ELLIPTIC CURVES AND INTEGRAL SOLUTIONS TO $A^4 + B^4 + C^4 = D^4$

ERIC S. ROWLAND

1. Introduction

In 1769 Euler conjectured that the equation

$$A_1^n + A_2^n + \cdots + A_{n-1}^n = A_n^n$$

has no positive integer solutions for $n \geq 3$. The case $n = 3$ corresponds to the case $A^3 + B^3 = C^3$ of Fermat's last theorem and was proven to have no nontrivial solutions by Fermat himself. However, for $n \geq 4$ the conjecture was open until 1966, when Lander and Parkin in [6] found the following counterexample for $n = 5$ by computer search:

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

The only other known primitive solution for $n = 5$ was found by J. Frye in August 2004:

$$55^5 + 3183^5 + 28969^5 + 85282^5 = 85359^5.$$

(See [7] for a large collection of identities involving sums of like powers.) While these solutions are small enough to have been found without the use of much theory, the first counterexamples to the $n = 4$ case,

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

were found by reducing the problem to that of finding rational points on elliptic curves. In 1988 Elkies found the solution

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

and shortly after, R. Frye found the smallest counterexample to Euler's conjecture for $n = 4$:

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

For every primitive solution to (1), Elkies's method provides infinitely many additional primitive solutions; these are obtained via the group law on an elliptic curve. In the current account, we follow Elkies's paper [5] in showing the role of elliptic curves in the discovery of Elkies's first solution and how to obtain other solutions.

Date: December 16, 2004.

Six solutions to (1) are currently known that were not discovered from other points via the group law:

$$1390400^4 + 2767624^4 + 673865^4 = 2813001^4,$$
$$5507880^4 + 8332208^4 + 1705575^4 = 8707481^4,$$
$$5870000^4 + 11289040^4 + 8282543^4 = 12197457^4,$$
$$12552200^4 + 14173720^4 + 4479031^4 = 16003017^4,$$
$$3642840^4 + 7028600^4 + 16281009^4 = 16430513^4,$$
$$219076465^4 + 275156240^4 + 630662624^4 = 638523249^4.$$

The solutions $D = 2813001$ and $D = 638523249$ were found by MacLeod using Elkies's method (on a different elliptic curve than Elkies's), and the other four were found by Bernstein using an algorithm that does not employ elliptic curves. See [7] and [1] for more details.

It is interesting to note that, in light of these counterexamples and other identities involving sums of like powers, an "Euler's extended conjecture" has been formulated by Ekl in [4]. This revised version states that if

$$\sum_{i=1}^{n} A_i^k = \sum_{j=1}^{m} B_j^k$$

for positive integers A_i, B_j with $A_i \neq B_j$ for all i and j, then $m + n \geq k$. No counterexamples to this conjecture are known, and equality is achieved in the above examples, where $m = 1$ and $n = k - 1$.

2. An Example

Finding an integral solution to (1) is equivalent to finding a rational point on the surface given by the equation

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

In [3] Demjanenko parametrizes the surface $r^4 + s^4 + t^2 = 1$ as a family of conics in the parameter u. Replacing t by $\pm t^2$ in this parametrization gives the following parametrization of (2):

$$r = x + y, \quad s = x - y; \tag{3a}$$
$$(u^2 + 2)y^2 = -(3u^2 - 8u + 6)x^2 - 2(u^2 - 2)x - 2u, \tag{3b}$$
$$\pm(u^2 + 2)t^2 = 4(u^2 - 2)x^2 + 8ux - (u^2 - 2). \tag{3c}$$

These equations, along with (2), define a conic for each value of the parameter u. To find rational points (r, s, t) on (2), our method will be to look for rational points on (3) for fixed values of u.

For example, letting $u = 0$ gives the equations

$$y^2 = -3x^2 + 2x,$$
$$\pm t^2 = -4x^2 + 1.$$

The first conic has the obvious rational point $(x, y) = (0, 0)$. We parametrize the rational solutions as follows. The line of rational slope k passing through $(0, 0)$

intersects $y^2 = -3x^2 + 2x$ at another rational point,

$$(x, y) = \left(\frac{2}{k^2+3}, \frac{2k}{k^2+3}\right),$$

so we have

$$\pm t^2 = -4x^2 + 1 = \frac{k^4 + 6k^2 - 7}{(k^2+3)^2}.$$

Introducing the variable $z = (k^2+3)t$ gives

$$\pm z^2 = k^4 + 6k^2 - 7.$$

These two curves are of genus 1 and have the rational point $(k, z) = (1, 0)$, so they are elliptic curves. The change of variables $k = 1 - 4/(1 \mp X), z = 8Y/(1 \mp X)^2$ puts them into Weierstrass form:

