Acta Acad. Paed. Agriensis, Sectio Mathematicae **27** *(2000) 19–24*

FAST ALGORITHM FOR SOLVING SUPERELLIPTIC EQUATIONS OF CERTAIN TYPES

László Szalay (Sopron, Hungary)

Abstract. The purpose of this paper is to give a simple, elementary algorithm for finding all integer solutions of the diophantine equation

$$y^2=x^{2k}+a_{2k-1}x^{2k-1}+\ldots+a_1x+a_0,$$

where the coefficients $a_{2k-1},\ldots,a_0$ are integers and $k\geq 1$ is a natural number.

AMS Classification Number: 11B41

1. Introduction

Let $F(X)$ be a monic polynomial of even degree with integer coefficients. Suppose that $F(X)$ is not a perfect square. We consider the diophantine equation

$$y^2 = F(x) \tag{1}$$

in integers x and y.

The present paper provides a fast and elementary algorithm for solving equation (1). The method is a generalization of a result of D. Poulakis [4], who treated the case $\deg(F(X)) = 4$. (Here and in the sequel $\deg(F(X))$ denotes the degree of the polynomial $F(X)$.) For other results concerning superelliptic equations see, for example, C. L. Siegel [5], A. Baker [1], Y. Bugeaud [2] or D. W. Masser [3].

2. The algorithm

There is given the non-square polynomial

$$F(X) = X^{2k} + a_{2k-1}X^{2k-1} + \cdots + a_1X + a_0, \quad (k \geq 1) \tag{2}$$

Research supported by Hungarian National Foundation for Scientific Research Grant No. 25157/1998.

over the ring of rational integers. The following procedure determines all integer solutions (x, y) of the diophantine equation

$$y^2 = F(x). \tag{3}$$

Step 1. Find polynomials $B(X) \in \mathbf{Q}[X]$ and $C(X) \in \mathbf{Q}[X]$ such that

$$F(X) = B^2(X) + C(X) \tag{4}$$

with the assumption $\deg(C(X)) < k$.

Step 2. If $C(X) = 0$ then output *"$F(X)$ is perfect square"* and terminate the algorithm.

Step 3. Find the least natural number α for which $2\alpha B(X)$ and $\alpha^2 C(X)$ are polynomials with integer coefficients.

Step 4. Set

$$P_1(X) = 2\alpha B(X) - 1 + \alpha^2 C(X) \tag{5}$$

and

$$P_2(X) = 2\alpha B(X) + 1 - \alpha^2 C(X). \tag{6}$$

Step 5. Let

$$H = \{a \in \mathbf{R} : \ P_1(a) = 0 \text{ or } P_2(a) = 0\}. \tag{7}$$

Step 6. If $H \neq \emptyset$ then let $m = \lceil \min(H) \rceil$, $M = \lfloor \max(H) \rfloor$ and for each integer element x of the interval $[m, M]$ compute $F(x)$. If $F(x)$ is a square of an integer y then output the solution $(x, \pm y)$.

Step 7. Determine the integer solutions x of the equation $C(x) = 0$, output $(x, B(x))$ and $(x, -B(x))$, and terminate algorithm.

Summarizing the method, to reach our goal first we need a special decomposition of the polynomial $F(X)$, then we have to determine the real roots of two polynomials. After then the integer elements of a quite short interval must be checked. Finally, we have to compute the integer solutions of a polynomial with rational coefficients.

3. Examples

Using the steps of the algorithm, we solve three numerical examples.

Example 1. $y^2 = x^8 + x^7 + x^2 + 3x - 5$,
$B(X) = X^4 + \frac{1}{2}X^3 + \frac{1}{8}X^2 + \frac{1}{16}X - \frac{5}{128}$,
$C(X) = \frac{7}{128}X^3 + \frac{505}{512}X^2 + \frac{3077}{1024}X - \frac{81945}{16384}$,
$\alpha = 128 = 2^7$,
$P_1(X) = 256X^4 + 1024X^3 + 16128X^2 + 49248X - 81956$,
$P_2(X) = 256X^4 - 768X^3 - 16192X^2 - 49216X + 81936$,
$[m, M] = [-4, 10]$, $C(x) = 0$ has no integer solution.
All integer solutions are $(x, y) = (-2, \pm 11)$, $(1, \pm 1)$.

Example 2. $y^2 = x^4 - 2x^3 + 2x^2 + 7x + 3$,
$P_1(X) = 16X^2 - 528X - 167$,
$P_2(X) = 16X^2 + 496X + 183$,
$[m, M] = [-30, 33]$, $C(x) = 0$ has no integer solution.
All integer solutions are $(x, y) = (-1, \pm 2)$, $(1, \pm 5)$.

