Author: Laszlo Szalay

Title: Superelliptic Equations of the form y^p=x^kp+a_(kp-1)x^(kp-1)+...+a_0

Creator: HDML

BULLETIN OF THE
GREEK MATHEMATICAL SOCIETY
VOLUME 46, 2002 (23 – 33)

Superelliptic equations of the form $y^p = x^{kp} + a_{kp-1}x^{kp-1} + \ldots + a_0$

László Szalay[1]
FR. 6.1 Mathematik, Universität des Saarlandes
D-66041 Saarbrücken, Deutschland, Pf. 151150
e-mail: laszalay@math.uni-sb.de

Received 20 – 2 – 2001, Revised 3 – 5 – 2001

1 Introduction

Consider the diophantine equation

$$y^L = x^K + a_{K-1}x^{K-1} + \ldots + a_0 \tag{1}$$

in integers x and y, where $a_{K-1}, \ldots, a_0, L, K \in \mathbf{Z}$ satisfy $L \geq 2$ and $K \geq 2$.

Although many results have dealt with elliptic and superelliptic equations, only few of them describe practical methods for determining all the solutions of such an equation.

By a consequence of a theorem of Siegel [8] the equation (1), under some assumptions, has a finite number of solutions if $L = 2$. In [1] Baker showed that if $m \geq 3$, $n \geq 3$ then the equation

$$y^m = a_0x^n + a_1x^{n-1} + \ldots + a_n \tag{2}$$

has finitely many solutions if the polynomial on the right-hand side of (2) possesses at least two simple zeros. A similar result was proved for $m = 2$, supposing three simple zeros of the polynomial. The theorems of Baker give effective upper bounds for the absolute values of the solutions, however these bounds usually are huge too to solve practically equation (2).

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

A method for determining all integral points on elliptic curves

$$E:\ y^2 = x^3 + ax + b \tag{3}$$

was developed, among others, by GEBEL, PETHŐ and ZIMMER [2]. The algorithms is implemented in the computer algebraic system SIMATH [9]. In [11] TZANAKIS gives a procedure for computing the integer solutions of the equation

$$y^2 = f(x), \tag{4}$$

where $f(X)$ is a polynomial of degree four with integer coefficients and non-zero disriminant. His method based on some estimates on linear forms in elliptic logarithm. Some bounds of [11] are improved by HERRMANN [4]. If $f(X)$ is monic and not a perfect square POULAKIS [6] describes a nice method for solving (4), moreover his algorithm was generalized by SZALAY [10] for monic and non-square polynomial $f(X)$ of arbitrary even degree. Their results are elementary way of application of the Runge's method.

More general problem was considered by RUNGE [7], who showed that if the polynomial

$$F(X,Y) = \sum_{i=0}^{k}\sum_{j=0}^{n} c_{ij}X^iY^j \in \mathbf{Z}[\mathrm{X},\mathrm{Y}] \tag{5}$$

is irreducible in $\mathbf{Q}[\mathrm{X},\mathrm{Y}]$ and some other conditions are fulfilled then the equation

$$F(x,y) = 0 \tag{6}$$

in $x \in \mathbf{Z}$ and $y \in \mathbf{Z}$ has only finitely many solutions. GRYTCZUK and SCHINZEL [3], further WALSH [12] provided upper bounds for the absolute value of the solutions of (6). In [12] WALSH took the polynomial $F(X,Y) = Y^L - P(X)$ as a special case of (6) with $\deg(P) = K$ and proved the following theorem.

