MATHEMATICS OF COMPUTATION
VOLUME 51, NUMBER 184
OCTOBER 1988, PAGES 825–835

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

By Noam D. Elkies

Abstract. We use elliptic curves to find infinitely many solutions to $A^4+B^4+C^4 = D^4$ in coprime natural numbers A, B, C, and D, starting with

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

We thus disprove the $n = 4$ case of Euler's conjectured generalization of Fermat's Last Theorem. We further show that the corresponding rational points $(\pm A/D, \pm B/D, \pm C/D)$ on the surface $r^4 + s^4 + t^4 = 1$ are dense in the real locus. We also discuss the smallest solution, found subsequently by Roger Frye.

1. Introduction. Euler conjectured in 1769 that the Diophantine equation $A^4 + B^4 + C^4 = D^4$, or more generally

$$A_1^N + A_2^N + \cdots + A_{N-1}^N = A_N^N \qquad (N \geqslant 4),$$

has no solution in positive integers. (See [4, pp. 648ff.] for the early history of this and related problems, and [5, Problem D1] for more recent research.) Nearly two centuries later, a computer search [7] found the first and hitherto only known counterexample to the general conjecture,

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

but direct computer searches found no counterexample for $N = 4$, even though this first case of the conjecture could not be proved.

In this paper we disprove this conjecture, exhibiting several counterexamples and giving a recursive construction of infinitely many solutions for $A^4 + B^4 + C^4 = D^4$ in relatively prime natural numbers A, B, C, D. Since that Diophantine equation is homogeneous, solving it is equivalent to finding a point

$$(r, s, t) = \left(\pm\frac{A}{D}, \pm\frac{B}{D}, \pm\frac{C}{D}\right)$$

on the surface $r^4 + s^4 + t^4 = 1$ with rational coordinates r, s, t. In Section 2, we start with an analysis of a parametrization of the simpler equation $r^4 + s^4 + t^2 = 1$ as a pencil of conics. This yields a parametrization of $r^4 + s^4 + t^4 = 1$ as a pencil of curves of genus one. We consider this parametrization in Section 3, and find the simplest curve in the pencil which could possibly have a rational point that would disprove Euler's conjecture. It happens that there is such a rational point of sufficiently small height to have been found by a direct computer search; this produced our first solution

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

Received October 14, 1987; revised January 21, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11D25, 11G05.

(This solution was beyond the range of earlier exhaustive searches. We could only find it by restricting the variables to lie on an appropriate curve. The transformation from the natural coordinates on that curve to the values of r, s, t required rational functions sufficiently complicated (see (6) below) to get from the 2- and 3-digit numerator and denominator of the X-coordinate on that curve to our solution's 7- and 8-digit numbers.) We then show, in Section 4, how to use the theory of elliptic curves to recursively generate arbitrarily many other solutions from our first one. Throughout this paper we shall assume and use basic definitions and facts about elliptic curves, for which a good reference is [9].

The author gratefully acknowledges the support of Harvard University's Society of Fellows and the Communications Research Division of the Institute for Defense Analyses for the research reported in this paper. The numerical and symbolic computations needed for this research were greatly facilitated by the computer program MACSYMA.

2. The Surface $r^4 + s^4 + t^2 = 1$. In [3, p. 135] Demjanenko expresses the surface

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

as a pencil of conics parametrized by u:

$$r = x + y, \quad s = x - y; \tag{2a}$$

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

$$(u^2 + 2)t \quad = 4(u^2 - 2)x^2 + 8ux + (2 - u^2). \tag{2c}$$

[We also have the conic $y^2 = -2x - 3x^2$, $t = 4x^2 - 1$ corresponding to the limit $u \to \infty$; this special case is equivalent to a parametrization given by Escott in the late 19th century (see [4, p. 658])—we shall say more about this, and the similar parametrization with $u = 0$, in Section 3. The parametrization (2) has been independently rediscovered at least three times, by Andrew Bremner, Don Zagier and the present author. Bremner wrote (1) as

$$2(1 + r^2)(1 + s^2) = (1 + r^2 + s^2)^2 + t^2$$

and factored both sides over $\mathbf{Q}(\sqrt{-1})$ [1]. Zagier, generalizing from several special cases of (2) communicated to him by de Vogelære, observed that Escott's parametrization is equivalent to the identity $1 - r^4 - s^4 = P_0^2 - 2Q_0R_0$ with

