JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematical Sciences
Vol. 72B, No. 1, January–March 1968

The Diophantine Equation $P(x, y) = (xy + d)z$

Charles F. Osgood

Institute for Basic Standards, National Bureau of Standards, Washington, D.C. 20234

(January 9, 1968)

Under certain conditions the algebraic equation $P(x, y) = (xy + d)z$, where $P(x, y)$ is a polynomial in x and y with integral coefficients and d is an integer, is shown to have an infinite number of distinct solutions with x, y, and z each an integer

Key Words: Algebraic equations, diophantine equations, integers, three variables.

L. J. Mordell[1] suggested the problem of finding solutions of the diophantine equation

$$ax^3 + by^3 + c = z(xy + d)$$

where a, b, c, and d are integers. We shall prove below that under certain conditions the equation

$$P(x, y) = z(xy + d)$$

has an infinite number of solutions, where $P(x, y)$ denotes a polynomial in x and y with integral coefficients.

We may write $P(x, y) \equiv P_1(x) + P_2(y) \mod (xy + d)$ and suppose that $P_2(0) = 0$. It is easily verified that this representation is unique. Suppose now that (a) $\deg P_1(x) + \deg P_2(y) \geq 4$, (b) $\alpha = \deg P_2(y) \geq \max(\deg P_1(x), 3)$, (c) $d \neq 0$, and (d) that $(P_1(t), d) = 1$ whenever $(t, d) = 1$. Additionally, where $P_2(y) = \beta_0 y^\alpha + \beta_1 y^{\alpha-1} + \ldots$, we suppose that (e) $\beta_0 | \beta_1^k$ for some $k \geq 1$. Under these conditions we shall prove:

THEOREM. *The diophantine equation*

$$\mathrm{P(x, y) = z(xy + d)}$$

has an infinite number of distinct solutions.

PROOF: The genesis of the following proof was the rather trivial remark that if x and y are chosen such that $xy = 1 - d$ then $(x, y, ax^3 + by^3 + c)$ is a solution of our equation. This gives only a finite number of solutions; however, we are able to show that if $|d| > 1$ then there is almost a 1–1 correspondence of solutions between our equation and each of an infinite collection of equations of the same general type, where the number of divisors of the integer corresponding to $1 - d$ is *not uniformly bounded.* (Note $d = 0$ is contrary to the hypotheses. If $d = \pm 1$, $\{(0, y, \pm P(0, y))\}$ is an infinite collection of distinct solutions. Therefore we assume $|d| > 1$ in what follows.)

We must show that if $|d| > 1$

$$P_1(x) + P_2(y) = z(xy + d) \tag{1}$$

[1] L. J. Mordell, The congruence $ax^3 + by^3 + c = 0 \pmod{xy}$ and integer solutions of cubic equations in three variables, Acta Math. **88,** 77–83 (1922).

has an infinite number of solutions. Now (1) is implied by

$$x^{\alpha}(P_1(x)+P_2(y))=z'(xy+d), \tag{2}$$

where $(xy,\ d)=1$. We may reduce $x^{\alpha}(P_1(x)+P_2(y))$ modulo $xy+d$ to obtain

$$R(x)=a_nx^n+\ .\ .\ .+a_jx^j\ .\ .\ .+a_3x^3+a_2dx^2+a_1d^2x+a_0d^3,$$

for integers $a_n,\ .\ .\ .,\ a_0$ with $n\geqslant 4$, $a_n\neq 0$, and $a_0\neq 0$. (Recall that $\deg P_1(x)+\deg P_2(x)\geqslant 4$ and $\alpha=\deg P_2(y)\geqslant 3$.) Also $a_0|a_1^k$ for some $k\geqslant 1$. This means (1) is implied by

$$R(x)=z''(xy+d), \tag{3}$$

where $(xy,\ d)=1$. Since $x^{\alpha}(P_1(x)+P_2(y))\equiv R(x) \bmod (xy+d)$ we have, setting $y=0$,

$$R(x)\equiv x^{\alpha}(P_1(x)) \bmod d.$$

Hence if $\qquad (xy,\ d)=1$ then $(R(x),\ d)=1$ by hypothesis (d).