Theorem A. *Let $L \geq 2$, $K \geq 2$ be integers such that $\gcd(L,K) = p > 1$. Suppose further that $P(X) = \sum_{i=0}^{K} c_iX^i \in \mathbf{Z}[\mathrm{X}]$ is a monic polynomial of degree K such that $Y^L - P(X)$ is irreducible in $\mathbf{Q}[\mathrm{X},\mathrm{Y}]$. Put $h = \max_i |c_i|$ and let $l > 1$ denote a divisor of p. All integer solutions of the superelliptic equation*

$$y^L = P(x) \tag{7}$$

satisfy

$$|x| \leq l^{2K-l}\left(\frac{K}{l}+2\right)^{l}(h+1)^{K+l}. \tag{8}$$

This theorem, as well as the following result due to LE, makes it possible, in several cases, to give all the integer solutions of (7). In [5] LE investigated the diophantine equation

$$y^L = x^K + c_{K-1}x^{K-1} + \ldots + c_0 \tag{9}$$

and showed

Theorem B. *If $K \equiv 0 \pmod{L}$, $c_{K-1}, \ldots, c_0$ not all zeros and the first nonzero coefficient is coprime with L, then (9) has only finitely many solutions (x, y). Moreover, all solution of (9) satisfy*

$$|x| < (4Kh)^{\left(\frac{2K}{L}+1\right)}, \tag{10}$$

$$|y| < (4Kh)^{\left(\frac{2K^2}{L^2}+\frac{K}{L}+1\right)}, \tag{11}$$

where $h = \max_i |c_i|$.

The effective Theorem A and Theorem B provide general upper bounds for the solutions of equations (7) and (9), respectively. Our application of Runge's method described below gives an own interval (i.e. bounds) for the solutions x of each equation. That is why this method gives quite bid far bounds in certain cases, which may have great advantage if one really means to solve such an equation. In exceptional case it can be occurred that an integer solution x is outside of the interval, but then x must be a root of a polynomial $C(X) \in \mathbf{Z}[X]$, which can easily be determined.

2 Results

The purpose of the present paper is to extend the earlier results of POULAKIS [6] and the author [10] for the title equation, by giving an elementary and easily applicable method for solving equation (1), if the greatest common

divisor of the exponents L and K is greater than one. Let $\gcd(L, K) = p > 1$, $L = lp$ and $K = kp$. It is obviously sufficient to consider the equation

$$y^p = x^{kp} + a_{kp-1}x^{kp-1} + \ldots + a_0. \tag{12}$$

There is no restriction in assuming that p is prime, but it is not necessary. It is worth remarking that the equation

$$y^p = a^p x^{kp} + a_{kp-1}x^{kp-1} + \ldots + a_0 \tag{13}$$

also leads to equation (12). Here $a = -1$ is also possible if p is odd. Copying the coefficients of the right-hand side of (12) we introduce the polynomial

$$F(X) = X^{kp} + a_{kp-1}X^{kp-1} + \ldots + a_0. \tag{14}$$

Finally, suppose that $F(X) \neq G^p(X)$ for any $G(X) \in \mathbf{Z}[\mathrm{X}]$, i.e. $F(X)$ is not a perfect p^{th} power. For simplicity, equation (12) may be written in the form

$$y^p = F(x). \tag{15}$$

Algorithm for determining all integer solutions of (12).

Step 1. Find polynomials $B(X) = X^k + b_{k-1}X^{k-1} + \ldots + b_0 \in \mathbf{Q}[\mathrm{X}]$ and $C(X) \in \mathbf{Q}[\mathrm{X}]$ with $\deg(C(X)) \leq kp - k - 1$, such that

$$F(X) = B^p(X) + C(X). \tag{16}$$

Step 2. Find the least positive integer α for which $\alpha B(X) \in \mathbf{Z}[\mathrm{X}]$. (Then we also have $\alpha^p C(X) \in \mathbf{Z}[\mathrm{X}]$.)
Step 3. Set

$$P_1(X) = -(\alpha B(X) - 1)^p + \alpha^p B^p(X) + \alpha^p C(X), \tag{17}$$

and

$$P_2(X) = (\alpha B(X) + 1)^p - \alpha^p B^p(X) - \alpha^p C(X). \tag{18}$$

Step 4. Let $H = \{r \in \mathbf{R} | \mathrm{P_1(r)} = 0 \text{ or } \mathrm{P_2(r)} = 0\}$. (Approximations are allowed.)

