JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume 5, June 1992

On The Diophantine equation $A^4 + B^4 + a^2C^4 = D^4$

S. HAHN AND Y. OH

Generalizing the Fermat's last conjecture, Euler made a conjecture that the Diophantine equation

$$A_1^N + A_2^N + \cdots + A_{N-1}^N = A_N^N$$

has no solution in positive integers if N is greater than 3. After two centuries, for $N = 5$, a first counterexample was found by a through computer search. It was

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

And this was the only known counterexample until recently. In 1988, Noam Elkies found a counterexample for the Diophantine equation

$$A^4 + B^4 + C^4 = D^4.$$

Actually he found infinitely many counterexamples. One of the solutions is

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Let a be a positive integer. In this paper we want to study the Diophantine equation

$$A^4 + B^4 + a^2C^4 = D^4 \tag{1}$$

Received by the editors on April 20, 1992.
1980 *Mathematics subject classifications*: Primary 11D.

of the title. Here we may assume that a is square-free. Our method is a slight generalization of Elkies' original ideas. First consider the surface

$$r^4 + s^4 + a^2t^2 = 1 \tag{2}$$

by dividing the original equation by D^4. Let's change the variables by $r = x + y, s = x - y$. Don Zagier observed the following identity

$$1 - r^4 - s^4 = P^2 - 2QR$$

where

$$P = 4x^2 - 1, Q = y^2 + 3x^2 + 2x, R = y^2 + 3x^2 - 2x.$$

(There is a misprint in Elkies' paper, where y in Q and R should be changed to y^2.) If we let $Q = 0$, then $1 - r^4 - s^4$ is a perfect square. Applying to this identity the automorphism group of the ternary quadratic form $P^2 - 2QR$, one obtain infinitely many conics $Q = 0$ on which $1 - r^4 - s^4$ is a perfect square. And the surface is given as a pencil of conics parametrized by u:

$$(u^2 + 2)y^2 = -(3u^2 - 8u + 6)x^2 - 2(u^2 - 2) - 2u, \tag{3.1}$$

$$(u^2 + 2)at = 4(u^2 - 2)x^2 + 8ux + (2 - u^2). \tag{3.2}$$

The involution $u \mapsto 2/u$ changes (r, s, t, x, y) by $(-s, -r, -t, -x, y)$. So we may take u to be of the form $u = 2m/n$ with m and n relatively prime integers, $m \geq 0$ and n odd. Then the parametrization is written as :

$$(2m^2 + n^2)y^2 = -(6m^2 - 8mn + 3n^2)x^2 - 2(2m^2 - n^2)x - 2mn, \tag{4.1}$$

$$(4.2) \qquad (2m^2 + n^2)at = 4(2m^2 - n^2)x^2 + 8mnx + (n^2 - 2m^2).$$

Now we want to find some $u = 2m/n$ for which the conic (4.1) has infinitely many solutions. For an integer k define $S(k) =$ the largest positive integer whose square divides k. Also define $R(k) = k/S^2(k)$. For the conic (4.1) to have infinitely many rational points it is necessary and sufficient that both

$$R(2m^2 + n^2), R(2m^2 - 4mn + n^2)$$

are products of primes congruent to 1 mod 8.

Let's take an example of Elkies, with $(m, n) = (2, 1)$. Then from the conic $9y^2 = -11x^2 - 14x - 4$ we get a solution $(x, y) = (-1/2, 1/6)$ and the parametrizations

$$(x, y) = \left(-\frac{k^2 + 2k + 17}{2k^2 + 22}, -\frac{k^2 + 6k - 11}{6k^2 + 66}\right),$$

$$(r, s, at) = \left(\frac{2k^2 + 6k + 20}{3k^2 + 33}, \frac{k^2 + 31}{3k^2 + 33}, \frac{4(2k^4 - 3k^3 + 28k^2 - 75k + 80)}{(3k^2 + 33)^2}\right).$$

For the Diophantine equation (1) to have a solution, t has to be a square. So $a(2k^4 - 3k^3 + 28k^2 - 75k + 80)$ must be a square. Hence we are led to find rational solutions of the elliptic curve

$$E/\mathbf{Q} : Y^2 = a(2X^4 - 3X^3 + 28X^2 - 75X + 80).$$

As an example let $a = 47$. Then $E(\mathbf{Q})$ has a point $P = (X, Y) = (7, 470)$. From this we get a solution $(8, 4, 1, 9)$ of the equation

$$A^4 + B^4 + 2209C^4 = D^4.$$

From this solution we can try to find other solutions. This is done exactly by the addition law on the elliptic curve $E/\mathbf{Q}$ since each point of $E(\mathbf{Q})$ gives a solution of the equation (1). One easy way to do this is let $Y = bX^2 + cX + d$ and find the coefficients b, c, and d so that the intersection of this parabola with the elliptic curve has a triple multiple point at P. By this way one get

$$196912^4 + 180236^4 + 2209 \cdot 9677^4 = 225333^4$$

which corresponds to $2P$. If we proceed one more time, we get

$$A = 2527070945952645400163757129068028930455\!60,$$

$$B = 3430370689351650739166563862767661672277\!64,$$

$$C = 2326880313730193601859577105628055478100\!1,$$

$$D = 3691652980004434867664880717650269965556\!65.$$

Note that if the rank of $E(\mathbf{Q})$ is positive then we get infinitely many solutions.

