Pacific Journal of Mathematics

THE DIOPHANTINE EQUATION $Y(Y+m)(Y+2m)(Y+3m) = 2X(X+m)(X+2m)(X+3m)$

S. JEYARATNAM

Vol. 60, No. 1 September 1975

PACIFIC JOURNAL OF MATHEMATICS
Vol. 60, No. 1, 1975

THE DIOPHANTINE EQUATION $Y(Y+m)(Y+2m)(Y+3m) = 2X(X+m)(X+2m)(X+3m)$

S. JEYARATNAM

J. H. E. Cohn has shown that the equation of the title has only four pairs of nontrivial solutions in integers when $m = 1$. The object of this paper is to prove the following two theorems concerning the solutions of the equation of the title:

THEOREM 1. *The equation of the title has only four pairs of nontrivial solutions in integers given by* $X = 4m$ **or** $-7m$, $Y = 5m$ **or** $-8m$ *when* m *is of the form*

$$2^r \prod p_i^{s_i} \prod q_j^{t_j}$$

where r, s_i**'s** *and* t_j**'s** *are nonnegative integers,* p_i**'s** *are positive primes* $\equiv 3, 5 \pmod 8$ *and* q_j**'s** *are positive primes* $\equiv 1 \pmod 8$ *such that*

$$2^{(q_j-1)/4} \equiv -1 \pmod{q_j}.$$

THEOREM 2. *The only positive integral solution of the equation of the title, for all positive integral values of* $m \leqq 30$, *is* $X = 4m$, $Y = 5m$.

We shall call a solution of

$$(1)\quad Y(Y+m)(Y+2m)(Y+3m) = 2X(X+m)(X+2m)(X+3m)$$

primitive if it satisfies $(X, Y, m) = 1$.

LEMMA 1. *Every solution of* (1) *which is not a primitive solution is a multiple of a primitive solution with a smaller* m *and conversely.*

Suppose X, Y, m satisfy (1) and $(X, Y, m) = K > 1$. Dividing both sides of (1) by K^4, we have

$$\frac{Y}{K}\left(\frac{Y}{K}+\frac{m}{K}\right)\left(\frac{Y}{K}+2\left(\frac{m}{K}\right)\right)\left(\frac{Y}{K}+3\left(\frac{m}{K}\right)\right) = 2\frac{X}{K}\left(\frac{X}{K}+\frac{m}{K}\right)\left(\frac{X}{K}+2\left(\frac{m}{K}\right)\right)\left(\frac{X}{K}+3\left(\frac{m}{K}\right)\right)$$

and the lemma follows.

LEMMA 2. *Equation* (1) *with* $(X, Y, m) = 1$ *is equivalent to*

$$A^2 - 2B^2 = -m^4; \quad (A, B) = 1 \tag{2}$$

$$5m^2 + 4A = y^2 \tag{3}$$

and

$$5m^2 + 4B = x^2. \tag{4}$$

Substituting $x = 2X + 3m$ *and* $y = 2Y + 3m$ *in* (1), *we get*

$$\left(\frac{y^2 - 5m^2}{4}\right)^2 - 2\left(\frac{x^2 - 5m^2}{4}\right)^2 = -m^4.$$

Now putting

$$A = \frac{y^2 - 5m^2}{4} \quad \text{and} \quad B = \frac{x^2 - 5m^2}{4}$$

we obtain (2), (3) *and* (4). *It is easily seen that* $(X, Y, m) = 1$ *implies* $(A, B) = 1$ *and conversely.*

LEMMA 3. *There does not exist any primitive solution of* (1) *if* m *has a prime factor* $p \equiv 2, 3, 5 \pmod 8$.

By Lemma 2, (1) leads to $A^2 - 2B^2 = -m^4$; $(A, B) = 1$. It is sufficient to show that $p \mid A$ and $p \mid B$.

