi^{(1)}| \\ \vdots \\ \log|\phi^{(r+1)}| \end{pmatrix}.$$

Hence we can solve for $v_1, \ldots, v_r$. This will be a floating-point solution. To obtain an integral solution, we round the result and test it in equation (7).

Another method to solve for $v_1, \ldots, v_r$ is to find $a_0, A, p_1, \ldots, p_t$ in terms of the generators of the S-units of K. We know the δ_i in terms of such generators. Hence, ϕ can be written down as a product of powers of the fundamental

units of K and a unit of finite order. The unknowns $v_1, \ldots, v_r$ can then be simply read off.

We have the equations (with $x_i \in \mathbb{Z}$ unknown)

$$\sum_{i=1}^{v} l_{i,j} x_i = \xi \eta_1^{v_1} \cdots \eta_r^{v_r} \pi_1^{a_1} \cdots \pi_s^{a_s} \delta_j = \tau_j \ , \qquad 1 \le j \le m.$$

Let $\mathbb{Z}_K$ have an integral basis, $\omega_1, \ldots, \omega_n$. Then we can write τ_i and $l_{i,j}$ in terms of this basis as

$$\tau_i = \sum_{j=1}^{n} t_{i,j} \omega_j \ , \quad l_{i,j} = \sum_{k=1}^{n} r_{i,j,k} \omega_k \ , \qquad t_{i,j}, \ r_{i,j,k} \in \mathbb{Z}.$$

Hence, we have the $m \cdot n$ linear equations with $\mathbb{Z}$ coefficients and variables, given by,

$$\sum_{i=1}^{v} r_{i,j,k} \, x_i = t_{j,k} \ , \qquad 1 \le j \le m \ , \ 1 \le k \le n.$$

We solve for the x_i's to obtain our final solution $(x_1, \ldots, x_v)$, which we check to satisfy

$$F(\underline{x}) = A p_1^{z_1} \cdots p_t^{z_t} \quad \text{and} \quad \gcd(\underline{x}) = 1.$$

9. Example

Suppose we wish to find all monic quintic polynomials with integral coefficients and with discriminant a product of powers of two and three only, which factor over $\mathbb{Q}$ as a product of one quadratic polynomial and one cubic polynomial. We first need to decide on the splitting fields of the two polynomials. Here I will deal with the case where the quadratic polynomial factors over $\mathbb{Q}(\alpha)$ and the cubic factors over $\mathbb{Q}(\beta)$, where

$$\alpha^2 + 3 = 0 \ , \qquad \beta^3 - 3\beta - 1 = 0.$$

Hence, I will be able to give a list, by [18], of curves of genus 2 with one rational Weierstrass point (at infinity), two Weierstrass points in $\mathbb{Q}(\alpha)$ and three in $\mathbb{Q}(\beta)$ with good reduction outside the set $\{2, 3\}$.

9.1. **The initial bounds and reduction.** Set $K = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$, where $f = \theta^6 - \theta^3 + 1 = 0$. By using the package KANT, [20], we find that K has unit group given by $U_K = \langle \xi \rangle \times \langle \eta_1 \rangle \times \langle \eta_2 \rangle$, where $\xi = \theta^5$ is a generator of the 18 units of finite order and $\eta_1 = \theta^2 - \theta^3$, $\eta_2 = 1 - \theta^2 - \theta^3 + \theta^4 + \theta^5$ are fundamental units. There is only one prime ideal above each of the rational primes 2 and 3, and both of these ideals are principal,

$$(2) = \wp_2 \ , \qquad (3) = \wp_3^6 = (1 - \theta^3 + \theta^4)^6.$$

We let $\pi = 1 - \theta^3 + \theta^4$. In our previous notation we let $S_f = \{\wp_2, \wp_3\}$.