$$P_0 = 4x^2 - 1, \quad Q_0 = y + 3x^2 + 2x, \quad R_0 = y + 3x^2 - 2x$$

(x, y given by (2a)), and, applying to this identity the automorphism group (isomorphic to $PSL_2(\mathbf{Q})$) of the ternary quadratic form $P^2 - 2QR$, obtained infinitely many representations of $1 - r^4 - s^4$ as $P^2 - 2QR$, and so infinitely many conics $Q = 0$ on which $1 - r^4 - s^4$ is a perfect square ([10], which also finds the conditions of Lemmas 1 and 2 below). The present author looked directly for an ellipse in the rs-plane tangent to the Fermat quartic $r^4 + s^4 = 1$ at four points.]

Solving (2b) for u, we find

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

and (2c) then selects the plus sign. Thus every rational solution of (1) lies on the conic (2) for some rational or infinite value of u. Furthermore, the involution $u \mapsto 2/u$ merely replaces (r, s, t, x, y) by $(-s, -r, -t, -x, y)$ in the parametrization (2). Thus we may take u of the form $2m/n$ with m and n relatively prime integers, $m \geqslant 0$ and n odd, because otherwise $2/u$ is of that form and the two corresponding conics (2) are essentially the same.

We may now write (2b,c) in the form

$$(3b) \qquad (2m^2 + n^2)y^2 = -(6m^2 - 8mn + 3n^2)x^2 - 2(2m^2 - n^2)x - 2mn,$$
$$(3c) \qquad (2m^2 + n^2)t = 4(2m^2 - n^2)x^2 + 8mnx + (n^2 - 2m^2).$$

If rational numbers x and y satisfy (3b) then we may recover t from (3c) and r, s from (2a) and thus find a rational solution to (1); so we need only consider the conic (3b). It will be convenient to define the functions $S(k)$, $R(k)$ of a nonzero integer k by $S(k)$ = the largest positive integer whose square divides k and $R(k) = k/S^2(k)$; for instance, for $k = \pm 23, \pm 24, \pm 25$ we have $S(k) = 1, 2, 5$ and $R(k) = \pm 23, \pm 6, \pm 1$. Then we have

LEMMA 1. *The conic* (3b) *has infinitely many rational points* (x, y) *if*

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

are both products of primes congruent to 1 mod 8, *and none otherwise.*

Remarks. i) In particular, $2m^2 - 4mn + n^2$ must be positive, that is, $u^2 - 4u + 2 > 0$ so $|u - 2| > \sqrt{2}$, else even the real locus of (3b)—and a fortiori also the rational locus—is empty. This is an example of a "local condition at infinity"; the congruence condition on the prime factors of $2m^2 + n^2$ and $2m^2 - 4mn + n^2$ comes from local conditions at these finite primes. Since the curve (3b) has genus zero, these necessary local conditions for the existence of a rational point are also sufficient ("Hasse principle"). Compare this with the situation for curves of genus one to be encountered in the next Section.

ii) By Quadratic Reciprocity, the prime factors of $R(2m^2 + n^2)$ are already all congruent to 1 or 3 mod 8, and those of $R(2m^2 - 4mn + n^2)$ to ± 1 mod 8, so the 1 mod 8 condition is not as stringent as it may first appear.

Proof. First reduce (3b) to the standard form

$$(4) \qquad X^2 + aY^2 + bZ^2 = 0$$

with a and b squarefree integers, by "completing the square":

$$\begin{aligned}[2mn + (2m^2 - n^2)x]^2 \\ &= 2mn[2mn + 2(2m^2 - n^2)x + (6m^2 - 8mn + 3n^2)x^2] \\ &\quad + (4m^4 - 12m^3n + 12m^2n^2 - 6mn^3 + n^4)x^2 \\ &= -2mn(2m^2 + n^2)y^2 + (2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2)x^2,\end{aligned}$$

and taking $X = 2mn+(2m^2-n^2)x$, $Y = \alpha y$, $Z = \beta x$, where $\alpha = S(2mn(2m^2+n^2))$ and $\beta = S((2m^2 - 2mn+n^2)(2m^2 - 4mn+n^2))$; then $a = R(2mn(2m^2+n^2))$ and $b = R((2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2))$ in (4). Note that from a nontrivial rational solution to (4) we may recover a rational solution to (3b) by multiplying X, Y, and Z by a constant factor to make $X = 2mn + (2m^2 - n^2)x$ and $Z = \beta x$ consistent.