Case (i). Let $p = 2$. Then $2 \mid A^2 \Rightarrow 2 \mid A \Rightarrow 2 \mid B^2 \Rightarrow 2 \mid B$.

Case (ii). Let $p \equiv 3, 5 \pmod 8$. Suppose $p \nmid A$. Then $p \nmid B$. Also $A^2 \equiv 2B^2 \pmod p$. Therefore the Jacobi-Legendre symbol $(2B^2 \mid p) = 1$. But $(2B^2 \mid p) = (2 \mid p) = (-1)^{(p^2-1)/8} = -1$ and we have a contradiction. Hence $p \mid A$ and therefore $p \mid B$ also.

LEMMA 4. *There is no primitive solution of* (1) *if* m *has any prime factor* $p \equiv 1 \pmod 8$ *such that* $2^{(p-1)/4} \equiv -1 \pmod p$.

From (2), *we have*

$$A^2 - 2B^2 \equiv 0 \pmod p; \quad (A, B) = 1. \tag{5}$$

Suppose $p \nmid A$, then $p \nmid B$. By (3) and (4), A and B are quadratic residues of p and therefore by Euler's criterion

$$A^{(p-1)/2} \equiv B^{(p-1)/2} \equiv 1 \pmod p. \tag{6}$$

Now from (5), $A^{(p-1)/2} \equiv 2^{(p-1)/4} \cdot B^{(p-1)/2} \pmod{p}$, and using (6), we have $2^{(p-1)/4} \equiv 1 \pmod{p}$, a contradiction. The lemma follows.

Proof of Theorem 1. Combining Lemmas 2, 3 and 4, we see that (1) has no primitive solution when m takes the form stated in the theorem and $m > 1$.

J. H. E. Cohn [1] has shown that (1) has only four pairs of nontrivial solutions given by $X = 4$ or -7, $Y = 5$ or -8, when $m = 1$. The theorem now follows in view of Lemma 1.

Now we shall show that if all positive solutions of (1) are known, all the solutions of (1) can be written down with a little effort.

In Lemma 2 removing the restriction $(X, Y, m) = 1$, we have (3), (4),

$$A^2 - 2B^2 = -m^4 \tag{7}$$

$$x = 2X + 3m \tag{8}$$

and

$$y = 2Y + 3m. \tag{9}$$

In view of (8) we see that if $|x| \leqq 3m$ then $0 \leqq X \leqq -3m$. Clearly if x satisfies (4) so will $-x$. Also, when $x > 3m$, $-x < -3m$ and x leads to a positive X while $-x$ leads to a negative X. A similar argument holds for y. The result now becomes obvious.

Next we shall show that (1) has no positive primitive solution when $m = 7$ or 23.

When $m = 7$, (2), (3) and (4) read

$$A^2 - 2B^2 = -7^4; \quad (A, B) = 1 \tag{10}$$

$$5 \cdot 7^2 + 4A = y^2 \tag{11}$$

$$5 \cdot 7^2 + 4B = x^2. \tag{12}$$

All the solutions of a class of solutions of

$$A^2 - 2B^2 = -7^4 \tag{13}$$

whose fundamental solution is $a + b\sqrt{2}$ are given by

$$a_k + b_k\sqrt{2} = (a + b\sqrt{2})(3 + \sqrt{2})^k.$$

Now, the fundamental solutions of (13) are

$$\pm 49 \pm 49\sqrt{2}, \quad \pm 7 \pm 35\sqrt{2}, \quad \pm 31 \pm 41\sqrt{2}.$$

The classes of solutions of the first eight fundamental solutions cannot give rise to primitive solutions. We note that negative solutions of (13) can also be ignored as they cannot lead to positive solutions of (1). Thus for $a_k > 0$, $b_k > 0$ we must have $a + b\sqrt{2} > 0$ and accordingly need consider only the two cases

$$a_k + b_k\sqrt{2} = (31 + 41\sqrt{2})(3 + 2\sqrt{2})^k$$

and

$$a_k + b_k\sqrt{2} = (-31 + 41\sqrt{2})(3 + 2\sqrt{2})^k.$$

In each case we find that $b_{k+3} \equiv b_k \pmod 7$, and in each case the only residues modulo 7 which occur are 3, 5 and 6; since none of these is a quadratic residue modulo 7, the conclusion follows.