If (3) has an infinite number of solutions with $(xy,\ d)=1$ then (1) has an infinite number of solutions. For technical reasons we shall find it easier to show that

$$y_1^n-a_1dy_1^{n-1}+a_2(a_0d^2)y_1^{n-2}+a_3a_0d(-a_0d^2)y_1^{n-3}+\ .\ .\ .+a_ja_0d(-a_0d^2)^{j-2}$$

$$y_1^{n-j}+\ .\ .\ .+a_na_0d(-a_0d^2)^{n-2}=w_4(x_1y_1-a_na_0d(-a_0d^2)^{n-3}), \tag{4}$$

with $(x_1y_1,\ a_na_0d)=1$, has an infinite number of solutions. Hence we must show that (4) having an infinite number of solutions implies that (3) has an infinite number of solutions. Looking at (4) mod y_1 we see that it implies, setting $w_4=xy_1+a_0d^2$ and $(x_1y_1-a_na_0d(-a_0d^2)^{n-3})=w_3$ that we have

$$y_1^n-a_1dy_1^{n-1}+a_2(a_0d^2)y_1^{n-2}+a_3a_0d(-a_0d^2)y_1^{n-3}+\ .\ .\ .+a_ja_0d(-a_0d^2)^{j-2}$$

$$y_1^{n-j}+\ .\ .\ .+a_n(a_0d)\,(-a_0d^2)^{n-2}=w_3(xy_1+a_0d^2). \tag{5}$$

Now $(y_1,\ a_0d)\ =1$ so $(y_1-a_1d,\ a_od)=1$ (use $a_o|a_1^k$ for some k), and $(xy_1,\ a_0d)=1$. We note that

$$(y_1,\ x,\ w_3)=\left(y_1,\ \frac{w_4-a_0d^2}{y_1},\ x_1y_1-a_na_0d(-a_0d^2)^{n-3}\right)$$

so distinct solutions go into distinct solutions. It follows that (5) implies, setting $w_2=a_0d^3w_3$, that

$$a_n(-a_0d^2)^n+\ .\ .\ .+a_j(-a_0d^2)^jy_1^{n-j}+\ .\ .\ .+a_3(-a_0d^2)^3y_1^{n-3}$$

$$+a_2d(-a_0d^2)^2y_1^{n-2}+a_1d^2(-a_0d^2)\,y_1^{n-1}+a_0d^3y_1^n=w_2(xy_1+a_0d^2) \tag{6}$$

where

$$(xy_1,\ a_od)=1.$$

Now (6) implies, setting $w_1=w_2y_1^{-n}$, that

$$R(x)=a_nx^n+\ .\ .\ .+a_jx^j+\ .\ .\ .+a_3x^3+a_2dx^2+a_1d^2x+a_0d^3=w_1(xy_1+a_0d^2). \tag{7}$$

We conclude that (7) implies, setting $w_1 = (xy+d)$ and $(xy_1 + a_0d^2) = z''$, that

$$R(x) = z''(xy+d). \tag{3}$$

Since $(x, d) = 1$ we have $(R(x), d) = 1$, so $(xy, d) = 1$. In this last change of variables (x, y_1, w_1) becomes

$$\left(x, \frac{z_1'' - a_0d^2}{x}, xy+d\right)$$

so distinct solutions go into distinct solutions.

Now to show that (4) has an infinite number of solutions. We shall show that there exists an infinite sequence of equations $E_0, E_2, \ldots$ with $E_0 = (4)$ and $E_{2i} \leftrightarrow E_{2i+2}$ in the sense that a sequence of *reversible* steps takes one equation into the other—inducing a 1–1 correspondence of solutions. Then we shall end with a proof that given $N > 0$ there exists an n such that E_{2n} has at least N distinct solutions.

DEFINITION: *Let* $\beta(\mathrm{m})$ *be a function from the integers to the integers defined by* $\beta(0) = 0$, $\beta(1) = 1$, *and*

$$\beta(\mathrm{m}) = (\mathrm{n}-2)\beta(\mathrm{m}-1) - \beta(\mathrm{m}-2).$$

Notice that since $\mathrm{n} \geq 4$ *if* $\mathrm{s}(\mathrm{m})$ *satisfies the above recurrence relation and* $0 \leq \mathrm{s}(0) \leq \mathrm{s}(1)$ *then* $\mathrm{s}(\mathrm{m})$ *is nondecreasing for all* $\mathrm{m} \geq 0$. *Therefore* $\beta(\mathrm{m}+1) - \beta(\mathrm{m})$ *is nondecreasing for all* $\mathrm{m} \geq 0$.

