MATHEMATICS OF COMPUTATION
Volume 77, Number 264, October 2008, Pages 2447–2453
S 0025-5718(08)02141-8
Article electronically published on May 19, 2008

SOLVING RESULTANT FORM EQUATIONS OVER NUMBER FIELDS

ISTVÁN GAÁL AND MICHAEL POHST

Abstract. We give an efficient algorithm for solving resultant form equations over number fields. This is the first time that such equations are completely solved by reducing them to unit equations in two variables.

1. Introduction

There is an extensive literature on solving various types of resultant form equations. Let R be an integral domain, let $0 \neq r_0 \in R$, $f \in R[x]$ be given and consider the solutions of

$$\operatorname{Res}(f,g) = r_0 \quad \text{in} \quad g \in R[x]. \tag{1}$$

Under various assumptions many authors, including W.M. Schmidt [14], J.H. Evertse and K. Győry [5] considered this problem. In the number field case, I. Gaál [7] gave an efficient algorithm to find all monic quadratic g satisfying the equation. Polynomials of "small" height satisfying the equation were calculated by I. Járási [11].

Continuing our study of diophantine equations over function fields [8], [9], recently we considered the problem of solving resultant form equations [10]. In this paper we show how those ideas can also be applied in the number field case.

Resultant form equations are known to give a typical example for unit equations in three variables. If $\alpha_1, \ldots, \alpha_n \in R$ are the roots of f and $\beta_1, \ldots, \beta_m \in R$ are the roots of g, then equation (1) implies

$$(\alpha_i - \beta_k) - (\alpha_i - \beta_l) + (\alpha_j - \beta_l) - (\alpha_j - \beta_k) = 0$$

whence

$$\frac{\alpha_i - \beta_k}{\alpha_j - \beta_k} - \frac{\alpha_i - \beta_l}{\alpha_j - \beta_k} + \frac{\alpha_j - \beta_l}{\alpha_j - \beta_k} = 1,$$

where the fractions are elements of a suitable group of S-units of R. Since there are no effective results on unit equations in three variables, no algorithms were developed to solve equation (1) completely.

In this paper we show how to reduce resultant form equations to unit equations in two variables and how to solve completely equation (1).

Received by the editor February 9, 2007.

2000 *Mathematics Subject Classification.* Primary 11D57, 11Y50.

Key words and phrases. Resultant form equations, unit equations, Baker's method, reduction, LLL.

Research supported in part by K67580 and T048791 from the Hungarian National Foundation for Scientific Research.

2. Reducing resultant form equations to unit equations in two variables

Let K be a number field of degree d with ring of integers $\mathbb{Z}_K$. Assume that $f(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree $n \geq 2$ with roots $\alpha_1, \dots, \alpha_n$ contained in $\mathbb{Z}_K$. We suppose that f has at least two distinct roots, say α_1, α_2. Let $0 \neq r_0 \in \mathbb{Z}$ and $m \in \mathbb{N}$ be given. We want to determine the monic polynomials $g(x) \in \mathbb{Z}[x]$ of degree m with roots $\beta_1, \dots, \beta_m \in \mathbb{Z}_K$ ($m \geq 2$) satisfying

$$\mathrm{Res}(f, g) = r_0. \tag{2}$$

Obviously, the above polynomials satisfy

$$\mathrm{Res}(f, g) = \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

If all roots of g are equal to β, then equation (2) can be written in the form

$$(-1)^{mn} (f(\beta))^m = r_0.$$

That equation can be solved easily in the only unknown β.

Our arguments are based on the identity

$$\frac{\alpha_1 - \beta_i}{\alpha_1 - \alpha_2} + \frac{\beta_i - \alpha_2}{\alpha_1 - \alpha_2} = 1. \tag{3}$$

This is obviously a unit equation in two variables. This enables us to give effective upper bounds for the heights of the solutions of equation (2) (cf. Section 3) as well as to give an efficient algorithm for finding all solutions of equation (2) (cf. Section 4). In Section 7 we illustrate our algorithm with an example.