$$Y^2 = X^3 + X \mp 2. \tag{4}$$

These appear as curves #112A and #56C in [2] (p. 96 and 87). The curve $Y^2 = X^3 + X - 2$ has only two rational points: the point at infinity and $(1, 0)$. The curve $Y^2 = X^3 + X + 2$ has only four rational points: the point at infinity, $(-1, 0)$, and $(1, \pm 2)$. The points $(\pm 1, 0)$ correspond to the trivial solution

$$\begin{aligned} r = x + y &= \frac{2 + 2k}{k^2+3} = \frac{X^2 - 1}{X^2 + 3} = 0, \\ s = x - y &= \frac{2 - 2k}{k^2+3} = \frac{\pm 2X + 2}{X^2 + 3} = 1, \\ \pm t^2 &= \frac{k^4 + 6k^2 - 7}{(k^2+3)^2} = -\frac{4(X^3 + X \mp 2)}{(X^2+3)^2} = 0 \end{aligned}$$

of (2), and the points $(1, \pm 2)$ correspond to the solution $r = 0, s = 0, t = 1$. By projectivizing $X \mapsto X/Z, Y \mapsto Y/Z$, one finds that for both curves (4) the point $[X, Y, Z] = [0, 1, 0]$ at infinity corresponds to the solution $0^4 + 0^4 + 0^4 = 0^4$ of (1). Thus $u = 0$ does not yield any nontrivial rational points.

3. First Solution

We must choose a different value for u in order to find nontrivial solutions. Fortunately, it is possible to narrow the search in several ways. First we show that we need only consider rational u.

Note that since $r = x + y$ and $s = x - y$, we have $r^4 + s^4 = 2x^4 + 12x^2y^2 + 2y^4$. We solve (3b) for u and replace $x \mapsto (r+s)/2, y \mapsto (r-s)/2$ to find

$$\begin{aligned} u &= \frac{-1 + 4x^2 \pm \sqrt{1 - 2x^4 - 12x^2y^2 - 2y^4}}{2x + 3x^2 + y^2} \\ &= \frac{-1 + (r+s)^2 \pm \sqrt{1 - r^4 - s^4}}{r^2 + rs + s^2 + r + s} \\ &= \frac{-1 + (r+s)^2 \pm t^2}{r^2 + rs + s^2 + r + s}. \end{aligned}$$

Therefore every rational solution (r, s, t) of (2) lies on the conic (3) for some rational (or infinite) u.

Besides u being rational, we can restrict its form as follows. Replacing u by $2/u$ in (3b) has the effect of applying the map $(x, y) \mapsto (-x, y)$. Similarly, replacing u by $2/u$ in (3c) has the effect of mapping $(x, t^2) \mapsto (-x, -t^2)$. Therefore the involution

$u \mapsto 2/u$ simply takes $(x, y, t^2) \mapsto (-x, y, -t^2)$ and consequently $(r, s) \mapsto (-s, -r)$. Since the two solutions (r, s, t) and $(-s, -r, t)$ are so similar, we can eliminate the redundancy by considering only u of the form $2m/n$ with $(2m, n) = 1$ and $m \geq 0$, since if u is not of this form then $2/u$ is.

Now (3b,c) become

$$(2m^2 + n^2)y^2 = -(6m^2 - 8mn + 6n^2)x^2 - 2(2m^2 - n^2)x - 2mn, \tag{5b}$$

$$\pm(2m^2 + n^2)t^2 = 4(2m^2 - n^2)x^2 + 8mnx - (2m^2 - n^2). \tag{5c}$$

For a nonzero integer n, define $P(n)$ as the set of primes p dividing n with odd exponent. That is, if n factors as $n = \pm p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, let

$$P(n) = \{p_i \mid \alpha_i \equiv 1 \bmod 2\}.$$

For example, $P(\pm p^k) = \{p\}$ for prime p and odd k, and $P(\pm n^2) = \varnothing$ for $n \neq 0$. Vacuously, we have $P(\pm 1) = \varnothing$.

The next lemma (of [5]) gives sufficient conditions for (5b,c) to have rational solutions.

Lemma.

