PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 109, Number 3, July 1990

THE DIOPHANTINE EQUATION $f(x) = g(y)$

TODD COCHRANE

(Communicated by William Adams)

ABSTRACT. Let $f(x)$, $g(y)$ be polynomials over $\mathbb{Z}$ of degrees n and m respectively and with leading coefficients a_n, b_m. Suppose that $m|n$ and that a_n/b_m is the mth power of a rational number. We give two elementary proofs that the equation $f(x) = g(y)$ has at most finitely many integral solutions unless $f(x) = g(h(x))$ for some polynomial $h(x)$ with rational coefficients taking integral values at infinitely many integers.

The problem of showing that a given polynomial diophantine equation

$$p(x, y) = 0 \tag{1}$$

has at most finitely many integral solutions has been a central problem of research in number theory. Deep results in algebraic geometry and diophantine approximation have been employed to address this problem; (see [2, 3] for surveys). For instance, in 1929 Siegel [5] used such methods to prove one of the most celebrated results in this area; namely, that if the curve given by (1) is irreducible and of positive genus then it has at most finitely many points with integral coordinates. Moreover, he was able to characterize those curves of genus zero having infinitely many points with integral coordinates. The object of this paper is to obtain the same type of result for a special class of diophantine equations as an easy corollary of two lemmas from elementary complex analysis. A second proof of the result is given at the end of the paper using only elementary methods.

We shall restrict our attention to diophantine equations of the type

$$f(x) \equiv a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = b_m y^m + b_{m-1}y^{m-1} + \cdots + b_0 \equiv g(y) \tag{2}$$

with integer coefficients, $a_n \neq 0$, $b_m \neq 0$, although the method we use may be applied to a wider variety of equations of type (1).

Theorem. *Suppose that* $m|n$ *and that* (a_n/b_m) *is the* mth *power of a rational number. Then either*

(iCC) $f(x) = g(h(x))$ *for some polynomial* $h(x)$ *with rational coefficients taking integral values at infinitely many integers; or*

(ii) *equation* (2) *has at most finitely many integral solutions.* □

Received by the editors June 17, 1988 and, in revised form, October 10, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11D41.

It is clear that in the first case (2) has an infinite family of integral solutions of the type $(x, h(x))$ where x runs through those values making $h(x)$ integral. Moreover, we shall see in this case that if m is odd, then all solutions with $|x|$ sufficiently large are of the type $(x, h(x))$. If m is even, then there is possibly a second polynomial $h_2(x)$ with rational coefficients such that $f(x) = g(h_2(x))$, and thus a second family of solutions of (2).

The theorem follows readily from the following two lemmas.

Lemma 1. *Suppose that* $h(z) = c_d z^d + \cdots + c_0 + c_{-1} z^{-1} + \cdots$ *is a Laurent series with rational coefficients converging on an annulus* $|z| > R$, *and taking on integer values for infinitely many integers* z. *Then* $h(z)$ *is a polynomial, that is* $c_{-k} = 0$ *for* $k \in \mathbf{N}$.

Proof. This is a result of Skolem [6] and the proof we give here can be found for example in Polya and Szego [4, Number 188, p. 142]. Let λ be the l.c.m. of the denominators of $c_d, c_{d-1}, \ldots, c_0$. Set $k(z) = \lambda[h(z)] - \lambda(c_d z^d + \cdots + c_0)$, so that $k(z) = \frac{\lambda}{z}(c_{-1} + \frac{c_{-2}}{z} + \ldots)$. Then $k(z)$ is integral valued for infinitely many integral z and of absolute value less than one for $|z|$ sufficiently large, whence $k(z) = 0$ for infinitely many integral z. But this implies that $k(\frac{1}{z})$ has a cluster point of zeros about $z = 0$, and so $k(\frac{1}{z})$ and $k(z)$ are identically zero.