3. Effective upper bounds for the solutions of resultant form equations

Let R_K, h_K, r denote the regulator, class number and unit rank of K, respectively. Let S be a finite set of places of K containing the infinite places, such that S contains all places of K lying above any rational prime dividing r_0. Denote by P the maximum of these primes ($P = 1$ if there are none). Denote by s the cardinality of S and by R_S the S-regulator of K (cf. [2]). For any algebraic number $\gamma \in K$ of degree k the absolute height of γ is defined by

$$h(\gamma) = \left(|a_0| \cdot \prod_{i=1}^{k} \max(1, |\gamma_i|) \right)^{1/k},$$

where a_0 is the leading coefficient of the minimal polynomial of γ over $\mathbb{Z}$ and γ_i are the conjugates of γ. As usual, $|\overline{\gamma}|$ is the size of γ, that is, the maximum absolute value of its conjugates. Let $h_0 = h(1/(\alpha_1 - \alpha_2))$. In the following we set $\log^* c = \max(\log c, 1)$ for any $c > 0$. Finally, let

$$c_1 = 3^{25+9(s+1)} d^{2(s+1)} \left(\frac{\log d}{\log \log d} \right)^{3(s+1)} s^{5s+10},$$

$$c_2 = P^d R_S (\log^* R_S) \left(\frac{\log^*(P R_S)}{\log^* P} \right).$$

Using the above notation we obtain

Theorem 3.1. *All solutions $g(x) \in \mathbb{Z}[x]$ of equation* (2) *satisfy*

$$H(g) < 2^m \cdot (\exp(d\ c_1\ c_2\ \log h_0) + |\overline{\alpha_1}|)^m \,.$$

In the theorem $H(g)$ is the usual height of the polynomial $g(x) \in \mathbb{Z}[x]$, that is the maximum absolute value of its coefficients.

Proof. Consider the unit equation (3). The theorem of Y. Bugaeud and K. Győry [2] implies

$$h(\alpha_1 - \beta_i) < \exp(c_1 c_2 \log h_0) =: c_3,$$

whence

$$|\overline{\alpha_1 - \beta_i}| < c_3^d,$$

and

$$|\overline{\beta_i}| < c_3^d + |\overline{\alpha_1}|.$$

Since this holds for any i $(1 \leq i \leq m)$, we obtain

$$H(g) < 2^m\ (c_3^d + |\overline{\alpha_1}|)^m. \qquad \square$$

4. An efficient algorithm for solving completely resultant form equations

Denote by $\eta_1, \dots, \eta_r$ a set of fundamental units of K. These can be calculated by Kash [3]. If we intend to calculate all solutions $g(x) \in \mathbb{Z}[x]$ of equation (2) it is better to view it as a usual unit equation (not S-unit equation). Namely, for any solution $g(x) = (x - \beta_1) \dots (x - \beta_m)$ of equation (2) any $\alpha_i - \beta_j$ is an integer in K, the norm of which divides r_0^d. (This constant can be reduced considerably by utilizing special properties of the field; see Section 7). Using Kash [3] we can calculate a complete set of nonassociated integers $\mu_1, \dots, \mu_t$ in K of norm dividing r_0^d. Hence

$$\alpha_1 - \beta_1 = \mu\ \eta_1^{a_1} \dots \eta_r^{a_r}$$

and

$$\beta_1 - \alpha_2 = \nu\ \eta_1^{b_1} \dots \eta_r^{b_r}$$

where μ, ν are from the set $\{\mu_1, \dots, \mu_t\}$ (also including signs and roots of unity), $a_1, \dots, a_r, b_1, \dots, b_r \in \mathbb{Z}$. We set $A = \max |a_i|$, $B = \max |b_i|$ and we write equation (3) in the form

$$\gamma\ \eta_1^{a_1} \dots \eta_r^{a_r}\ +\ \delta\ \eta_1^{b_1} \dots \eta_r^{b_r}\ =\ 1, \tag{4}$$

where

$$\gamma = \frac{\mu}{\alpha_1 - \alpha_2} \quad \delta = \frac{\nu}{\alpha_1 - \alpha_2}.$$

This is an ordinary unit equation in two variables. We only give a sketch of the main steps of the standard arguments. For details consult [6] and [2].

4.1. **Baker's method.** Assume that $A \geq B$ (the opposite case can be considered similarly). In the following $c_4, c_5, \ldots$ denote positive constants that can easily be calculated. Set $\eta = \eta_1^{a_1} \ldots \eta_r^{a_r}$. There is a conjugate j_0 such that

$$|\log|\eta^{(j_0)}|| > c_4 \ A;$$

otherwise, by solving the system of linear equations

$$a_1 \log|\eta_1^{(j)}| + \ldots + a_r \log|\eta_r^{(j)}| \leq c_4 \ A$$

(for $1 \leq j \leq d$) we would get a contradiction. By $\sum_{j=1}^{d} |\log|\eta^{(j)}|| = 0$ this implies that another conjugate i_0 satisfies

$$\log|\eta^{(i_0)}| < -\frac{c_4}{2} \ A. \tag{5}$$

Let us use the i_0-th conjugate of all elements in equation (4). For simplicity, from now on we omit the notation of this conjugate by noting that the following procedure must be performed for all possible values of i_0. Using Baker's method (e.g. the estimates of A. Baker and G. Wüstholz [1]), by equation (4) and the estimate (5) we get