DEFINITION: *For each integer* m *set*

$$\mathrm{r_m} = (-1)^{\beta(\mathrm{m}+1)+1}(\mathrm{a_n d^{-1}})^{\beta(\mathrm{m}+1)}(-\mathrm{a_0 d^2})^{\beta(\mathrm{m}+2)} \equiv (-1)^{\beta(\mathrm{m}+1)+1}(-\mathrm{a_n a_0 d}(-\mathrm{a_0 d^2})^{\mathrm{n}-4})^{\beta(\mathrm{m}+1)}(-\mathrm{a_0 d^2})^{\beta(\mathrm{m}+1)-\beta(\mathrm{m})},$$

using $\beta(\mathrm{m}+2) = (\mathrm{n}-4)\beta(\mathrm{m}+1) + \beta(\mathrm{m}+1) + \beta(\mathrm{m}+1) - \beta(\mathrm{m})$. *From the second expression for* $\mathrm{r_m}$ *we are able to conclude that if* $\mathrm{m} \geq 0$ *then* $(\mathrm{a_n a_0 d})^{-1}(\mathrm{r_m})^{-1}\mathrm{r_{m+1}}$ *is an integer by using the facts that* $\beta(\mathrm{m}+2) - \beta(\mathrm{m}+1)$ *is nondecreasing if* $\mathrm{m} \geq -1$, *and* $\beta(1) - \beta(0) = 1$.

Now write (4) as

$$\sum_{k=0}^{n} A_k^0 y^k = z''(xy + r_0)$$

which defines A_k^0 for each $0 \leq k \leq n$. In what follows we assume $m \geq 0$. Let

$$A_k^{2m} = A_k^0 \prod_{j=1}^{m} (r_{2j-1} r_{2j-2}^{-1})^{n-k}. \tag{8}$$

Then $|A_k^{2m}|$ is a power product of a_0, a_n, and d. By our remarks above $(a_n a_0 d)^{-1} A_k^{2m}$ is an integer if $0 \leq k < n$.

Using (8) we derive the result that for each $0 \leq k \leq n$

$$(r_{2m})^k A_k^{2m} (A_0^{2m})^{-1} = \left\{ \prod_{j=1}^{m} (r_{2j} r_{2j-1}^{-1})^k \right\} r_0^k A_k^0 (A_0^0)^{-1}. \tag{9}$$

Checking (4), we see that $r_0^k A_k^0 (A_0^0)^{-1}$ is always an integer, hence so is the left side of (9). If $0 < k \leq n$, $(a_0 a_n d)^{-1} r_{2m}^k A_k^{2m} (A_0^{2m})^{-1}$ is an integer by the remark after the definition of r_m. We need to show that

$$r_{2m+1} = (-1)^n (A_0^{2m})^{-1} (r_{2m})^{n-1}. \tag{10}$$

Using (9) with $k = n$ we see that the right-hand side of (10) is

$$(-1)^n (A_0^0)^{-1} r_0^n r_{2m}^{-1} \left\{ \prod_{j=1}^{m} (r_{2j} r_{2j-1}^{-1})^n \right\}.$$

Using the definition of r_m, we compare the exponents on r_0, $a_n d^{-1}$, and $-a_0 d^2$, and observe that

$$n\sum_{j=1}^{m}\{\beta(2j+1)-\beta(2j)\}=\sum_{j=1}^{m}\{\beta(2j+2)+2\beta(2j+1)+\beta(2j)-\beta(2j+1)-2\beta(2j)-\beta(2j-1)\}$$

$$=\beta(2m+2)+\beta(2m+1)-\beta(2)-\beta(1)=\gamma(2m+2)-\gamma(2) \text{ where } \gamma(m)=\beta(m)+\beta(m-1).$$