Example 3. $y^2 = x^2 - 5x - 11$,
$B(X) = X - \frac{5}{2}$, $C(X) = -\frac{69}{4}$, $\alpha = 2$,
$P_1(X) = 4X - 80$, $P_2(X) = 4X + 60$,
$[m, M] = [-15, 20]$.
All integer solutions are $(x, y) = (-5, \pm 17)$, $(-4, \pm 5)$, $(9, \pm 5)$, $(20, \pm 17)$
($C(X) \neq 0$ is a constant polynomial, so it has no (integer) root).

Remark. The equation of Example 3 can easily be solved by using another simple elementary method. (The equation $y^2 = x^2 - 5x - 11$ is equivalent to $(2y - 2x + 5)(2y + 2x - 5) = -69$, and the decomposition the rational integer -69 into prime factors provides the solutions.) Here we only would like to demonstrate that if $k = 1$ then the algorithm can be applied, too.

4. Proof of rightness of the algorithm

Going through on the steps of the described algorithm we show that the procedure is correct. As earlier, let

$$F(X) = X^{2k} + a_{2k-1}X^{2k-1} + \cdots + a_1X + a_0, \tag{8}$$

where k is an integer greater than zero.

4.1 First we prove that the decomposition $F(X) = B^2(X) + C(X)$ in Step 1 of the algorithm uniquely exists if we assume that the leading coefficient of $B(X)$ is positive. We have to show that there is a polynomial

$$B(X) = b_k X^k + b_{k-1} X^{k-1} + \cdots + b_1 X + b_0 \in \mathbf{Q}[X] \tag{9}$$

$(b_k > 0)$, such that the first $k+1$ coefficients coincide in $F(X)$ and in $B^2(X)$. Consequently, the degree of the polynomial

$$C(X) = F(X) - B^2(X) \tag{10}$$

is less than k.

The proof depends on the fact that the system of the following $k+1$ equations

$$\begin{aligned} b_k^2 &= 1, \\ 2b_k b_{k-1} &= a_{2k-1}, \\ 2b_k b_{k-2} + b_{k-1}^2 &= a_{2k-2}, \\ &\vdots \\ 2b_k b_0 + 2b_{k-1} b_1 + \cdots &= a_k \end{aligned} \tag{11}$$

uniquely solvable in the rational variables $b_k > 0, b_{k-1}, \ldots, b_0$, where the coefficients $a_{2k-1}, \ldots, a_k$ of the polynomial $F(X)$ are fixed integers.

Observe that in the i^{th} equation of (11) $(1 \le i \le k+1)$ there are exactly i variables and only one of them (b_{k+1-i}) does not occur in the first $i-1$ equations $(i > 1)$. Consequently, this "new" linear variable can directly expressed from the i^{th} equation. Hence we have the unique solution

$$\begin{aligned} b_k &= 1 \ (> 0), \\ b_{k-1} &= \frac{a_{2k-1}}{2b_k} = \frac{a_{2k-1}}{2}, \\ b_{k-2} &= \frac{a_{2k-2} - b_{k-1}^2}{2b_k} = \frac{a_{2k-2}}{2} - \frac{a_{2k-1}^2}{8}, \\ &\vdots \\ b_0 &= \frac{a_k - (2b_{k-1} b_1 + \cdots)}{2b_k} = \cdots \end{aligned} \tag{12}$$

of the system (11), which proves the unique existence of the decomposition $F(X) = B^2(X) + C(X)$. We note that the equations of (11) come from the coincidence of the first $k+1$ coefficients of $F(X)$ and the square

$$B^2(X) = \sum_{i=0}^{k} \left(\sum_{j=0}^{i} b_{k-j} b_{k+j-i} \right) X^{2k-i} + B_1(X) = B_0(X) + B_1(X) \tag{13}$$

with some polynomial $B_1(X)$, where $\deg(B_1(X)) < k$. From (13) it follows that

$$B_0(X) = \left(b_k^2\right) X^{2k} + (2b_k b_{k-1}) X^{2k-1} + \left(2b_k b_{k-2} + b_{k-1}^2\right) X^{2k-2} + \cdots + (2b_k b_0 + 2b_{k-1} b_1 + \cdots) X^k, \tag{14}$$

which provides the system (11).

4.2 In the next step we check that the polynomial $F(X)$ is perfect square or not. If $F(X) = B^2(X)$ then the equation has infinitely many solutions and the algorithm is terminated. In the sequel, we can assume that $C(X) \neq 0$.