Step 5. If $H \neq \emptyset$ then let $h_1 = \lceil \min H \rceil$ and $h_2 = \lfloor \max H \rfloor$, and for each integer element of the interval $[h_1, h_2]$ compute $F(x)$. If $F(x) = y^p$ satisfies with some integer y then output: (x, y).
Step 6. Determine all integer solutions of the equation $C(x) = 0$. If x is such an integer then output: $\left(x, (\pm)\sqrt[p]{F(x)}\right)$. (If p is even then we may use $\pm$.)

Remarks.

1. *Step 1.* gives a polynomial $B(X)$, which is the polynomial part of the Puiseaux expansion

$$y_1(X) = c_{-k}X^k + \ldots c_{-1}X + c_0 + c_1X^{-1} + \ldots \tag{19}$$

of the algebraic function $G(X, Y) = Y^p - F(X)$, i.e. $B(X) = c_{-k}X^k + \ldots c_{-1}X + c_0$.

2. In case of $p = 2$ and $k = 1$, $C(X) = a_1^2 - \frac{a_0^2}{4}$ is a constant polynomial (nonzero, hence it has no any roots), $\alpha = 2$ or $\alpha = 1$ depending on the parity of a_1, further

$$P_1(X) = (2\alpha)X - 1 + \alpha a_1 + \alpha^2\left(a_0 - \frac{a_1^2}{4}\right) \tag{20}$$

and

$$P_2(X) = (2\alpha)X + 1 + \alpha a_1 - \alpha^2\left(a_0 - \frac{a_1^2}{4}\right) \tag{21}$$

are linear polynomials. It is readily verified by *Step 4* and *Step 5* of the algorithm that

$$|x| \leq \begin{cases} \frac{h^2+6h+1}{4} & \text{if } a_1 \text{ is odd,} \\ \frac{h^2+8h+4}{8} & \text{if } a_1 \text{ is even,} \end{cases} \tag{22}$$

which is partially improve WALSH's result in [12].

It is easy to recognize that the efficiency of this method mainly depends on the length of the interval $[h_1, h_2]$. In many cases this interval proves itself to be unexpectedly short, and this fact enables us to use the algorithm. Of course, if the height and the degree of the polynomial $F(X)$ become large, the method becomes less powerful (as well as other algorithms). To prove the correctness of our method we need two statements, a lemma and a theorem.

Lemma. *Suppose that $p \geq 2$ and $k \geq 1$ are integers and*

$$F(X) = X^{kp} + a_{kp-1}X^{kp-1} + \ldots + a_0 \tag{23}$$

is a polynomial with integer coefficents. Then uniquely exist polynomial

$$B(X) = X^k + b_{k-1}X^{k-1} + \ldots + b_0 \in \mathbf{Q}[\mathrm{X}] \tag{24}$$

and $C(X) \in \mathbf{Q}[\mathrm{X}]$ with $\deg(C(X)) \leq kp - k - 1$ for which

$$F(X) = B^p(X) + C(X). \tag{25}$$

Proof of Lemma. By the notation of Lemma, let $F(X) = X^{kp} + a_{kp-1}X^{kp-1} + \ldots + a_0$, $B(X) = X^k + b_{k-1}X^{k-1} + \ldots + b_0$, further let $B^p(X) = X^{kp} + \sum_{i=1}^{kp} c_{kp-i}X^{kp-i}$. We must show that rational numbers $b_{k-1}, \ldots, b_0$ can be choosen such that the coefficients c_{kp-i} and a_{kp-i} coincide for each integer $i \in \{1, \ldots, k\}$. Applying the Polynomial Theorem to $(X^k + b_{k-1}X^{k-1} + \ldots + b_0)^p$, it follows that