When $m = 23$, the fundamental solutions of (7) are

$$\pm 529 \pm 529\sqrt{2}, \quad \pm 161 \pm 391\sqrt{2}, \quad \pm 151 \pm 389\sqrt{2}$$

and a similar method can be used to show that (1) has no positive primitive solution when $m = 23$.

Proof of Theorem 2. We note that $2^{(17-1)/4} \equiv -1 \pmod{17}$. Now, applying Theorem 1, Theorem 2 is true for

$$m = 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18,$$
$$19, 20, 22, 24, 25, 26, 27, 29 \text{ and } 30.$$

When $m = 7$, (1) has no positive primitive solution. Combining this result with Lemmas 1 and 3, Theorem 2 is true for

$$m = 7, 14, 21 \text{ and } 28.$$

The fact that when $m = 23$ (1) has no positive primitive solution, completes the proof of the theorem.

REMARKS. When $m = 7$, all the solutions of (1) can be written down using the result following the proof of Theorem 1. The nontrivial solutions are the twelve pairs,

$$X = 4 \cdot 7 \text{ or } -7 \cdot 7, \qquad Y = 5 \cdot 7 \text{ or } -8 \cdot 7$$
$$X = -10 \text{ or } -11, \qquad Y = 1 \text{ or } -22$$
$$X = -15 \text{ or } -6, \qquad Y = -5 \text{ or } -16.$$

Similarly when $m = 23$, the only solutions apart from the trivial ones are the eight pairs,

$$X = 4 \cdot 23 \text{ or } -7 \cdot 23, \qquad Y = 5 \cdot 23 \text{ or } -8 \cdot 23$$
$$X = -18 \text{ or } -51, \qquad Y = -6 \text{ or } -63.$$

When $m = 31$, there are infinite number of positive solutions of (7) which are quadratic residues of 31 and thus the method used for the cases $m = 7$, 23 fails here.

Lastly I should like to express my thanks to the referee and to Professor P. Kanagasabapathy for many helpful suggestions.

REFERENCE

1. J. H. E. Cohn, *The diophantine equation* $Y(Y+1)(Y+2)(Y+3) = 2X(X+1)(X+2)(X+3)$, Pacific J. Math., **37** (1971), 331–335.

Received March 27, 1974 and in revised form November 22, 1974.

UNIVERSITY OF SRI LANKA,
PERADENIYA,
SRI LANKA (CEYLON).