We denote the roots of f by $\theta_1, \ldots, \theta_6$ and we order them in such a way that we have

$$\theta_1 = \theta = \xi^{11}, \quad \theta_2 = -\theta^2 = \xi^{13}, \quad \theta_3 = -\theta^4 = \xi^{17},$$
$$\theta_4 = -\theta^5 + \theta^2 = \xi^7, \quad \theta_5 = \theta^4 - \theta = \xi^5, \quad \theta_6 = \theta^5 = \xi.$$

The galois group of $K/\mathbb{Q}$ is then given by $G = \langle\sigma\rangle$, where $\sigma = (123456)$. We have that

$$\alpha^{(1)} = \alpha = \xi^{14}\eta_1^{-1}\eta_2^{-1}\pi^3, \quad \beta^{(1)} = \xi^{13}\eta_1$$

and

$$\sigma(\alpha^{(1)}) = \alpha^{(2)} = -\alpha,$$
$$\sigma(\beta^{(1)}) = \beta^{(3)}, \quad \sigma(\beta^{(2)}) = \beta^{(1)}, \quad \sigma(\beta^{(3)}) = \beta^{(2)}.$$

The automorphism σ acts on η_i and π in the following way:

$$\sigma(\eta_1) = \eta_2^{-1}\xi^{13}, \quad \sigma(\eta_2) = \eta_1\eta_2^{-1}\xi^{13}, \quad \sigma(\pi) = \pi\eta_2^{-1}\xi^{13}.$$

We let

$$\gamma = a + b(1+\alpha)/2, \quad \delta = c + d(t\beta + v\beta^2),$$

where $a, c, t, v \in \mathbb{Z}$ with $(t, v) = 1$ and $b, d \in \{\pm 2^{s_1}3^{s_2} : s_1, s_2 \in \mathbb{N}\}$. Now $\Gamma_{i,j} = \gamma^{(i)} - \delta^{(j)}$ must be an S-unit of K for $i = 1, 2$ and $j = 1, 2, 3$. This means that $2\Gamma_{i,j}$ is also an S-unit of K, so we set $x_1 = 2a + b - 2c$, $x_2 = b$, $x_3 = -2dt$, $x_4 = -2dv$ and form the linear forms

$$l_{2i-1} = x_1 + x_2\alpha + x_3\beta^{(i)} + x_4\beta^{(i)2},$$
$$l_{2i} = x_1 - x_2\alpha + x_3\beta^{(i)} + x_4\beta^{(i)2},$$

for $i = 1, 2, 3$. Then $L_1 \cdots L_6 \in \mathbb{Z}[x_1, \ldots, x_4]$ is a decomposable form, but it is not triangularly connected. But we can produce a triangularly connected form by also defining $L_7 = 2x_2\alpha$. Then we have a new form $F(x_1, \ldots, x_4)$, which is triangularly connected, given by

$$F(\underline{x}) = L_7(\underline{x})^2 \prod_{i=1}^{6} L_i(\underline{x}) \in \mathbb{Z}[\underline{x}].$$

This is a TCDF, as we have $L_{2i-1} - L_{2i} - L_7 = 0$ for $i = 1, 2, 3$. Note that we have the relations

$$(8) \quad \sigma^3(L_{2i-1}) = L_{2i}, \quad \sigma(L_1) = L_6, \quad \sigma^2(L_1) = L_3, \quad \sigma(L_7) = -L_7.$$

We wish to solve the equation

$$F(\underline{x}) = L_7^2 \prod_{i=1}^{6} L_i = \pm 2^{z_1}3^{z_2}.$$

In view of the relations (8), we need only solve one S-unit equation, namely

$$\frac{L_1}{L_7} - \frac{L_2}{L_7} - 1 = 0.$$

Also, as we have $\sigma^3(L_1/L_7) = -L_2/L_7$, this becomes

$$\frac{L_1}{L_7} + \sigma^3\left(\frac{L_1}{L_7}\right) - 1 = 0.$$

We set

$$\frac{L_1}{L_7} = \xi^a \eta_1^{a_1} \eta_2^{a_2} 2^{a_3} \pi^{a_4}.$$

Then we have the following S-unit equation to solve:

$$\xi^a \eta_1^{a_1} \eta_2^{a_2} 2^{a_3} \pi^{a_4} + \xi^{17a+8a_1+12a_2+7a_4} \eta_1^{a_1} \eta_2^{a_2} 2^{a_3} \pi^{a_4} - 1 = 0.$$