Lemma 2. *If* $f(z)$, $g(z)$ *are polynomials as in* (2) *with* $m|n$, *say* $md = n$, *then there exist* m *distinct Laurent series of the type* $h(z) = c_d z^d + c_{d-1} z^{d-1} + \cdots + c_0 + c_{-1} z^{-1} + \cdots$ *such that* $f(z) = g(h(z))$ *on some annulus* $|z| > R$. *Moreover* $c_k \in \mathbf{Q}(c_d)$, *for* $k \leq d$. *Thus the coefficients of* $h(z)$ *are rational if* c_d *is rational.*

Proof. We treat x and y as complex variables and consider solving the equation $f(x) = g(y)$ for y in terms of x. Setting $x = \frac{1}{s}$, $y = \frac{1}{t}$ and multiplying by $s^n t^m$, the equation becomes

$$t^m(a_n + a_{n-1}s + \cdots + a_0 s^n) = s^n(b_m + b_{m-1}t + \cdots + b_0 t^m). \tag{3}$$

Thus it suffices to solve the equation,

$$t(a_n + a_{n-1}s + \cdots + a_0 s^n)^{1/m} = s^d(b_m + b_{m-1}t + \cdots + b_0 t^m)^{1/m}$$

for t, where the mth root denotes any one of the m branches. These branches will be analytic for $|s|$ and $|t|$ sufficiently small, since $a_n \neq 0$ and $b_m \neq 0$. Viewing the preceding equality as an equation of the type $F(s, t) = 0$ and observing that $\frac{\partial F}{\partial t}(0, 0) = a_n^{1/m} \neq 0$, we obtain from the implicit function theorem that t can be solved for as an analytic function of s, say $t = h_1(s)$, on a neighborhood $|s| < \delta$ of zero. It is clear from (3) that $h_1(s)$ has a zero of order d at the origin and so

$$t = h_1(s) = s^d(\alpha_d + \alpha_{d-1}s + \alpha_{d-2}s^2 + \ldots)$$

for some $\alpha_j \in \mathbf{C}$, $j \leq d$, $\alpha_d \neq 0$. Thus

$$y = \frac{1}{t} = s^{-d}(c_d + c_{d-1}s + c_{d-2}s^2 + \dots)$$

for some $c_j \in \mathbf{C}$, $j \leq d$, and so

$$y = x^d(c_d + c_{d-1}x^{-1} + c_{d-2}x^{-2} + \dots), \tag{4}$$

on the annulus $|x| > \frac{1}{\delta}$.

The m distinct solutions are obtained by taking the m distinct branches of the mth root function. Inserting the expansion (4) into (2) we see that

$$c_d^m = a_n/b_m$$

and that for $k < d$, c_k is a rational function in $c_d, c_{d-1}, \dots, c_{k+1}, a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m$, with rational coefficients. Thus $c_k \in \mathbf{Q}(c_d)$ for $k \leq d$.

Proof of theorem. We start by observing that under the assumptions of Lemma 2, every solution (x, y) of (2) with $|x|$ sufficiently large is of the form $y = h_i(x)$ for some i, $1 \leq i \leq m$, where $h_1(x), \dots, h_m(x)$ are the m series given in Lemma 2. This follows, for if we fix x then (2) has at most m distinct solutions y. On the other hand, for $|x|$ sufficiently large the m values of y given by $h_1(x), h_2(x), \dots, h_m(x)$ are all distinct, for the leading coefficients of these series are the m distinct mth roots of a_n/b_m.

Suppose now that a_n/b_m is the mth power of a rational number. Then if m is even, exactly two of the series, say $h_1(x)$, $h_2(x)$ have rational coefficients, and if m is odd, exactly one, say $h_1(x)$, has rational coefficients. The remaining series have nonreal leading coefficients. If (2) has infinitely many integral solutions it follows that either $h_1(x)$ or $h_2(x)$ takes on integral values for infinitely many integral x. Hence by Lemma 1, either $h_1(x)$ or $h_2(x)$ is just a polynomial with rational coefficients. □

Example. It is well known that a polynomial $f(x)$ with integer coefficients takes on the value of an mth power of an integer for all positive integers x if and only if $f(x)$ itself is the mth power of a polynomial with integer coefficients; see [3, Number 114, p. 132]. Setting $g(y) = y^m$ in our theorem we obtain a stronger result for a more restricted set of polynomials. Namely, if the degree of $f(x)$ is a multiple of m and the leading coefficient of $f(x)$ is a perfect mth power, then $f(x)$ takes on the value of an mth power infinitely often if and only if $f(x)$ is the mth power of a polynomial with integer coefficients.

Remarks. (1) The assumption in the theorem that a_n/b_m be the mth power of a rational number is essential. For example, whenever a is not a perfect square, the Pell equation $y^2 = ax^2 + 1$ has infinitely many integral solutions.

