Elem. Math. 54 (1999) 32 – 36
0013-6018/99/010032-5 $ 1.50+0.20/0

Elemente der Mathematik

A simple method for solving the diophantine equation $Y^2 = X^4 + aX^3 + bX^2 + cX + d$

Dimitrios Poulakis

Dimitrios Poulakis was born in 1956 in Athens (Greece). After his studies in mathematics at the University of Ioannina, he received his PhD from the University of Paris XI in 1983. He then went back to the University of Ioannina, where he taught mathematics for three years. Since 1988 he is at the department of mathematics of the Aristotle University of Thessaloniki. His main research interests are Diophantine Equations and Arithmetic Algebraic Geometry.

1 Introduction

We consider the diophantine equation

$$Y^2 = f(X),$$

where $f(X)$ is a polynomial of degree four with integer coefficients. For $f(X)$ monic and not a perfect square Masser [2] has shown that any integer solution (x, y) of the above equation satisfies

$$|x| \leq 26\, H(f)^3,$$

where $H(f)$ denotes the maximum of the absolute values of the coefficients of $f(X)$. As far as we know, this bound is the best one for $|x|$ that exists in the literature. It follows that for small values of $H(f)$ the integer solutions of $Y^2 = f(X)$ can be obtained by a direct

Die Frage Diophants nach den ganzzahligen Lösungen einer gegebenen algebraischen Gleichung hat historisch immer wieder Anlass zu wichtigen Entwicklungsschritten in der Zahlentheorie gegeben; das Fermat-Problem liefert dafür ein wohlbekanntes und eindrückliches Beispiel. Das Fermat-Problem illustriert auch treffend die mathematikhistorische Erfahrung, dass die Behandlung diophantischer Probleme in der Regel schwierig ist. Vor diesem Hintergrund ist es immer überraschend, wenn für spezielle Gleichungen eine vollständige Antwort gefunden werden kann: Dimitrios Poulakis beschreibt im vorliegenden Beitrag eine einfache Methode, die für eine ganze Klasse von algebraischen Gleichungen sämtliche ganzzahligen Lösungen liefert. *ust* computer search. In the case where the discriminant of $f(X)$ is not zero, Tzanakis [4] has recently given a practical method for computing all integer solutions of $Y^2 = f(X)$. This method relies on a lower bound for linear forms in elliptic logarithms. It is easily applicable once one knows a Mordell-Weil basis for the elliptic curve associated with the equation $Y^2 = f(X)$. Some interesting numerical examples are given in [4].

The purpose of this note is to describe a very simple and elementary method for computing the integer solutions of $Y^2 = f(X)$ in the case where $f(X)$ is monic and not a perfect square. We give two quadratic polynomials depending on the coefficients of $f(X)$ with the property that their roots determine a region to which the x-coordinates of the integer solutions (x, y) of $Y^2 = f(X)$ belong. From this the integer solutions of $Y^2 = f(X)$ can be obtained by a direct computer search. More precisely we prove the following result:

Theorem 1. *Let a_1, a_2, a_3, a_4 be integers such that the polynomial $f(X) = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4$ is not a perfect square. Let*

$$\Pi_1(X) = 16X^2 + 8(a_1 - 8a_3 + 4a_1a_2 - a_1^3)X + 8a_2 - 2a_1^2 + 1 - 64a_4 + 16a_2^2 + a_1^4 - 8a_2a_1^2$$

and

$$\Pi_2(X) = 16X^2 + 8(a_1 + 8a_3 - 4a_1a_2 + a_1^3)X + 8a_2 - 2a_1^2 - 1 + 64a_4 - 16a_2^2 - a_1^4 + 8a_2a_1^2.$$

For $i = 1, 2$ denote by π_{i1}, π_{i2} the roots of the polynomial $\Pi_i(X)$. If π_{i1}, π_{i2} are real, we set $I_i = [\pi_{i1}, \pi_{i2}]$ (or $I_i = [\pi_{i2}, \pi_{i1}]$); otherwise $I_i = \emptyset$. Then, if (x, y) is an integer solution of $y^2 = f(x)$, one has $x \in I_1 \cup I_2 \cup \{x_0\}$, where

$$x_0 = \frac{64a_4 - 16a_2^2 - a_1^4 + 8a_2a_1^2}{8(-8a_3 + 4a_1a_2 - a_1^3)}.$$

Remark. If a_1 is odd, then it is easily seen that x_0 is not an integer.