So we have four exponential variables to bound and locate, rather than the initial eight exponential variables. We apply the previous algorithm for S-unit equations, noting that we can use Corollary 1. This gives initial bounds of $K_0 = 3.9$ and $K_1 = 2.0 \times 10^{32}$. We apply the reduction algorithms to obtain $H \leq 245$. Then we sieve the equation to find all solutions to this S-unit equation; they are given by the following table.

a	3	15	4	6	13	17	2	12	0	7	10	3	8	4	15	2	3
a_1	0	0	-1	-1	0	0	1	1	0	1	1	0	0	1	1	0	0
a_2	0	0	0	0	1	1	-1	-1	0	1	1	0	0	0	0	1	1
a_3	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0
a_4	0	0	0	0	0	0	0	0	0	-3	-3	-1	-1	-1	-1	-1	-1

It took 39 hours and 18 minutes to find all these solutions on a SUN-4 and to show that these were the only solutions. The code to do this was written in $c++$. This was with a serial sieve. If the sieve had been performed in parallel, on a MEIKO Transputer Surface, then the whole algorithm would have taken 23 hours.

From the above solutions to our S-unit equation we need to locate the solutions to our TCDF. This takes about 2 minutes of CPU-time. I shall now explain the details.

If we set $L_7 = \tau'$, then we can express all of our linear forms in terms of τ' and $a, a_1, .., a_4$ as follows:

$$\begin{aligned}
L_1 &= \tau' \xi^a \eta_1^{a_1} \eta_2^{a_2} 2^{a_3} \pi^{a_4}, \\
L_2 = \sigma^3(L_1) &= \tau' \xi^{9+17a+8a_1+12a_2+7a_4} \eta_1^{a_1} \eta_2^{a_2} 2^{a_3} \pi^{a_4}, \\
L_3 = \sigma^2(L_1) &= \tau' \xi^{13a+4a_1+17a_2+17a_4} \eta_1^{-a_1-a_2-a_4} \eta_2^{a_1} 2^{a_3} \pi^{a_4}, \\
L_4 = \sigma^5(L_1) &= \tau' \xi^{9+5a+11a_2} \eta_1^{-a_1-a_2-a_4} \eta_2^{a_1} 2^{a_3} \pi^{a_4}, \\
L_5 = \sigma^4(L_1) &= \tau' \xi^{7a+11a_1+a_2} \eta_1^{a_2} \eta_2^{-a_1-a_2-a_4} 2^{a_3} \pi^{a_4}, \\
L_6 = \sigma(L_1) &= \tau' \xi^{9+11a+13a_1+13a_2+13a_4} \eta_1^{a_2} \eta_2^{-a_1-a_2-a_4} 2^{a_3} \pi^{a_4}.
\end{aligned}$$

We check that $L_3 - L_4 - \tau' = 0$ and $L_5 - L_6 - \tau' = 0$. This can be done by referring to the table of solutions of $L_1 - L_2 - \tau' = 0$ given above.

We then set $\tau' = \epsilon 2^{a_1'} \pi^{a_2'} = 2x_2\alpha$ and carry out the following for each of our solutions to the S-unit equation. Set $b_1 = -a_3$ and $b_2 = -a_4$. Then put $a_1'' = a_1' - b_1$, $a_2'' = a_2' - b_2$, and $\lambda_j = L_j/\tau'$. For $j = 1, ..., 7$ we set

$$\delta_j = 2^{b_1} \pi^{b_2} \lambda_j, \quad \tau = \epsilon 2^{a_1''} \pi^{a_2''}, \quad L_j = \tau \delta_j.$$