(2) The condition is part (i) of the theorem that $h(x)$ take integral values at infinitely many integers is equivalent to $h(x)$ taking on an integral value at least once. If this condition is omitted from (i) then (2) may have no solutions. For example consider $f(x) = 2x + 1$, $g(y) = 2y$, $h(x) = x + 1/2$.

(3) Davenport, Lewis, and Schinzel [1] have given a criterion for when the polynomial $f(x) - g(y)$ is irreducible and of positive genus, whence Siegel's result implies that (2) has at most finitely many solutions. If we let $D(\lambda) = \operatorname{disc}(f(x) + \lambda)$ and $E(\lambda) = \operatorname{disc}(g(y) + \lambda)$, the result is that $f(x) - g(y)$ is irreducible and of positive genus if $D(\lambda)$ has at least $[n/2]$ distinct roots for which $E(\lambda) \neq 0$, except possibly when $m = 2$, or $m = n = 3$.

(4) A second proof of the Theorem can be given using a method suggested by Hugh L. Montgomery. Without loss of generality we may assume that b_m is positive. We first note that there exists a polynomial $p(x) = \beta_d x^d + \beta_{d-1} x^{d-1} + \cdots + \beta_0$ with rational coefficients such that

$$f(x) = g(p(x)) + r(x) \tag{5}$$

for some polynomial $r(x)$ with $\deg r(x) < n - d$; (just solve for $\beta_d, \beta_{d-1}, \ldots, \beta_0$). Let c be the least common multiple of the denominators of $\beta_d, \beta_{d-1}, \ldots, \beta_0$, and set $g_1(y) = c^m g(y/c) \in \mathbf{Z}[y]$.

Then for any pair (x, y) satisfying (2) we have $g(p(x)) + r(x) = g(y)$ and so

$$g_1(cp(x)) + c^m r(x) = g_1(cy).$$

Now by a Taylor series expansion of g_1 we know that

$$g_1(cp(x) + 1) = g_1(cp(x)) + g_2(x),$$

and

$$g_1(cp(x) - 1) = g_1(cp(x)) + g_3(x)$$

for some polynomials $g_2(x)$, $g_3(x)$ of degrees $(m-1)d = n - d$, with leading coefficients of opposite sign. Without loss of generality we assume that g_2 has the positive leading coefficient. Then, since $\deg r(x) < n - d$ we know that for x sufficiently large

$$g_3(x) < c^m r(x) < g_2(x)$$

and consequently,

$$g_1(cp(x) - 1) < g_1(cy) < g_1(cp(x) + 1). \tag{6}$$

If m is odd then $g_1(y)$ is monotone on a set of the type $\{|y| > M\}$ for M sufficiently large. Thus if (x, y) is a solution of (2) with $|cy| > M$, $|cp(x) + 1| > M$, and $|cp(x) - 1| > M$, then it follows from (6) that $cp(x) - 1$, cy, $cp(x) + 1$ are consecutive integers, that is $y = p(x)$. But this implies that $r(x) = 0$. Thus if (2) has infinitely many solutions then r has infinitely many zeros, and so r is identically zero and $f(x) = g(p(x))$ identically.

If m is even then a_n, b_m must have the same sign (a_n/b_m is an mth power). Thus, if (2) has infinitely many solutions then there must be infinitely many with x, y both positive or both negative. If β_d is taken to be positive then the same argument as above holds, upon observing that $g_1(y)$ is monotone on sets of the type $\{y > M\}$ and $\{y < -M\}$, for M sufficiently large. □

References

1. H. Davenport, D. J. Lewis, and A. Schinzel, *Equations of the form* $f(x) = g(y)$, Quart. J. Math. Oxford Ser. 2, **12** (1961), 304–312,
2. W. J. LeVeque, *Studies in number theory*, Math. Assoc. of Amer. 1969, pp. 4–24.
3. B. Mazur, *Arithmetic on curves*, Bull. Amer. Math. Soc. **14** (1986), 207–259.
4. G. Pólya and G. Szegö, *Problems and theorems in analysis* II, Springer-Verlag, New York, 1976.
5. C. L. Siegel, *Uber einige anwendungen diophantischer approximationen*, Abh. Preuss. Akad. Wiss. Phys. - Mat. Kl., no. 1 (1929).
6. T. A. Skolem, *Videnskapsselskapets Skrifter*, no. 17 (1921), Theorem 8.

Department of Mathematics, Kansas State University, Manhattan, Kansas 66506