In practice, the region for x obtained from Theorem 1 is much smaller than the one obtained from the inequality in [2]. Therefore, in numerous cases we do not actually need a computer to carry out the necessary computations; see the numerical examples in section 2. The examples (1) and (2) have been taken from [4]. It is apparent from [4] that the solution of these equations by the method applied there requires extensive computations.

2 Applications

In this section we solve some diophantine equations, using Theorem 1.

(1) Consider the equation

$$Y^2 = f(X) = X^4 - 8X^2 + 8X + 1.$$

We have the quadratic polynomials

$$\Pi_1(X) = 16X^2 - 512X + 897 \quad \text{and} \quad \Pi_2(X) = 8X^2 + 512X - 1025.$$

The zeros of $\Pi_1(X)$ lie in the open interval $(1,31)$ and the zeros of $\Pi_2(X)$ in $(-34,2)$. Further, $x_0 = 15/8$. Thus, if x, y are integers with $y^2 = f(x)$, then Theorem 1 gives $-33 \le x \le 31$. On the other hand we have $y^2 \equiv x^4 + 1 \pmod 8$. If x is odd, then $x \equiv \pm 1, \pm 3 \pmod 8$ and we deduce $y^2 \equiv 2 \pmod 8$. Since this congruence has no solution, we obtain a contradiction. Thus x is even. We check one by one the even values from -33 to 31, and we obtain as the only possibilies $x = 0, 2, -6$. Therefore, the only integer solutions of $Y^2 = f(X)$ are $(x,y) = (0,\pm 1), (2,\pm 1), (-6,\pm 31)$. Note that the bound of [2] yields $|x| \le 13312$.

(2) Consider Fermat's equation

$$Y^2 = f(X) = X^4 + 4X^3 + 10X^2 + 20X + 1$$

(see [3]). The zeros of the quadratic polynomials

$$\Pi_1(X) = 16X^2 - 480X + 561 \quad \text{and} \quad \Pi_2(X) = 16X^2 + 544X - 465$$

lie in the set $(-34,1) \cup (1,29)$. Further, $x_0 = 5/8$. Let x, y be integers with $y^2 = f(x)$. Then Theorem 1 implies $-33 \le x \le 0$ or $2 \le x \le 28$. On the other hand we have $y^2 \equiv x^4 + 4x^3 + 1 \pmod 5$, whence it follows that $x \not\equiv 4(\pmod 5)$. Thus $-33 \le x \le 28$ and $x \ne -31, -26, -21, -16, -11, -6, 1, 4, 9, 14, 19, 24$. Checking the remaining values for x one by one, we deduce that the only integer solutions of $Y^2 = f(X)$ are

$$(x,y) = (0,\pm 1), (1,\pm 6), (-3,\pm 2), (-4,\pm 9).$$

In this case the bound of [2] gives $|x| \le 208000$.

(3) The discriminant of the polynomial

$$f(X) = (X+1)^2(X^2+15) = X^4 + 2X^3 + 16X^2 + 30X + 15$$

is zero. Thus the method of [4] is not applicable to the equation $Y^2 = f(X)$. On the other hand the bound of [2] gives $|x| \le 702000$. In order to apply Theorem 1, we consider the quadratic polynomials

$$\Pi_1(X) = 16X^2 - 944X + 2761 \quad \text{and} \quad \Pi_2(X) = 16X^2 + 976X - 2521.$$

Their zeros lie in the interval $(-64,56)$ and $x_0 = 11/4$. By Theorem 1, we have that the integer solutions (x,y) of $Y^2 = f(X)$ satisfy $-64 \le x \le 56$. If x is even, then y is odd and $y^2 \equiv 3 \pmod 4$, which is a contradiction. Thus x is odd. Suppose 3 divides x. Then 3 divides y and we deduce that 9 divides 15 which is not true. So 3 does not divide x. Similarly we deduce that 5 does not divide x. Let p be an odd prime divisor of x. Then 15 is a quadratic residue modulo p. Since

$$\left(\frac{15}{13}\right) = \left(\frac{15}{19}\right) = \left(\frac{15}{23}\right) = \left(\frac{15}{29}\right) = \left(\frac{15}{31}\right) = \left(\frac{15}{37}\right) = \left(\frac{15}{41}\right) = -1,$$

it follows that the primes 13, 19, 23, 29, 31, 37 and 41 do not divide x. Hence

$$x \in \{\pm 1, \pm 7, \pm 11, \pm 17, \pm 43, \pm 47, \pm 49, \pm 53, -59, -61\}.$$

Checking the elements of this set one by one, we obtain that the only integer solutions of $Y^2 = f(X)$ are $(x,y) = (1,\pm 8), (-1,0), (7,\pm 64), (-7,\pm 48)$.