We find that $c_{19} = 8916100448256$, so we apply our method to find that

$$0 \leq a_1'' \leq 8, \qquad 0 \leq a_2'' \leq 34.$$

We now need to find ϵ, but we note that this is easy, as we have for $x_2 = \pm 2^{g_1}3^{g_2}$

$$\tau = \epsilon 2^{a_1''}\pi^{a_2''} = \frac{2x_2\alpha}{2^{b_1}\pi^{b_2}}$$
$$= 2^{1-b_1+g_1}\pi^{6g_2+3-b_2}\xi^{9v+g_2+14}\eta_1^{-1-2g_2}\eta_2^{-1-2g_2},$$

where $v = 0$ or 1, i.e., $g_1 = a_1'' + b_1 - 1$ and $g_2 = (a_2'' + b_2 - 3)/6$. Hence we have

$$L_j = \xi^{9v+14+g_2}\left(\eta_1^{-1}\eta_2^{-1}\right)^{1+2g_2}2^{a_1''}\pi^{a_2''}\delta_j.$$

It remains to determine x_1, x_3, x_4; so we solve

$$\begin{pmatrix} 1 & \beta^{(1)} & \beta^{(1)2} \\ 1 & \beta^{(2)} & \beta^{(2)2} \\ 1 & \beta^{(3)} & \beta^{(3)2} \end{pmatrix}\begin{pmatrix} x_1 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} L_1 - x_2\alpha \\ L_2 - x_2\alpha \\ L_3 - x_2\alpha \end{pmatrix}.$$

Given that $x_2 = \xi^{9v}2^{g_1}3^{g_2}$, we can do this symbolically and hence get exact results for x_1, x_3, x_4 and avoid rounding errors.

From the 17 solutions to our S-unit equation we find the following solutions to our TCDF.

$\pm x_1$	$\pm x_2$	$\pm x_3$	$\pm x_4$		$\pm x_1$	$\pm x_2$	$\pm x_3$	$\pm x_4$	
-1	-1	-2	0		-11	-1	-2	4	
-1	-1	-4	2		-11	1	-2	4	
-1	-1	0	0	*	-3	-1	-2	2	
-1	-1	2	2		-3	-1	0	0	*
-1	1	-2	0		-3	1	0	0	*
-1	1	-4	2		-3	1	-2	2	
-1	1	0	0	*	-5	-1	0	2	
-1	1	2	2		-5	1	0	2	
0	1	0	0	*					

However, we do not require those solutions marked * for what follows, as they give curves with no Weierstrass points in $\mathbb{Q}(\beta)$. Now by [18, Theorem 4] the curves that are required have Weierstrass points given by

$$\gamma_i = z(x_1 + x_2\alpha^{(i)})/2 + c$$

and

$$\gamma_{j+2} = z(-x_3\beta^{(j)} - x_4\beta^{(j)^2})/2 + c,$$

where $1 \le i \le 2$, $1 \le j \le 3$, $c \in \mathbb{Z}$ and $z \in \{\pm 2^{s_1}3^{s_2} : s_1, s_2 \in \mathbb{Z}\}$. That is,

$$Y^2 = \prod_{i=1}^{5}(X - \gamma_i).$$

Now if we make the change of variable $X = X' + c$, we obtain an isomorphic curve

$$Y^2 = \prod_{i=1}^{5}(X' - (\gamma_i - c)).$$

So we may assume that $c = 0$. Now by passing to another isomorphic curve, we can take z to be $\pm 2^a 3^b$, where $0 \leq a, b \leq 1$. So all curves (up to isomorphism) of genus 2, with two Weierstrass points in $\mathbb{Q}(\sqrt{-3})$, three Weierstrass points in $\mathbb{Q}(\beta)$ and one rational Weierstrass point with good reduction outside the set $\{2, 3\}$ are given by

$$Y^2 = X^5 + a_1 z X^4 + a_2 z^2 X^3 + a_3 z^3 X^2 + a_4 z^4 X + a_5 z^5.$$

a_1	a_2	a_3	a_4	a_5
1	-2	-4	-4	-1
7	10	8	2	-1
23	202	820	1418	589
9	30	48	36	9
11	46	88	68	7