But it is known that, in general, an equation (4) has a rational solution—indeed, infinitely many rational solutions—if and only if at least one of a and b is negative and $-a$ and $-b$ are congruent to squares modulo b and a respectively (see [6, pp. 272–275] for an effective algorithmic proof). Since n is odd and m, n are relatively prime, we easily show that m, n, $2m^2+n^2$, $2m^2-2mn+n^2$, and $2m^2-4mn+n^2$ are relatively prime in pairs, and thus that we need only ask that $-2mn(2m^2 + n^2)$ be a square modulo each prime dividing $R(2m^2 - 2mn+n^2)$ and $R(2m^2 - 4mn+n^2)$, and that $(2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2)$ be a square modulo each prime dividing $R(m)$, $R(n)$ and $R(2m^2 + n^2)$. Three of these five conditions always hold: $(2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2)$ is congruent modulo m and n to the squares n^4, $4m^4$ respectively, and

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

The remaining two conditions yield the lemma's constraints, for

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

so each prime factor of $R(2m^2 + n^2)$ must have not only -2 but also $+2$ as a quadratic residue; likewise

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

so each prime factor of $R(2m^2 - 4mn + n^2)$ must have both -2 and $+2$ as quadratic residues; thus all these primes must be congruent to 1 mod 8. (Note that, since n is odd, so are $2m^2 + n^2$ and $2m^2 - 4mn + n^2$, whence 2 cannot occur as a prime factor.) Finally, if $R(2m^2 - 4mn + n^2) = -b$ is a product of positive primes then b is negative in (4), so we are done. □

For instance, we may take $u = 4$, when $(m, n) = (2, 1)$ satisfies the hypotheses of Lemma 1; then (3b) becomes $9y^2 = -11x^2 - 14x - 4$, for which we find by inspection the rational solution $(x, y) = (-\frac{1}{2}, \frac{1}{6})$ and recover from (2) the solution $(r, s, t) = (\frac{1}{3}, \frac{2}{3}, \frac{8}{9})$ to (1). Furthermore, projecting from the known point $(x, y) = (-\frac{1}{2}, \frac{1}{6})$ we find the parametrization

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

of the conic $9y^2 = -11x^2 - 14x - 4$ (this is the other point on the intersection of the conic with the line of slope $k/3$ through $(-\frac{1}{2}, \frac{1}{6})$), from which we recover a parametric solution

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

to (1). In general, whenever u satisfies the hypotheses of Lemma 1 we will find a similar parametric solution of (1) with r and s of degree 2 and t of degree 4 with square denominator.

3. The Surface $r^4 + s^4 + t^4 = 1$. To find a rational solution (r, s, t) of

$$r^4 + s^4 + t^4 = 1, \tag{5}$$

we must solve (1) with the additional restriction that $\pm t$ be a square. Reasoning as before, we see that such a solution must necessarily have

$$r = x + y, \qquad s = x - y; \tag{6a}$$

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

$$\pm(2m^2 + n^2)t^2 = 4(2m^2 - n^2)x^2 + 8mnx + (n^2 - 2m^2) \tag{6c}$$

for some relatively prime integers m, n with n odd. For example, take $(m, n) = (0, 1)$ to get $y^2 = -3x^2 + 2x$, $\pm t^2 = 1 - 4x^2$. The first conic has the obvious point $(x, y) = (0, 0)$, from which we find the parametrization

$$x = \frac{2}{k^2 + 3}, \qquad y = kx,$$

so

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

or, with the new variable $z = (k^2 + 3)t$,

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

These are two curves of genus one with rational points $(k, z) = (1, 0)$ and are thus elliptic curves. To bring them into Weierstrass form, perform the change of coordinates $k = 1 - 4/(1 \mp X)$, $z = 8Y/(1 \mp X)^2$ to obtain the elliptic curves

$$Y^2 = X^3 + X \mp 2.$$

These curves are listed as #112A and #56C in [2, pp. 96 and 87], where we find that they have only two and four rational points respectively: the point at infinity, the 2-torsion point $(X, Y) = (\pm 1, 0)$, and (for the curve $Y^2 = X^3 + X + 2$) the 4-torsion points $(X, Y) = (1, \pm 2)$. These correspond to the trivial solutions of (5) which are permutations of $(\pm 1, 0, 0)$.