3 Proof of Theorem 1

We shall use an argument that goes back to an idea of H.L. Montgomery [1, page 576]. Write

$$f(X) = (X^2 + b_1X + b_2)^2 + c_0X + c_1.$$

Equating coefficients of terms of same degree, we get

$$b_1 = \frac{a_1}{2}, \quad b_2 = \frac{a_2}{2} - \frac{a_1^2}{8}$$

and

$$c_0 = a_3 - \frac{a_1a_2}{2} + \frac{a_1^3}{8}, \quad c_1 = a_4 - \frac{a_2^2}{4} - \frac{a_1^4}{64} + \frac{a_2a_1^2}{8}.$$

Putting

$$B(X) = X^2 + b_1X + b_2 \quad \text{and} \quad C(X) = c_0X + c_1,$$

we have

$$f(X) = B(X)^2 + C(X).$$

Since $f(X)$ is not a perfect square, the linear polynomial $C(X)$ is not zero.

Consider the quadratic polynomials

$$\begin{aligned}\Pi_1(X) &= 16B(X) + 1 - 64C(X)\\ &= 16X^2 + 8(a_1 - 8a_3 + 4a_1a_2 - a_1^3)X\\ &\quad + 8a_2 - 2a_1^2 + 1 - 64a_4 + 16a_2^2 + a_1^4 - 8a_2a_1^2\end{aligned}$$

and

$$\begin{aligned}\Pi_2(X) &= 16B(X) - 1 + 64C(X)\\ &= 16X^2 + 8(a_1 + 8a_3 - 4a_1a_2 + a_1^3)X\\ &\quad + 8a_2 - 2a_1^2 - 1 + 64a_4 - 16a_2^2 - a_1^4 + 8a_2a_1^2.\end{aligned}$$

For $i = 1, 2$ let π_{i1}, π_{i2} be the roots of the polynomial $\Pi_i(X)$. If π_{i1}, π_{i2} are real, set $I_i = [\pi_{i1}, \pi_{i2}]$ (or $I_i = [\pi_{i2}, \pi_{i1}]$); and $I_i = \emptyset$ otherwise. Then, if (x, y) is an integer solution of $y^2 = f(x)$, one has

$$y^2 = B(x)^2 + C(x).$$

Suppose that x does not lie in $I_1 \cup I_2$. Then $\Pi_1(x) > 0$ and $\Pi_2(x) > 0$, whence it follows that

$$-16B(x) + 1 < 64C(x) < 16B(x) + 1.$$

Adding everywhere $64B(x)^2$, we get

$$(8B(x) - 1)^2 < (8y)^2 < (8B(x) + 1)^2.$$

Since $8B(x)$ and y are integers, the above inequality implies $y^2 = B(x)^2$. Thus $C(x) = 0$. The polynomial $C(X)$ is not zero. If $c_0 = 0$, then we get $c_1 = 0$ and therefore $C(X)$ is zero, which is a contradiction. Thus $c_0 \neq 0$, and we obtain $x = -c_1/c_0$. The theorem follows.

References

[1] T. Cochrane, *The diophantine equation* $f(x) = g(x)$, Proc. Amer. Math. Soc. **3** (1990), 573–577.

[2] D. W. Masser, *Polynomial Bounds for Diophantine Equations,* Amer. Math. Monthly **93** (1986), 486–488.

[3] J. Top, *Fermat's "primitive solutions" and some arithmetic of elliptic curves,* Indag. Math. **4** (1993), 211–222.

[4] N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations,* Acta Arithm. **LXXV.2** (1996), 165–190.

Dimitrios Poulakis
Aristotle University of Thessaloniki
54006 Thessaloniki
Greece