$$c_{kp-1} = pb_{k-1}, \tag{26}$$

and the coefficient b_{k-i} $(i = 2, \ldots, k)$ appears first in c_{kp-i}. More exactly,

$$c_{kp-i} = Q_i(b_{k-1}, \ldots, b_{k-i+1}) + pb_{k-i}, \quad (i = 2, \ldots, k) \quad , \tag{27}$$

where Q_i denotes certain polynomial of degree i in variables $b_{k-1}, \ldots, b_{k-i+1}$ with positive integer coefficients $(i = 2, \ldots, k)$. Consequently if we choose

$$b_{k-1} = \frac{a_{kp-1}}{p}, \tag{28}$$

and

$$b_{k-i} = \frac{a_{kp-i} - Q_i(b_{k-1}, \ldots, b_{k-i+1})}{p}, \quad (i = 2, \ldots, k) \tag{29}$$

then $B(X)$ is established. Finally let $C(X) = F(X) - B^p(X)$, i.e.

$$C(X) = (a_{kp-k-1} - c_{kp-k-1})X^{kp-k-1} + \ldots + (a_0 - c_0), \tag{30}$$

which has degree at most $kp - k - 1$. The polynomial $B(X)$ and $C(X)$ with rational coefficients are uniquely given and satisfying all the conditions of Lemma. ■

Theorem. *Using the notations have been introduced above, if (x, y) is a solution of the equation*

$$y^p = F(x) \tag{31}$$

and $x \notin [h_1, h_2]$ then $C(x) = 0$.

Proof of Theorem. Take the decomposition $F(X) = B^p(X) + C(X)$ guaranted by Lemma, where $\deg(B(X)) = k$ and $\deg(C(X)) \leq kp - k - 1$. Determining the least positive integer α, and by (17) and (18) we get polynomials $P_1(X)$ and $P_2(X)$ with integer coefficients. From the proof of Lemma it follows that $\alpha = p^\beta$ with some non-negative integer β. If k and p are given then the least upper bound $\beta_0(p, k)$ of β can be determined. For instance, $\beta_0(p, 1) = 1$, $\beta_0(2, 2) = 3$, if $p > 2$ then $\beta_0(p, 2) = 2$, $\beta_0(3, 3) = 4$, $\beta_0(5, 5) = 6$. Simple calculation shows that both $P_1(X)$ and $P_2(X)$ have $p\alpha^{p-1}$ as positive leading coefficent, moreover

$$\deg(P_1(X)) = \deg(P_2(X)) = kp - k > \deg(C(X)). \tag{32}$$

Now suppose that (x, y) is a solution of (31). Then

$$y^p = F(x) = B^p(x) + C(x). \tag{33}$$

The properties of polynomials $P_1(X)$ and $P_2(X)$ imply that if $x \notin [h_1, h_2]$ then $P_1(x) > 0$ and $P_2(x) > 0$ or in case of odd $kp - k$ $(= \deg(P_i(X)))$ $P_1(x) < 0$ and $P_2(x) < 0$ can even be occurred.

A) First examine the case $P_1(x) > 0$ and $P_2(x) > 0$, so that

$$-(\alpha B(X) - 1)^p + \alpha^p B^p(X) + \alpha^p C(X) > 0, \tag{34}$$

and

$$(\alpha B(X) + 1)^p - \alpha^p B^p(X) - \alpha^p C(X) > 0. \tag{35}$$

Combining (34) and (35) we have

$$(\alpha B(x) - 1)^p < \alpha^p \left(B^p(x) + C(x)\right) < (\alpha B(x) + 1)^p. \tag{36}$$

By (33) together with (36) give

$$(\alpha B(x) - 1)^p < (\alpha y)^p < (\alpha B(x) + 1)^p, \tag{37}$$

and since $\alpha B(x)$ is an integer thanks to the multiplier α, the terms of inequalities (37) must be p^{th} power of three consecutive integers. Hence $\alpha^p y^p = \alpha^p B^p(x)$, which together with (33) provide $C(x) = 0$.