It follows that

$$r_0^n(a_n d^{-1})^{\gamma(2m+2)-\gamma(2)}(-a_0 d^2)^{\gamma(2m+3)-\gamma(3)}(-1)^{\gamma(2m+2)-\gamma(2)+n}=A_0^0 r_{2m}r_{2m+1}.$$

Using the first expression for r_{2m} we see that this is equivalent to

$$(-1)^n r_0^{n-1}r_1^{-1}=A_0^0 \tag{11}$$

or

$$-(-a_n a_0 d(-a_0 d^2)^{n-4})^{n-1}\cdot((-a_n a_0 d(-a_0 d^2)^{n-4})^{-(n-2)}(-a_0 d^2)^2)=a_n a_0 d(-a_0 d^2)^{n-2}=A_0^0,$$

which may be verified from (4).

We must also establish

$$r_{2m+2}=A_0^{2m}(r_{2m+1})^{n-1}(r_{2m})^{-n}. \tag{12}$$

This is equivalent to

$$r_{2m+2}r_{2m+1}=(r_{2m+1}r_{2m}^{-1})^n A_0^{2m}.$$

By (8) we must prove that

$$r_{2m+2}r_{2m+1}=A_0^0\prod_{j=1}^{m+1}(r_{2j-1}r_{2j-2}^{-1})^n.$$

Summing exponents again we have

$$r_{2m+2}r_{2m+1}=A_0^0(-a_n d^{-1})^{\gamma(2m+3)-\gamma(1)}(-a_0 d^2)^{\gamma(2m+4)-\gamma(2)}$$

$$=A_0^0 r_{2m+2}r_{2m+1}(-a_n d^{-1})^{-\gamma(1)}(-a_0 d^2)^{-\gamma(2)}=A_0^0 r_{2m+2}r_{2m+1}(r_0 r_{-1})^{-1},$$

using the recursion formula for $\beta(m)$ and the formula for r_m. We see that (12) is equivalent to

$$A_0^0=r_0 r_{-1}=(-1)^n r_0^{n-1}r_1^{-1},$$

which is (11).

We verify that

$$A_k^{2m}(-r_{2m})^k(-r_{2m+1})^{n-k}((-r_{2m})^n)^{-1}=A_k^{2m}(r_{2m+1}r_{2m}^{-1})^{n-k}=A_k^{2m+2}, \tag{13}$$

using the definition of A_k^{2m+2}.

Set $k=0$ in (13). Then using $A_0^{2m+2}=A_0^{2m}(r_{2m+1}r_{2m}^{-1})^n$ along with (12) we may write

$$r_{2m+2}=A_0^{2m+2}(r_{2m+1})^{-1}. \tag{14}$$

We define E_{2m} to be the equation

$$\sum_{k=0}^{n} A_k^{2m}x^k=v_1(xy+r_{2m}), \tag{15}$$

where $$(xy,\ a_0a_nd)=1.$$

Now $E_0=(4)$. By induction we shall show that for each $m\geqslant 0$ E_{2m+2} is equivalent to E_{2m}. Line (15) is equivalent to

$$\sum_{k=0}^{n} A_k^{2m}x^ky^n=v_2(xy+r_{2m}) \text{ with } (xy,\ a_0a_nd)=1. \tag{16}$$

(Recall that r_m is a power product of a_0, a_n, and d which is divisible by a_0a_nd, for each $m\geqslant 0$.)

Line (16) is equivalent to

$$\sum_{k=0}^{n} A_k^{2m}(-r_{2m})^ky^{n-k}=v_3(xy+r_{2m}), \text{ with } (xy,\ a_0a_nd)=1. \tag{17}$$

Now (17) is equivalent to

$$\sum_{k=0}^{n} A_k^{2m}(A_0^{2m})^{-1}(-r_{2m})^ky^{n-k}=v_4(xy+r_{2m}), \text{ with } (xy,\ a_0a_nd)=1 \tag{18}$$

by the comment after (9) and the fact that $|A_0^{2m}|$ is a power product of a_0, a_n, and d. Taking both sides of (18) mod y and using $(y,\ a_0a_nd)=1$ we see that

$$v_4=x_1y+(A_0^{2m})^{-1}(-r_{2m})^n(r_{2m})^{-1}=x_1y+r_{2m+1}$$

by (10). Since a_0a_nd divides $A_k^{2m}(A_0^{2m})^{-1}(-r_{2m})^k$ if $k>0$ (see the comment after line (9)) we see that $(x_1y,\ a_0a_nd)=1$. Using (10) we may write the equivalent statement

$$\sum_{k=0}^{n} A_k^{2m}(A_0^{2m})^{-1}(-r_{2m})^ky^{n-k}=v_5(x_1y+r_{2m+1}), \text{ with } (x_1y,\ a_0a_nd)=1. \tag{19}$$

