A NOTE ON A DIOPHANTINE EQUATION CONSIDERED BY POWELL

B. G. Sloss*
Department of Mathematics, Advanced College, RMIT University,
GPO Box 2476V, Melbourne, Victoria 3001, Australia
(Submitted April 2000)

1. INTRODUCTION

B. J. Powell [2] conjectured that, for any positive even integer m and for any positive integer n sufficiently large for which $mn+1=q$, where q is a prime, the Diophantine equation

$$Ax^n + By^n = Cz^n \tag{1}$$

has no solutions in positive integers x, y, and z, where A, B, and C are natural numbers. Q. Sun [4] provided evidence in favor of this conjecture by showing that, if

$$(A \pm B \pm C)(A \pm B)(A \pm C)(B \pm C) \neq 0,$$

where A, B, and C are even nonzero integers, then, if

$$n > [(|A| + |B| + |C|)^{\phi(m)} - 1]/m$$

and $q = nm+1$ is prime, $\phi(m)$ is Euler's totient function, then equation (1) has only the trivial solution $xyz = 0$.

A corollary of a theorem in the paper of G. Faltings [1] is that equation (1) has only finitely many solutions, coprime in pairs, for $n > 3$.

Thus, there has been considerable interest in the problem of the solvability of (1) in integers. In this paper we find further conditions under which (1) has no nontrivial natural number solutions. Various relationships between variables in the equation are found excluding the possibility of nontrivial solutions.

In the following we denote by $\mathbb{N}$ the set of nonzero positive integers and we denote by $\mathbf{Z}$ the set of integers.

2. RESULTS

We consider the Diophantine equation

$$Ax^n + Y = Cz^n, \tag{2}$$

where A, C, Y, x, n, and z are all integers. Clearly, (1) is a special case of (2). Therefore, if (2) has no solutions for $Y = By^n$, then (1) has no solutions.

Two lemmas are given before our main theorem. This Theorem 1 specifies conditions on a prime natural number, such that if these conditions hold then (2) has no solutions and therefore the corresponding version of (1) has no solution for a specific choice of variables.

Lemma 1: If $A, C, Y, x, z, n \in \mathbb{N}$ in equation (2), then $A > C$ implies $x < z$.

Proof: If $A > C$, then $x^n < \frac{A}{C}x^n < z^n$ because $Ax^n < Cz^n$. So $x < z$. □

---

* We must sadly report that the author of this article recently passed away so any questions or concerns should be sent to the editor.

The following lemma is an application of the binomial theorem and is crucial to our arguments.

Lemma 2: Suppose q is a prime, $N, M, x, z \in \mathbb{Z}$ and $A, C, q, u, t \in \mathbb{N}$. $Ax^m + q^t M = Cz^m$ and $Ax^r + q^u N = Cz^r$, where $q^t | C^m A^r - C^r A^m$ (which is satisfied, in particular, by $q^t | C - A$), and $(q, m) = (q, C) = (q, A) = (q, x) = (q, N) = 1$, then $u \geq t$.

Proof: Now

$$z^{mr} = \left(\frac{A}{C}x^m + \frac{q^t M}{C}\right)^r = \left(\frac{A}{C}x^r + \frac{q^u N}{C}\right)^m.$$

So, from the binomial theorem, we find that

$$N_1 q^{2t} + N_2 q^{2u} = (C^m A^r - C^r A^m)x^{rm} + rC^m A^{r-1} x^{m(r-1)} q^t M - mC^r A^{m-1} x^{r(m-1)} q^u N$$

for particular $N_1, N_2 \in \mathbb{Z}$.

So $t > u$ implies $q | mCAxN$, which implies $q | m$ or $q | C$ or $q | A$ or $q | x$ or $q | N$; which are all contradictions. □

Theorem 1: Let q be a prime, when there exists $t, n \in \mathbb{N}$, $n > q - 1$ such that $q^t | A - C, q^t \| Y$ then there are no solutions to the Diophantine equation (2) for $(q, n) = (q, Ax) = (q, Cz) = 1$, where q^t does not divide $z^{q-1} - x^{q-1}$. In particular, this last condition holds if either

(a) $t > (q-1)\log_q z$ and $A > C, Y, x, z \in \mathbb{N}$, or,

(b) if q^2 does not divide $z - x$ but $q | z - x, Y \in \mathbb{Z}$.