BIBLIOGRAPHY

1. M. Agrawal, J. Coates, D. Hunt, and A.J. van der Poorten, *Elliptic curves of conductor* 11, Math. Comp. **35** (1980), 991–1002.
2. A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. **442** (1993), 19–62.
3. J.H. Evertse and K. Győry, *Decomposable form equations*, New Advances in Transcendence Theory (A. Baker, ed.) Cambridge Univ. Press, 1988, pp. 175–202.
4. I. Gaál, A. Pethő, and M. Pohst, *On the resolution of index form equations in biquadratic number fields* I, J. Number Theory **38** (1991), 18–34.
5. ———, *On the resolution of index form equations in biquadratic number fields* II, J. Number Theory **38** (1991), 35–51.
6. I. Gaál and N. Schulte, *Computing all power integral bases of cubic fields*, Math. Comp. **53** (1989), 689–696.
7. K. Győry, *On the greatest prime factors of decomposable forms at integer points*, Ann. Acad. Sci. Fenn. Ser. A.I Math. **4** (1978/79), 341–355.
8. ———, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. **54** (1979), 585–600.
9. ———, *Explicit upper bounds for the solutions of some diophantine equations*, Ann. Acad. Sci. Fenn. Ser. A.I Math. **5** (1980), 3–12.
10. ———, *On certain graphs composed of algebraic integers of a number field and their applications* I, Publ. Math. Debrecen **27** (1980), 229–242.
11. ———, *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Queen's Papers in Pure and Applied Math., Kingston, Canada, 56, 1980.
12. ———, *On the representation of integers by decomposable forms in several variables*, Publ. Math. Debrecen **28** (1981), 89–98.
13. K. Győry and Z. Papp, *Effective estimates for the integer solutions of norm form and discriminant form equations*, Publ. Math. Debrecen **25** (1978), 311–325.
14. R.A. Horn and C.R. Johnson. *Matrix analysis*, Cambridge Univ. Press, 1985.
15. S. Lang. *Algebraic number theory*, Springer-Verlag, New York, 1986.
16. A. K. Lenstra, H. W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.
17. J. R. Merriman and N. P. Smart, *The calculation of all algebraic integers of degree* 3 *with discriminant a product of powers of* 2 *and* 3 *only*, Publ. Math. Debrecen **43** (1993), 195–205.
18. ———, *Curves of genus* 2 *with good reduction away from* 2 *with a rational Weierstrass point*, Proc. Cambridge Philos. Soc. **114** (1993), 203–214.

19. A. Pethő and B.M.M. de Weger, *Products of prime powers in binary recurrence sequences I. The hyperbolic case, with an application to the generalized Ramanujan-Nagell equation*, Math. Comp. **47** (1986), 713–727.
20. J. Graf v. Schmettow, *KANT—a tool for computations in algebraic number fields*, Computational Number Theory (A. Pethő, M. Pohst, H.C. Williams, and H.G. Zimmer, eds.), de Gruyter, Berlin, 1991.
21. N.P. Smart, *The computer solution of Diophantine equations*, Ph.D. thesis, University of Kent at Canterbury, 1992.
22. ———, *Solving a quartic discriminant form equation*, Publ. Math. Debrecen **43** (1993), 29–39.
23. N. Tzanakis and B.M.M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory **31** (1989), 99–132.
24. ———, *Solving a specific Thue-Mahler equation*, Math. Comp. **57** (1991), 799–815.
25. ———, *How to explicitly solve a Thue-Mahler equation*, Compositio Math. **84** (1992), 223–288.
26. B.M.M. de Weger, *Solving exponential diophantine equations using lattice basis reduction algorithms*, J. Number Theory **26** (1987), 325–367.
27. ———, *Algorithms for Diophantine equations*, Centre for Mathematics and Computer Science, Amsterdam, 1989. CWI-Tract.
28. ———, *A hyperelliptic diophantine equation related to imaginary quadratic number fields with class number* 2, J. Reine Angew. Math. **427** (1992), 137–156.
29. K. R. Yu, *Linear forms in p-adic logarithms*, Acta. Arith. **53** (1989), 107–186.

Department of Computing Mathematics, University College of Cardiff, Cardiff CF2 4YN, Wales
E-mail address: Nigel.Smart@cm.cf.ac.uk