For the surface $r^4 + s^4 + a^2t^4 = 1$, we get the parametrization

$$(5.1) \quad (2m^2 + n^2)y^2 = -(6m^2 - 8mn + 3n^2)x^2 - 2(2m^2 - n^2)x - 2mn,$$

$$(5.2) \quad \pm(2m^2 + n^2)at^2 = 4(2m^2 - n^2)x^2 + 8mnx + (n^2 - 2m^2).$$

By completing the square the second conic (5.2) reduces to the standard form

$$(6) \qquad X^2 + \alpha Y^2 + \beta Z^2 = 0$$

where

$$\alpha = \pm R((2m^2 - n^2)(2m^2 + n^2)a),$$
$$\beta = -R((2m^2 - 2mn + n^2)(2m^2 + 2mn + n^2)),$$

$$X = (-2m^2 + n^2) + 4mnx, Y = \gamma t, Z = 2x\delta,$$

and

$$\gamma = S((2m^2 - n^2)(2m^2 + n^2)a),$$
$$\delta = S((2m^2 - 2mn + n^2)(2m^2 + 2mn + n^2)).$$

This equation (6) has infinitely many integer solutions if and only if $-\alpha$ is a square modulo β and $-\beta$ is a square modulo α. For simplicity suppose that a is prime to

$$(2m^2 - n^2)(2m^2 + n^2)(2m^2 - 2mn + n^2)(2m^2 + 2mn + n^2).$$

Then the first condition is that $\mp(4m^4 - n^4)a$ is a square modulo $R(2m^2 - 2mn + n^2)$ and $R(2m^2 + 2mn + n^2)$. The second condition is that $4m^4 + n^4$ is a square modulo $R(2m^2 - n^2)$ and $R(2m^2 + n^2)$ and a. Note the congruences

$$(4m^4 - n^4)a \equiv 8m^4a \equiv -2n^4a \bmod (2m^2 \pm 2mn + n^2).$$

So $2a$ and $-2a$ must both be the quadratic residues of each prime factor of

$$R(2m^2 \pm 2mn + n^2).$$

Also note the congruences

$$4m^4 + n^4 \equiv 2n^4 \equiv -(2mn)^2 \bmod (2m^2 + n^2).$$

So -1 and 2 must both be quadratic residues of each prime factor of $R(2m^2 + n^2)$. And

$$4m^4 + n^4 \equiv (2mn)^2 \bmod (2m^2 - n^2).$$

So the second conic (5.2) has infinetely many rational points if and only if each prime divisor p of $R(2m^2-2mn+n^2)$ satisfies $p \equiv 1 \bmod 4$ and

$$\left(\frac{2a}{p}\right) = 1,$$

each prime divisor of $R(2m^2 + n^2)$ is congruent to 1 mod 8, and for each prime divisor p of a

$$\left(\frac{4m^4 + n^4}{p}\right) = 1.$$

Here $(\ /p)$ denotes the Legendre symbol. All this can be used to reduce the search range of possible $u = 2m/n$ but eventually one has to find a non-trivial rational point on some elliptic curve. We tried to find a non-trivial torsion point of an elliptic curve which gives a counterexample to Euler's conjecture, but without success.

In fact Demjanenko already found a two parameter family of solutions for (1) with $a = 1$. And in his parametrization, one has to find rational points on the following elliptic curve, for some rational number k, where

$$\begin{gathered} E/\mathbf{Q} \ : \ Y^2 = 8(1+k)^6X^4 \\ +4(1-10k-56k^2-96k^3-60k^4+20k^5+48k^6+24k^7+4k^8)X^3 \\ +8k(-1+14k+44k^2+18k^3-66k^4-106k^5-60k^6-12k^7)X^2 \\ +4(1+2k-32k^3-28k^4+124k^5+256k^6+200k^7+52k^8)X \\ +4k(-2-2k+6k^3-24k^4-94k^5-104k^6-48k^7). \end{gathered}$$

However it looks difficult to find a counterexample to Euler's conjecture because the degree of k is eight.

REFERENCES

[1] N. Elkies, *On* $A^4 + B^4 + C^4 = D^4$, Math. Comp. **Vol.51** No.184 (1988), 825-835.

[2] V. Demjanenko, *L. Euler's conjecture*, Acta. Arith. **Vol.25** (1973-74), 127–135 (Russian).

[3] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Springer-Verlag, 1990.

Department of Mathematics
KAIST
Taejon, 305-701, Korea