Proof: Now we may assume

$$Ax^n + q^t M = Cz^n \tag{3}$$

and

$$Ax^{n-q+1} + q^u N = Cz^{n-q+1}, \tag{4}$$

where $(q, N) = 1$ by the lesser Fermat theorem. Therefore, from Lemma 2,

$$u = t + k, \text{ where } k \in \mathbb{N} \cup \{0\}.$$

Hence, after multiplying (4) by x^{q-1}, we obtain that

$$Ax^n + q^{t+k+q-1} N_q = Cz^{n-q+1} x^{q-1} \tag{5}$$

for $N_q = x^{q-1} N \in \mathbb{Z}$. Then, after subtracting (3) from (5), we find that

$$q^{t+k+q-1} N_q = Cz^{n-q+1}(x^{q-1} - z^{q-1}) + q^t M.$$

Therefore, $q^t | z^{q-1} - x^{q-1}$, since $(C, q) = (x, q) = (z, q) = 1$. Thus, (2) has no solutions for $q^t > z^{q-1}$ when $A > C$, because $z > x$ from Lemma 1. After taking logarithms, this is equivalent to $t > (q-1)\log_q z$.

Now assume that the conditions of case (b) hold, then

$$\frac{z^{q-1} - x^{q-1}}{z - x} = z^{q-2} + xz^{q-3} + \cdots + x^{q-2}$$
$$\equiv (q-1)z^{q-2} \pmod{q}.$$

Hence, the left-hand side is not divisible by q, because $(q-1, q) = (q, z) = 1$. So q^2 does not divide $z^{q-1} - x^{q-1}$. □

3. EXAMPLES

As an example of our Theorem 1, we show that the following Diophantine problem is not solvable, where the details are given in our Theorem 2.

Theorem 2: If $x, y, t, k \in \mathbb{N}$, then the Diophantine equation $(1+3^t)x^5 + 3^t y^5 = 5^{5k}$ has no solution for $(x, 3) = (y, 3) = (k, 3) = 1$ and $t > 4k$.

Proof: The conditions of Theorem 1(a) are satisfied for $q = 3$, $A = (1+3^t)$, $z = 5^k$, and $n = 5$, since $t > 4k > 2k \log_3(5)$. □

It would be very interesting to find an elementary proof of Fermat's last theorem; to this end, we provide a new elementary sufficient condition for Fermat's last theorem to hold. This condition is given as Theorem 3. A more general result can be found in the paper by K. A. Ribet [3]. However, Theorem 2 provides a purely elementary route to a solution of the Diophantine equation under consideration.

Theorem 3: Fermat's last theorem holds if there are no $t \in \mathbb{N}$ and $x, y, z \in \mathbb{Z}$, such that, for $p \geq 3$ a prime, $x^p + 2^t y^p = z^p$ and $z - x = 2^t L$ for some $L \in \mathbb{Z}$ with $(x, 2y) = (2y, z) = (x, z) = (y, 2) = 1$.

Proof: It is well known that to prove Fermat's last theorem we need only show that there are no integer solutions to the Diophantine equation $x^p + y^p + z^p = 0$, with $(x, y) = (y, z) = (x, z) = 1$. Hence, we may assume that

$$x^p + 2^t y_1^p = z^p, \tag{6}$$

where x, z, $y_1 \in \mathbb{Z}$, with $(2y_1, z) = (x, z) = (2y_1, x) = (y_1, 2) = 1$, by rearranging the variables if necessary, since two of the x, y, z must be odd. All the conditions of Theorem 1 are satisfied for equation (6) for the case $q = 2$. Because x, z are odd, we may assume that $z - x = 2(2J+1)$ or $z - x = 4K$, where $J, K \in \mathbb{Z}$. In the first case, $2 | z - x$ but 4 does not divide $z - x$. Consequently, from Theorem 1, Fermat's theorem holds in this case. Hence, $z - x = 4L^1$ for $L^1 \in \mathbb{Z}$. Hence,

$$\begin{aligned} 2^t y^p &= z^p - x^p \\ &= (z-x)(z^{p-1} + xz^{p-2} + \cdots + x^{p-1}) \\ &= 4L^1((x+4L^1)^{p-1} + x(x+4L^1)^{p-2} + \cdots + x^{p-1}) \\ &= 4L^1 F, \end{aligned}$$

thus defining F.

So $2^{t-2} y^p = L^1 F$. Suppose $2 | F$, then $2 | px^{p-1}$, which implies $2 | p$ or $2 | x$; a contradiction. Thus, $2^{t-2} | L^1$ and $(2, F) = 1$. Therefore, there exists $L \in \mathbb{Z}$ such that $z - x = 2^t L$. □

The paper by K. A. Ribet [3] states that the Diophantine equation $x^n + q^t y^n + z^n = 0$, where q and n are distinct prime numbers and $q \in \{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}$ does not have any solution for $n > 11$. Theorem 4 uses Theorem 1 to obtain, in particular, an asymptotic result concerning the related Diophantine equation

$$x^n + q^t y^n = z^n \tag{7}$$

for infinitely many q and n. Note that Theorem 4 is not a special case of Q. Sun's aforementioned theorem, because in Theorem 4 n is not required to satisfy the constraint that $nm+1$ is a prime for suitable m, but n is required, in particular, to be coprime with respect to q; which is a weaker constraint.