As before we may write

$$\sum_{k=0}^{n} A_k^{2m}(A_0^{2m})^{-1}(-r_{2m})^ky^{n-k}x_1^n=v_6(x_1y+r_{2m+1}), \text{ with } (x_1y,\ a_0a_nd)=1, \tag{20}$$

instead of (19), so

$$\sum_{k=0}^{n} A_k^{2m}(A_0^{2m})^{-1}(-r_{2m})^k(-r_{2m+1})^{n-k}x_1^k=v_7(x_1y+r_{2m+1}) \text{ with } (x_1y,\ a_0a_nd)=1 \tag{21}$$

is also equivalent to (19). We may write, after dividing above by $(A_0^{2m})^{-1}(-r_{2m})^n$, the equivalent statement

$$\sum_{k=0}^{n} A_k^{2m+2}x_1^k=v_8(x_1y+r_{2m+1}), \text{ with } (x_1y,\ a_0a_nd)=1, \tag{22}$$

by (13) and the fact that $(A_0^{2m})^{-1}(-r_{2m})^n$ is a power product of a_0, a_n, and d. Taking (22) mod x_1 we see that

$$v_8 = x_1y_1 + A_0^{2m+2}(r_{2m+1})^{-1} = x_1y_1 + r_{2m+2}, \text{ by (14), where } (x_1y_1,\ a_0a_nd) = 1$$

by the remark after (8). Thus (15) is equivalent to

$$\sum_{k=0}^{n} A_k^{2m+2}x_1^k = v_9(x_1y_1 + r_{2m+2}). \tag{23}$$

This completes the induction.

Now to find solutions of

$$\sum_{k=0}^{n} A_k^{2m}x^n = v_1(xy + r_{2m}). \tag{24}$$

Suppose we solve $xy + r_{2m} = 1$. Obviously (24) has solutions corresponding to these choices of x and y.

Set $a_na_0d(-a_0d^2)^{n-4} = A$ and $-a_0d^2 = B$. Note $|A| > 1$ and $|B| > 1$, as $|d| > 1$. If

$$xy = A^{\beta(2m+1)}B^{\beta(2m+1)-\beta(2m)} + 1 = 1 - r_{2m}$$

we have a solution of E_{2m}. Given $N > 0$ we shall show that we may choose m such that $1 - r_{2m}$ has at least N distinct pairs of factors. (Then E_{2m} has at least N solutions as does the original equation.)

Let w and $\overline{w}$ be the roots of $x^2 - (n-2)x + 1 = 0$. Note that w is a unit in the ring R of algebraic integers in $Q(\sqrt{n^2-4n})$. Thus for any rational integer $k > 1$, w, and $\overline{w}$ go into units when we form the ring R/kR. The units in R/kR form a finite group so there exists a positive integer θ such that $(\omega)^\theta \equiv 1 \bmod kR$. Using the formula for $\beta(m)$ from finite differences, we see that

$$\beta(2m + 2\theta + 1) \equiv \beta(2m + 1) \bmod kR$$

and

$$\beta(2m + 2\theta) \equiv \beta(2m) \bmod kR;$$

clearly both congruences hold also mod k. Setting $k = \varphi(|1 - r_0|)$ it follows that $1 - r_0$ divides $1 - r_{2\theta}$. Now set $k_1 = \varphi(|1 - r_{2\theta}|)$, and continue. (Note that as $|A| > 1$ and $|B| > 1$ the $|1 - r_{2m}|$ form an increasing sequence.) We see that the number of factors of $1 - r_{2m}$ goes to infinity on a subsequence of positive integers m. This concludes the proof of the Theorem.

(Paper 72B1-255)