(1) *The conic* (5b) *has infinitely many rational points* (x, y) *if every prime*

$$p \in P(2m^2 + n^2) \cup P(2m^2 - 4mn + n^2)$$

satisfies $p \equiv 1 \bmod 8$. *Otherwise it has no rational points.*

(2) *The conic* (5c) *has infinitely many rational points* (x, t) *if every prime*

$$p \in P(2m^2 - 2mn + n^2) \cup P(2m^2 + n^2) \cup P(2m^2 + 2mn + n^2)$$

satisfies $p \equiv 1 \bmod 8$. *Otherwise it has no rational points.*

(The quadratic forms

$$2m^2 - 4mn + n^2, \quad 2m^2 - 2mn + n^2, \quad \text{and} \quad 2m^2 + 2mn + n^2$$

are nonzero for integers m, n, not both 0, since

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

We are interested, then, in relatively prime pairs (m, n), m nonnegative and n odd, that satisfy the conditions of both parts of the lemma, for then there are (infinitely many) rational points on $r^4 + s^4 + t^4 = 1$ with $u = 2m/n$. The first few such pairs are $(0, -1)$, $(0, 1)$, $(4, -7)$, $(8, -5)$, $(12, 5)$, $(8, -15)$, $(4, 25)$, $(20, -1)$, $(8, -27)$, $(20, -9)$, and $(12, -29)$. The first two yield $u = 0$, which we examined in Section 2. Next we consider $(m, n) = (4, -7)$, for which (5b,c) become

$$81y^2 = -467x^2 + 34x + 56,$$
$$\pm 81t^2 = -68x^2 - 224x + 17.$$

However, these cannot simultaneously hold: If either the denominator of x or the denominator of t is divisible by 5, then both denominators are divisible by 5. Reducing modulo 125 then results in a contradiction under this assumption, namely that ± 117 is a square mod 125. Therefore the denominators of x, t, and (by a similar argument) y are not divisible by 5. The right side $-68x^2 - 224x + 17$ is

$\pm$ a square modulo 5 only if $x \equiv 1 \bmod 5$, but then $-467x^2 + 34x + 56 \equiv 3 \bmod 5$ is not a square. Thus there are no rational solutions for $u = -8/7$.

We now try $(m, n) = (8, -5)$, for which (5b,c) become the system

$$153y^2 = -779x^2 - 206x + 80,$$
$$\pm 153t^2 = 412x^2 - 320x - 103,$$

which has rational solutions. The first conic has the rational point $(3/14, 1/42)$, and the line of slope $k/3$ passing through this point intersects it again at

$$(x, y) = \left(\frac{51k^2 - 34k - 5221}{14(17k^2 + 779)}, -\frac{17k^2 + 7558k - 779}{42(17k^2 + 779)} \right). \tag{6}$$

Substituting this value of x into the second conic gives the equation

$$\pm 21^2(17k^2 + 779)^2 t^2 = -4(31790k^4 - 4267k^3 + 1963180k^2 - 974003k - 63237532).$$

With the change of variables $X = (k + 2)/7, Y = 3(17k^2 + 779)t/14$, this becomes the curve

$$Y^2 = -31790X^4 + 36941X^3 - 56158X^2 + 28849X + 22030, \tag{7}$$

where we have taken the plus sign since the right side reduces modulo 3 to $(X^2 + X - 1)^2$ and -1 is not a square modulo 3. Elkies executed a computer search for rational values of X that make the right side of (7) a perfect square and discovered the point

$$(X_0, Y_0) = \left(-\frac{31}{467}, \frac{30731278}{467^2} \right),$$

which gives the value $k = 7X_0 - 2 = -1151/467$. Then the solution to (2) is

$$r = x + y = \frac{68k^2 - 3830k - 7442}{21(17k^2 + 779)} = \frac{2682440}{20615673},$$
$$s = x - y = \frac{85k^2 - 3728k - 8221}{21(17k^2 + 779)} = -\frac{18796760}{20615673},$$
$$t = \frac{14Y_0}{3(17k^2 + 779)} = \frac{15365639}{20615673}.$$

Clearing denominators gives Elkies's first solution to (1):

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

4. Additional Solutions

Since (7) has the rational points $P_\pm = (X_0, \pm Y_0)$, it is an elliptic curve E. We may use the group law on E to find additional rational points on E and thus additional rational points on (2). Letting P_- be the identity element of $E(\mathbb{Q})$, the point P_+ is identified with $Q = P_+ - P_-$. As the Weierstrass form of E with respect to the identity P_- has coefficients much larger than those of (7), it is more convenient to use coordinates X, Y rather than the Weierstrass coordinates. Rather than computing in the group by secant and tangent lines, we accordingly compute using secant and tangent parabolas $Y = aX^2 + bX + c$. If such a parabola intersects E in four points P_1, P_2, P_3, P_4 (counting multiplicity), then

$$\frac{aX^2 + bX + c - Y}{(X - X_0)^2}$$

is a rational function on E with divisor $P_1 + P_2 + P_3 + P_4 - 2(P_+ - P_-)$, so

$$P_1 + P_2 + P_3 + P_4 = 2Q$$

in the group law. Given three points P_1, P_2, P_3, we can find a, b, c so that the parabola $Y = aX^2 + bX + c$ passes through these points. Then the X-coordinate of the fourth point of intersection P_4 of the parabola with E will be the fourth root of a quartic equation with three known rational roots (the X-coordinates of P_1, P_2, P_3).