B) The same conclusion can be drawn in case of odd $kp - k$, i.e. p is even and k odd. (We would have even assumed that p is prime implying here $p = 2$.) Now from the inequalities

$$-(\alpha B(X) - 1)^p + \alpha^p B^p(X) + \alpha^p C(X) < 0, \tag{38}$$

and

$$(\alpha B(X) + 1)^p - \alpha^p B^p(X) - \alpha^p C(X) < 0 \tag{39}$$

it follows that

$$(\alpha B(x) + 1)^p < \alpha^p \left(B^p(x) + C(x)\right) < (\alpha B(x) - 1)^p, \tag{40}$$

which means that $B(x) < 0$, and (40), in the same way as above, leads to $C(x) = 0$. Then Theorem is proved. ■

Remark If the coefficients $a_{kp-1}, \ldots, a_0$ and $\deg(F(X))$ are not large too (see Examples) then we can check for each integer element of $[h_1, h_2]$ whether equation (31) is satisfied or not. Otherwise, if a solution x does not belong to $[h_1, h_2]$ or $H = \emptyset$ then $C(x) = 0$ and we can get x simply by determining all integer roots of $C(X)$. In a more precise approach we should determine all intervals I_j in $\mathbf{R}$, whose real elements r satisfy the inequality $P_1(r) \cdot P_2(r) \leq 0$, and taking $H = \bigcup_j I_j$ instead of the interval $[h_1, h_2]$, this refinement might have an important influence on the algorithm in certain cases, but on the grounds of experiences here we find sufficient our first (and more simple) version.

The power of the algorithm is demonstrated by three examples. Further Table 1 compares bounds provided by Theorem A, Theorem B and present paper.

3 Examples

Example 1.

$$y^2 = x^8 + x^7 + x^2 + 3x - 5, \tag{41}$$

$p = 2$, $k = \deg(B(X)) = 4$, $kp - k = \deg(P_i(X)) = 4 > \deg(C(X)) = 3$.
$B(X) = X^4 + \frac{1}{2}X^3 - \frac{1}{8}X^2 + \frac{1}{16}X - \frac{5}{128}$,
$C(X) = \frac{7}{128}X^3 + \frac{505}{512}X^2 + \frac{3077}{1024}X - \frac{81945}{16384}$.
$\alpha = 2^7$,
$P_1(X) = 256X^4 + 1024X^3 + 16128X^2 + 49248X - 81956$,
$P_2(X) = 256X^4 - 768X^3 - 16192X^2 - 49216X + 81936$.
$[h_1, h_2] = [-4, 10]$, $C(x) = 0$ has no integer solution.
The solutions of equation (41) are $(x, y) = (-2, \pm 11), (1, \pm 1)$.

Example 2.

$$y^3 = x^9 + 2x^8 - 5x^7 - 11x^6 - x^5 + 2x^4 + 7x^2 - 2x - 3, \tag{42}$$

$p = 3$, $k = \deg(B(X)) = 3$, $kp - k = \deg(P_i(X)) = 6 > \deg(C(X)) = 5$.
$B(X) = X^3 + \frac{2}{3}X^2 - \frac{19}{9}X - \frac{77}{81}$,
$C(X) = -\frac{628}{81}X^5 - \frac{4298}{243}X^4 - \frac{2908}{2187}X^3 + \frac{117460}{6561}X^2 + \frac{73285}{19683}X - \frac{1137790}{531441}$.
$\alpha = 3^4$,
$P_1(X) = 19683X^6 - 4094064X^5 - 9474084X^4 - 799713X^3 + 9576873X^2 + 2058210X - 1119771$,
$P_2(X) = 19683X^6 + 4146552X^5 + 9325368X^4 + 614061X^3 - 9451323X^2 - 1900206X + 1155347$.
$[h_1, h_2] = [-208, 210]$, $C(x) = 0$ has no integer solution.
The only solution of equation (42) is $(x, y) = (3, 24)$.