$$c_5 \ \exp(-C \ \log B) < c_5 \ |\log|\delta| + b_1 \log|\eta_1| + \ldots + b_r \log|\eta_r||$$

$$\leq \left| \frac{1 - \delta\eta_1^{b_1} \ldots \eta_r^{b_r}}{\gamma} \right| = |\eta| \leq \exp\left(-\frac{c_4}{2} \ A\right) \leq \exp\left(-\frac{c_4}{2} \ B\right),$$

with a big constant C (coming from Baker's method). Comparing the left and right hand sides of these inequalities we get an upper bound $B \leq B_0$. This bound is usually of magnitude $10^{30} - 10^{100}$.

5. Reduction

The huge upper bound $B \leq B_0$ obtained by Baker's method can be reduced by using the inequality

$$|\log|\delta| + b_1 \log|\eta_1| + \ldots + b_r \log|\eta_r|| < c_6 \ \exp\left(-\frac{c_4}{2} \ B\right), \tag{6}$$

which follows from the above estimates. The reduction procedure is based on Lemma 2.2.2 of [6]. We cite here an appropriate form of this statement.

Let H be a large constant (to be specified later) and consider the lattice $\mathcal{L}$ spanned by the columns of the $r+2$ by the $r+1$ matrix

$$\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 \\ H\log|\delta| & H\log|\eta_1| & \ldots & H\log|\eta_r| \end{pmatrix}.$$

Denote by $\underline{v}$ the first vector of an LLL-reduced basis of this lattice (cf. [12], [13])

Lemma 5.1. *If $B \leq B_0$ and $|\underline{v}| \geq \sqrt{(r+2)2^r} \cdot B_0$, then*

$$B \leq 2 \ \frac{\log H + \log c_6 - \log B_0}{c_4}.$$

An appropriate value for H is B_0^{r+1}. We reduce the bound by using the above lemma repeatedly usually in 3 to 7 steps. Especially the first reduction step requires multiple precision arithmetic. The final reduced bound $B \leq B_R$ is usually of magnitude $50 - 500$.

6. Sieving

If the unit rank r is larger than 4 or 5, then the range

$$-B_R \leq b_i \leq B_R \quad (1 \leq i \leq r) \tag{7}$$

still containes far too many possible vectors $(b_1, \ldots, b_r)$. In this case we use sieving (cf. [6] for details). We find a prime number p (not dividing the discriminant of K) such that the polynomial f splits into distinct linear factors modulo p. Let $\mathfrak{p}$ be a prime ideal lying above p, then we can calculate integers e_{ji}, g_i, d_i such that

$$\begin{aligned} \eta_j^{(i)} &\equiv e_{ji} \pmod{\mathfrak{p}}, \\ \gamma^{(i)} &\equiv g_i \pmod{\mathfrak{p}}, \\ \delta^{(i)} &\equiv d_i \pmod{\mathfrak{p}}. \end{aligned}$$

Then the conjugates of the unit equation (4) are of the form

$$g_i\, e_{1i}^{a_1} \ldots e_{ri}^{a_r} \; + \; d_i\, e_{1i}^{b_1} \ldots e_{ri}^{b_r} \equiv 1 \pmod{p}.$$

It is now easy and fast to check if the norm of $(1 - \delta \quad \eta_1^{b_1} \ldots \eta_r^{b_r})$ is equal to $\pm N_{K/Q}(\gamma)$ modulo p, that is, if

$$\prod_{i=1}^{d} \left(d_i\, e_{1i}^{b_1} \ldots e_{ri}^{b_r} \right) \equiv N_{K/Q}(\gamma) \pmod{p}.$$

Note that this test requires p^r steps instead of $(2B_R + 1)^r$ steps, which is essential especially if $p < B_R$. If an exponent vector $(b_1, \ldots, b_r)$ is suitable mod p, then we generate all integer vectors corresponding to it in the range (7) and test these vectors modulo other primes.

7. An example

Let $f(x) = x^4 - x^3 - 6x^2 + x + 1$. Denote by K the field generated by a root α of f over Q. We are going to find all monic irreducible g of degree $m = 4$ with roots in K satisfying

$$\mathrm{Res}(f, g) = \pm 2^k \tag{8}$$

with $k \leq 4$.