By this method we now compute the coordinates of $-Q$ in the group law on E. We put $P_1 = P_2 = P_3 = P_+$, so that $P_4 = 2Q - 3P_+ = -Q$. To obtain a parabola that has triple contact with E at P_+, we use the first few terms of the Taylor series of Y at $X = X_0$:

$$\begin{aligned} Y &= \sqrt{-31790X^4 + 36941X^3 - 56158X^2 + 28849X + 22030} \\ &= Y_0 + \alpha(X - X_0) + \beta(X - X_0)^2 + \cdots, \end{aligned}$$

where one computes

$$\begin{aligned} \alpha &= \frac{937766474523}{467 \cdot 15365639}, \\ \beta &= -\frac{2096569897386251210893331}{2 \cdot 15365639^3}. \end{aligned}$$

Then we let

$$aX^2 + bX + c = Y_0 + \alpha(X - X_0) + \beta(X - X_0)^2,$$

so that

$$\begin{aligned} a &= -\frac{2096569897386251210893331}{2 \cdot 15365639^3}, \\ b &= \frac{3349372196776233628154 66}{15365639^3}, \\ c &= \frac{1076124066222818157529571}{2 \cdot 15365639^3}. \end{aligned}$$

Substituting $aX^2 + bX + c$ for Y in (7) gives the quartic equation

$$(aX^2 + bX + c)^2 = -31790X^4 + 36941X^3 - 56158X^2 + 28849X + 22030,$$

which has a triple root at $X = X_0$ and a fourth root

$$X = \frac{1274739344939668202218656423135632 83}{1297595594858724312829527106686985 69}$$

as the X-coordinate of $-Q$. Unraveling the formulas for r, s, t in terms of X gives the solution

$$\begin{aligned} A &= 14399657106489544922685067718331752678502014266153004422182923363366 33, \\ B &= 44172646989945384969435974897549528458546724971790478988641242093469 20, \\ C &= 90339645774825323880594824293984572910049479250057430281474657326458 80, \\ D &= 91617818300354368478324523982672660382270029622572436620703708887221 69. \end{aligned}$$

One can continue in this manner to find additional rational points on (7), albeit of increasing height. We can repeat the procedure, for example, with $P_1 = P_2 = P_3 = -Q$ to compute $5Q$, but whereas the height of $-Q$ is on the order of 10^{70}, the height of $5Q$ is on the order of 10^{634}.

One may ask if infinitely many solutions can be obtained from Q. This is the question of whether Q is in the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$. By a theorem of Mazur

(Theorem VIII.7.5 in [8]), $E(\mathbb{Q})_{\text{tors}}$ has order at most 12, so to show that Q has infinite order it suffices to show that $[n]Q \neq 0$ for $n = 2, 3, \ldots, 12$, and indeed this is true. Therefore from the solution found in Section 3 we actually get infinitely many primitive solutions to (1).

Of course, some of the other values of u listed in Section 3 yield additional solutions. For example, Frye's minimal solution

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

lies on the curve given by $(m, n) = (20, -9)$.

References

[1] D. J. Bernstein, Enumerating solutions to $p(a) + q(b) = r(c) + s(d)$, *Math. Comput.* **70** (2001), 389–394.

[2] B. J. Birch and W. Kuyk, *Modular Functions on One Variable IV*, Lecture Notes in Math. **476**, Springer-Verlag, 1975.

[3] V. A. Demjanenko, L. Euler's conjecture, *Acta Arith.* **25** (1973–74), 127–135.

[4] R. L. Ekl, New results in equal sums of like powers, *Math. Comput.* **67** (1998), 1309–1315.

[5] N. D. Elkies, On $A^4 + B^4 + C^4 = D^4$, *Math. Comput.* **51** (1988), 825–835.

[6] L. J. Lander and T. R. Parkin, Counterexample to Euler's conjecture on sums of like powers, *Bull. Amer. Math. Soc.* **72** (1966), 1079.

[7] J.-C. Meyrignac, *Computing Minimal Equal Sums Of Like Powers*, http://euler.free.fr.

[8] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, 1986.