Example 3.

$$y^5 = x^{25} + x^{24} + x^{23} + \ldots + x^2 + x + 7 \tag{43}$$

$p = 5$, $k = \deg(B(X)) = 5$, $kp - k = \deg(P_i(X)) = 20 > \deg(C(X)) = 19$.
$B(X) = X^5 + \frac{1}{5}X^4 + \frac{3}{25}X^3 + \frac{11}{125}X^2 + \frac{44}{625}X + \frac{924}{15625}$,
$C(X) = \frac{4004}{15625}X^{19} + \ldots + \frac{65192573487738342547 51}{9313225746154785156 25}$.
$\alpha = 5^6$,
$P_1(X) = 298023223876953125X^{20} + \ldots + 6519257352410621188532$,
$P_2(X) = 298023223876953125X^{20} - \ldots - 6519257345121269531250$.
$[h_1, h_2] = [-799, 801]$, $C(x) = 0$ has no integer solution.
The only solution of equation (43) is $(x, y) = (1, 2)$.

Table 1. (Comparison the bounds in [12], bounds in [5] and bounds in present paper)

Let $F_4(X) = X^8 - 7X^7 - 2X^4 - X + 5$, $F_5(X) = X^{24} + X^{23} + \ldots + X + 33554434$ and $F_6(X) = X^4 - 99X^3 - 37X^2 - 51X + 100$.

equation	bound in [12]	bound in [5]	interval $[h_1, h_2]$
(41)	$3.57 \cdot 10^{13}$	$6.88 \cdot 10^{19}$	$[-4, 10]$
(42)	$1.60 \cdot 10^{22}$	$1.53 \cdot 10^{18}$	$[-208, 210]$
(43)	$5.92 \cdot 10^{62}$	$1.98 \cdot 10^{31}$	$[-799, 801]$
$y^2 = F_4(x)$	$6.34 \cdot 10^{14}$	$1.42 \cdot 10^{21}$	$[-59267, 59277]$
$y^2 = F_5(x)$	$6.45 \cdot 10^{211}$	$5.02 \cdot 10^{237}$	$[-650036, 650038]$
$y^2 = F_6(x)$	$1.09 \cdot 10^{15}$	$1.05 \cdot 10^{16}$	$[-492617, 492741]$

References

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

[2] Gebel, L. - Pethő, A. - Zimmer, H. G., Computing integral points on elliptic curves, Acta Arithm., **68** (1994), 171-192.

[3] Grytczuk, A. - Schinzel, A., On Runge's theorem about diophantine equations, Colloq. Math. Soc. J. Bolyai 60 (Sets, graphs and numbers, 1992), 329-356.

[4] Herrmann, E., Bestimmung aller ganzzahligen Lösungen quartischer elliptischer diophantischer Gleichungen unter Verwendung von Linearformen in elliptischen Logarithmen, Diplomarbeit, 1998.

[5] Le, M., A note on the integer solutions of hyperelliptic equations, Colloq. Math. **68** (1995), 171-177.

[6] 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.

[7] Runge, C., Über ganzzahlige Lösungen von Gleichungen zwissen zwei Veränderlichen, J. Reine Angew. Math. **100**, (1887), 425-435.

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

[9] SIMATH Manual, Saarbrücken, 1996.

[10] Szalay, L., Fast algoritm for solving superelliptic equations of certain types, Acta Acad. Paed. Agriensis, **27** Sectio Mathematicae (2000), 19-24.

[11] Tzanakis, N., Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations, Acta Arithm., **75** (1996), 165-190.

[12] Walsh, P. G., A quantitative version of Runge's theorem on diophantine equations, Acta Arithm., **62** (1992), 157-172.