The field K is totally real cyclic, it is one of the well-known simplest quartic fields. The Galois automorphism is given by $\sigma(x) = (x-1)/(x+1)$. Denote by $\alpha^{(i)}$ and $\beta^{(i)}$ the roots of f, g, respectively $(1 \leq i \leq 4)$. Taking norms in the equation

$$\prod_{i=1}^{4} \prod_{j=1}^{4} (\alpha^{(i)} - \beta^{(j)}) = \pm 2^k$$

we find that the product of the four equal numbers $N_{K/Q}(\alpha^{(i)} - \beta^{(i)})$ divides 2^{4k}, that is, $N_{K/Q}(\alpha^{(1)} - \beta^{(1)})$ can be $\pm 1, \pm 2, \pm 4, \pm 8, \pm 16$ and the same holds for $\beta^{(1)} - \alpha^{(2)}$.

Using Kash [3] we calculate the fundamental units in K as well as a complete set of nonassociated elements of norm $\pm 1, \pm 2, \pm 4, \pm 8, \pm 16$. We find that there are no elements of norm ± 2, there are four elements of norm ± 4, no elements of norm ± 8 and six elements of norm ± 16. The elements γ, δ may attain one of these ten elements or ± 1.

The application of Baker's method gives $B \leq 10^{23}$. This bound could be reduced to 115 in three steps in all the above cases (depending on the value of δ). In the first reduction step we used 200 digits precision and took $H = 10^{100}$. The reduction took just a few minutes.

We used sieving first modulo 13, this prime is rather small, hence the first sieving procedure was very fast. For all exponent vectors (b_1, b_2, b_3), suitable modulo 13, we generated all corresponding integer vectors with coordinates in the range $(-115, +115)$. Then we tested these vectors modulo 47, 523, 557. This test took a few hours, since it had to be performed in all cases depending on the value of δ.

We tested the numerical values only for those exponent vectors (b_1, b_2, b_3) that passed all of these modular tests; there were about 3000 such vectors. Representing $\beta^{(1)}$ we calculated the other roots by taking conjugates and then tested if (8) holds for the polynomial g.

Finally, we found that the only (irreducible) solution of (8) is the polynomial

$$g(x) = x^4 - 3x^3 - 3x^2 + 10x - 4$$

for which

$$\mathrm{Res}(f, g) = -16.$$

As a byproduct we also found that $\mathrm{Res}(f, x^4) = 1$.

Remark. Calculating the basic data of the number field, K was performed in Kash [3]. All other computations were executed in Maple under Linux on a 1.5GHz PC.

References

[1] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. **442**(1993), 19–62. MR1234835 (94i:11050)

[2] Y. Bugaeud and K. Győry, *Bounds for the solutions of unit equations*, Acta Arithm. **74**(1996), 67–80. MR1367579 (97b:11045)

[3] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner and K. Wildanger, *KANT V4*, J. Symbolic Comput. **24**(1997), 267–283. MR1484479 (99g:11150)

[4] J. H. Evertse and K. Győry, *Finiteness criteria for decomposable form equations*, Acta Arith. **50** (1988), 357–379. MR961695 (90a:11041)

[5] J. H. Evertse and K. Győry, *Lower bounds for resultants I*, Compos. Math. **88** (1993), 1–23. MR1234974 (94h:11036)

[6] I. Gaál, Diophantine equations and power integral bases, Birkhäuser, Boston, 2002. MR1896601 (2003a:11027)

[7] I. Gaál, *On the resolution of resultant type equations*, J. Symbolic Comput. **34**(2002), 137–144. MR1930830 (2003h:12013)

[8] I. Gaál and M. Pohst, *Diophantine equations over global function fields I: The Thue equation*, J. Number Theory **119**(2006), 49–65. MR2228949 (2007b:11041)

[9] I. Gaál and M. Pohst, *Diophantine equations over global function fields II: S-integral solutions of Thue equations*, Experimental Mathematics, **15**(2006), 1-6. MR2229380 (2007b:11040)

[10] I. Gaál and M. Pohst, *Diophantine equations over global function fields III: An application to resultant form equations*, submitted.

[11] I. Járási, *Computing small solutions of unit equations in three variables I: Application to norm form equations*, submitted, *II: Resultant form equations*, Publ. Math. (Debrecen), **65**(2004), 399–408. MR2107956 (2006c:11028)

[12] A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann., **261**(1982), 515–534. MR682664 (84a:12002)

[13] M. Pohst, Computational algebraic number theory, DMV Seminar Band 21, Birkhäuser, 1993. MR1243639 (94j:11132)

[14] W. M. Schmidt, *Inequalities for resultants and for decomposable form equations*, in: Diophantine approximation and its applications, pp. 235–253, Academic Press, New York, 1973. MR0354566 (50:7044)

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

Technische Universtät Berlin, Institut für Mathematik, Strasse des 17. Juni 136, Berlin, Germany
E-mail address: pohst@math.tu-berlin.de