Theorem 4: The Diophantine equation (7), with q, x, n, t, y, and z natural numbers, q an odd prime, and $(q,n)=(q,x)=(q,y)=(q,z)=1$, has no solutions if

$$\frac{z^n-x^n}{z^{q-1}-x^{q-1}}>y^n.$$

In particular, no solution exists if

$$x>y^{\frac{n}{n-1}}(q-1)^{\frac{1}{n-1}}z^{\frac{q-1}{n-1}}.$$

Hence, there exists a positive integer $N(x,q,y,z)$ such that there are no solutions to (7) for $n>N$ and $x>y$.

Proof: Suppose $q^t>z^{q-1}-x^{q-1}$, then q^t does not divide (fully) $z^{q-1}-x^{q-1}$. Therefore, from Theorem 1, there is no solution to the Diophantine equation (7) when

$$\frac{z^n-x^n}{y^n}=q^t>z^{q-1}-x^{q-1},$$

which is equivalent to

$$\frac{z^n-x^n}{z^{q-1}-x^{q-1}}>y^n, \tag{8}$$

given that (7) holds.

So there is no solution to (7), given that (8) holds, which, after canceling the factor $z-x$, results in

$$\frac{z^{n-1}+xz^{n-2}+\cdots+x^{n-1}}{z^{q-2}+xz^{q-3}+\cdots+x^{q-2}}>y^n.$$

Noting that $z>x$, this is satisfied if

$$\frac{nx^{n-1}}{(q-1)z^{q-1}}>y^n,$$

which occurs if and only if

$$\frac{\log(n)}{n}+\frac{n-1}{n}\log(x)>\log(y)+\frac{1}{n}\log((q-1)z^{q-1}).$$

This, in turn, is satisfied if

$$\log(x)>\frac{n}{n-1}\log(y)+\frac{1}{n-1}\log((q-1)z^{q-1}).$$

Consequently (7) has no solutions when

$$x>y^{\frac{n}{n-1}}(q-1)^{\frac{1}{n-1}}z^{\frac{q-1}{n-1}}.$$

In particular, let y, q, and z be all fixed, then, given $\varepsilon>0$, there is $M>0$ such that there are no solutions to (7) for $n>M$, $(n,q)=(x,q)=(y,q)=1$,

$$x>y(1+\varepsilon).$$

Thus, there exists $N > 0$ such that, if $n > N$, there are no solutions to (7) when $x > y$, because x and y are integers and ε may be chosen arbitrarily small. □

REFERENCES

1. G. Faltings. "Endlichkeitssätze für abelsche Varietäten über zahlenöpern." *Invent. Math.* **73** (1983):349-66.
2. B. J. Powell. "Proof of the Impossibility of the Fermat Equation $X^p + Y^p = Z^p$ for Special Values of p and of the More General Equation $bX^n + cY^n = dZ^n$." *J. Number Theory* **18** (1984):34-40.
3. K. A. Ribet. "On the Equation $a^p + 2^\alpha b^p + c^p = 0$." *Acta Arithmetica* **79** (1997):7-16.
4. Q. Sun. "On a Conjecture Posed by B. J. Powell." *Sichuan Daxue Xuebao* **31.2** (1994): 145-47.

AMS Classification Numbers: 11D09, 11D44

❖❖❖

Cal Long Active in Fibonacci Research Conferences

(Continued from page 242)

program, and he was a consultant to the Washington State Superintendent of Public Instruction, to the State Department of Education and to the National Science Foundation.

Concerning The Fibonacci Association, Cal is a Charter Member. He served on the Board of Directors from July 6, 1983 to June 19, 1999 and he was the President for the last fifteen years. He was a strong supporter of the Fibonacci Research Conferences, attending most of them and presenting papers. Under his leadership, the organization became stronger and more unified.

On the unprofessional side, Cal is an avid fisherman and lover of the outdoors. It was not unusual to see him fly casting in the lakes and streams or walking the trails of the idyllic Idaho wilderness and sometimes you could even see him boating down the rapids of the Snake River. Cal also has a beautiful tenor voice, which he put to good use as a member of his church choir, a member of the Vandeleers, a well known University of Idaho choral group, a member of the Eugene Gleesmen, during his graduate years, a member of the Pullman/Moscow Chorale and a member of the Idaho-Washington Symphony Chorale. Cal was also a very dedicated husband whose strongest supporter was his wife Jean on whom he always knew he could count on because her support was always there. Finally, Cal was a devoted father to his two children, Tracy and Greg.

Cal, for all that you have done in so many ways for so many people, we say thank you. Enjoy retirement and know that you have made a difference to so many people who have crossed your path.