4.3 Clearly, infinitely many natural number α_1 exist for which $2\alpha_1 B(X)$ and $\alpha_1^2 C(X)$ are polynomials with integer coefficients. Let α be the least among them. Since $C(X) = F(X) - B^2(X)$, together with (12) it follows that $\alpha = 2^\beta$, where the natural number β depends, of course, on the degree k and the coefficients $a_{2k-1}, \ldots, a_0$ of the polynomial $F(X)$. For instance, it is easy to see that if $k = 1$ then $\beta \leq 1$, if $k = 2$ then $\beta \leq 3$ and if $k = 3$ then $\beta \leq 4$.

4.4 The polynomials $P_1(X) = 2\alpha B(X) - 1 + \alpha^2 C(X)$ and $P_2(X) = 2\alpha B(X) + 1 - \alpha^2 C(X)$ provided by Step 4 of the algorithm possess the following properties. They have integer coefficients, $\deg(P_1(X)) = \deg(P_2(X)) = k$ because of $\deg(2\alpha B(X)) = k$ and $\deg(\alpha^2 C(X) - 1) < k$, moreover their leading coefficent 2α is positive.

4.5 It follows from the first part of Step 6 of the algorithm that it is sufficient to determine approximately the real roots of the polynomial $P_1(X)$ and $P_2(X)$. There are many numerical methods which give (rational) numbers very close to the exact roots, and several mathematical program package, for example Maple, Mathematica,..., are able to provide the approximations of the roots and establish the set H.

4.6 In Step 6 we are checking for each integer $x \in [m, M]$ that $F(x)$ is square or not (it can be done by computer, too). The length of the interval $[m, M]$ depends on the coefficients of $F(X)$. The examples in Section 3 show that $[m, M]$ may be quite small.

4.7 Now we have arrived at the main part of the proof of the rightness of the algorithm. We have to show that if an integer $x \notin [m, M]$ and $F(x)$ is square then $C(x) = 0$.

Suppose that $x \notin [m, M]$ and $F(x) = y^2$ for some $x, y \in \mathbf{Z}$. Since the leading coefficient of $P_1(X)$ and $P_2(X)$ is positive, $x \notin [m, M]$ implies that $P_1(x) > 0$ and $P_2(x) > 0$, or in case of odd k $P_1(x) < 0$ and $P_2(x) < 0$ can also be occurred. Assume now that $P_1(x) > 0$ and $P_2(x) > 0$, i.e.

$$2\alpha B(x) - 1 + \alpha^2 C(x) > 0 \tag{15}$$

and

$$2\alpha B(x) + 1 - \alpha^2 C(x) > 0. \tag{16}$$

Hence

$$-2\alpha B(x) + 1 < \alpha^2 C(x) < 2\alpha B(x) + 1. \tag{17}$$

Now add anywhere $\alpha^2 B^2(x)$ we have

$$(\alpha B(x) - 1)^2 < \alpha^2 \left(B^2(x) + C(x)\right) < (\alpha B(x) + 1)^2, \tag{18}$$

which together with $B^2(x) + C(x) = F(x) = y^2$ provides

$$(\alpha B(x) - 1)^2 < \alpha^2 y^2 < (\alpha B(x) + 1)^2. \tag{19}$$

Since $\alpha B(x) \pm 1$, $\alpha > 0$ and y are integers it follows that $B(x) > 0$, moreover $(\alpha B(x) - 1)^2$, $\alpha^2 y^2$ and $(\alpha B(x) + 1)^2$ are three consecutive squares, hence

$$B(x) = y^2. \tag{20}$$

But it means that $C(x) = 0$, so the integer x is a root of the polynomial $C(X)$.

In the other case, when k is an odd number, $P_1(x) < 0$ and $P_2(x) < 0$ we gain similar argument in similar manner:

$$(\alpha B(x) + 1)^2 < \alpha^2 y^2 < (\alpha B(x) - 1)^2, \tag{21}$$

which implies that $B(x) < 0$ and $B^2(x) = y^2$, i.e. $C(x) = 0$ for the integer x.

References

[1] Baker, A., Bounds for the solutions of the hyperelliptic equation, *Proc. Camb. Phil. Soc.*, **65** (1969), 439–444.

[2] Bugeaud, Y., Bounds for the solutions of superelliptic equations, *Compos. Math.*, **107** (1997), 187–219.

[3] Masser, D. W., Polynomial bounds for diophantine equations, *Amer. Math. Monthly*, **93** (1986), 486–488.

[4] Poulakis, D., A simple method for solving the diophantine equation $Y^2 = X^4 + aX^3 + bX^2 + cX + d$, *Elem. Math.*, **54** (1999), 32–36.

[5] Siegel, C. L., The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$, *J. London Math. Soc.*, **1** (1926), 66–68.

László Szalay
Institute of Mathematics
University of West Hungary
Bajcsy Zs. u. 4.
P.O. Box 132
H-9400 Sopron, Hungary
e-mail: laszalay@efe.hu