Vol. 60, No. 1

CONTENTS

D. E. Bennett, *Strongly unicoherent continua* 1
Walter R. Bloom, *Sets of p-spectral synthesis* 7
R. T. Bumby and D. E. Dobbs, *Amitsur cohomology of quadratic extensions: Formulas and number-theoretic examples* 21
W. W. Comfort, *Compactness-like properties for generalized weak topological sums* 31
D. R. Dunninger and J. Locker, *Monotone operators and nonlinear biharmonic boundary value problems* 39
T. S. Erickson, W. S. Martindale, 3rd and J. M. Osborn, *Prime nonassociative algebras* 49
P. Fischer, *On the inequality* $\sum_{i=1}^{n} p_i \frac{f(p_i)}{f(q_i)} \geqq 1$ 65
G. Fox and P. Morales, *Compact subsets of a Tychonoff set* 75
R. Gilmer and J. F. Hoffmann, *A characterization of Prüfer domains in terms of polynomials* 81
L. C. Glaser, *On tame Cantor sets in spheres having the same projection in each direction* 87
Z. Goseki, *On semigroups in which* $X = XYX = XZX$ *if and only if* $X = XYZX$ 103
E. Grosswald, *Rational valued series of exponentials and divisor functions* 111
D. Handelman, *Strongly semiprime rings* 115
J. N. Henry and D. C. Taylor, *The* $\bar{\beta}$ *topology for w*-algebras* 123
M. J. Hodel, *Enumeration of weighted p-line arrays* 141
S. K. Jain and S. Singh, *Rings with quasiprojective left ideals* 169
S. Jeyaratnam, *The diophantine equation* $Y(Y+m)(Y+2m)\times(Y+3m) = 2X(X+m)(X+2m)(X+3m)$ 183
R. Kane, *On loop spaces without p torsion* 189
Alvin J. Kay, *Nonlinear integral equations and product integrals* 203
A. S. Kechris, *Countable ordinals and the analytic hierarchy, I* 223
Ka-Sing Lau, *A representation theorem for isometries of* $C(X, E)$ 229
I. Madsen, *On the action of the Dyer-Lashof algebra in* $H_*(G)$ 235
R. C. Metzler, *Positive linear functions, integration, and Choquet's theorem* 277
A. Nobile, *Some properties of the Nash blowing-up* 297
G. E. Petersen and G. V. Welland, *Plessner's theorem for Riesz conjugates* 307

Pacific Journal of Mathematics
Vol. 60, No. 1 September, 1975

Donald Earl Bennett, *Strongly unicoherent continua* 1
Walter Russell Bloom, *Sets of p-spectral synthesis* 7
Richard Thomas Bumby and David Earl Dobbs, *Amitsur cohomology of quadratic extensions: formulas and number-theoretic examples* 21
W. Wistar (William) Comfort, *Compactness-like properties for generalized weak topological sums* 31
Dennis Robert Dunninger and John Stewart Locker, *Monotone operators and nonlinear biharmonic boundary value problems* 39
Theodore Erickson, Wallace Smith Martindale, III and J. Marshall Osborn, *Prime nonassociative algebras* 49
Pál Fischer, *On the inequality* $\sum_{i=0}^{n} [f(p_i)/f(q_i)]p_i \geq i$ 65
Geoffrey Fox and Pedro Morales, *Compact subsets of a Tychonoff set* 75
Robert William Gilmer, Jr. and Joseph F. Hoffmann, *A characterization of Prüfer domains in terms of polynomials* 81
Leslie C. Glaser, *On tame Cantor sets in spheres having the same projection in each direction* 87
Zensiro Goseki, *On semigroups in which* $x = xyx = xzx$ *if and only if* $x = xyzx$ 103
Emil Grosswald, *Rational valued series of exponentials and divisor functions* 111
David E. Handelman, *Strongly semiprime rings* 115
Jackson Neal Henry and Donald Curtis Taylor, *The* $\bar{\beta}$ *topology for* W^**-algebras* 123
Margaret Jones Hodel, *Enumeration of weighted p-line arrays* 141
Surender Kumar Jain and Surjeet Singh, *Rings with quasi-projective left ideals* 169
S. Jeyaratnam, *The Diophantine equation* $Y(Y+m)(Y+2m)(Y+3m) = 2X(X+m)(X+2m)(X+3m)$ 183
Richard Michael Kane, *On loop spaces without p torsion* 189
Alvin John Kay, *Nonlinear integral equations and product integrals* 203
Alexander S. Kechris, *Countable ordinals and the analytical hierarchy. I* 223
Ka-Sing Lau, *A representation theorem for isometries of* $C(X, E)$ 229
Ib Henning Madsen, *On the action of the Dyer-Lashof algebra in* $H_*(G)$ 235
Richard C. Metzler, *Positive linear functions, integration, and Choquet's theorem* 277
Augusto Nobile, *Some properties of the Nash blowing-up* 297
Gerald E. Peterson and Grant Welland, *Plessner's theorem for Riesz conjugates* 307