To find nontrivial solutions we must choose different m and n. We then obtain other curves of genus one (the values of u for which that curve degenerates to genus zero are not rational); these curves will necessarily be principal homogeneous spaces for some elliptic curves, but need not be globally trivial homogeneous spaces like the two we obtained for $(m, n) = (0, 1)$ that is, they might not contain any rational points. To narrow down our choices of (m, n), we first use Lemma 1 and

the analogous

LEMMA 2. *The conic* (6c) *has infinitely many rational points* (x,t) *if*

$$R(2m^2-2mn+n^2), \quad R(2m^2+n^2) \quad \text{and} \quad R(2m^2+2mn+n^2)$$

are all products of primes congruent to 1 mod 8, *and none otherwise.*

Proof. Again we complete the square to find

$$\begin{aligned}[4mnx+(n^2-2m^2)]^2 &= (n^2-2m^2)[(n^2-2m^2)+8mnx+4(2m^2-n^2)x^2]+(16m^4+n^4)x^2\\ &= \mp(2m^2-n^2)(2m^2+n^2)t^2\\ &\quad +4(2m^2-2mn+n^2)(2m^2+2mn+n^2)x^2.\end{aligned}$$

As in the proof of Lemma 1, we find that $2m^2 \pm 2mn + n^2$ and $2m^2 \pm n^2$ are relatively prime in pairs and we need only ask that $\mp(4m^4 - n^4)$ be a square modulo $R(2m^2-2mn+n^2)$ and $R(2m^2+2mn+n^2)$ and that $4m^4+n^4$ be a square modulo $R(2m^2-n^2)$ and $R(2m^2+n^2)$. (Since $16m^4+4n^4>0$ the negativity condition is automatically satisfied.) We find that

$$4m^4-n^4 \equiv 8m^4 \equiv -2n^4 \bmod 2m^2 \pm 2mn + n^2,$$

so -2 and 2 must both be quadratic residues of each prime factor of

$$R(2m^2-2mn+n^2);$$

also

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

so -1 and 2 must both be quadratic residues of each prime factor of $R(2m^2+n^2)$; thus all these prime factors are congruent to 1 mod 8. The remaining condition is always satisfied since

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

so we are done. □

In particular, m must be divisible by 4. The first few (m,n) which satisfy the conditions of both Lemma 1 and Lemma 2 are the pair $(0,1)$ already encountered, $(4,-7)$, $(8,-5)$, $(8,-15)$, $(12,5)$, $(20,-1)$, and $(20,-9)$. Taking $(m,n)=(4,-7)$ fails, because then (6b) and (6c) become

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

which cannot simultaneously hold: the second equation forces x to have denominator not divisible by 5 with $x \equiv 4 \bmod 5$, and the first equation then refines this to $x \equiv 14 \bmod 25$, when

$$(-68x^2-224x+17)/25 \equiv 3 \bmod 5$$

cannot be of the form $\pm 81t^2$. We next try $(m,n)=(8,-5)$ and obtain

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

On the first conic we find by trial and error (or by applying the algorithm in [6]) the small rational solution $(x,y)=(3/14,1/42)$ and thus the parametrization

$$x = \frac{51k^2-34k-5221}{14(17k^2+779)}, \qquad y = \frac{17k^2+7558k-779}{42(17k^2+779)}. \tag{7}$$

Substituting this value of x into the second conic and simplifying, we find

$$\pm 21^2(17k^2+779)^2t^2 = -4(31790k^4 - 4267k^3 + 1963180k^2 - 974003k - 63237532). \tag{8}$$

The right side of this reduces modulo 3 to $(x^2-x-1)^2$, from which we easily show that for (8) to hold with rational x and t, the plus sign must be chosen. Using new coordinates $X = (k+2)/7$, $Y = 3(17k^2+779)t/14$, we then further simplify (8) to

$$Y^2 = -31790X^4 + 36941X^3 - 56158X^2 + 28849X + 22030. \tag{9}$$

We easily verify that there is no local obstruction to a rational solution for (9). This does not yet guarantee that such a solution exists, because (9) could still represent a nontrivial element of the Tate-Šafarevič group of the elliptic curve which is its Jacobian. But it does encourage us to look for small rational solutions, and in this case a few hours' computer (VAX) search for rational X such that the right-hand side of (9) is a perfect square revealed the solution

$$(X, Y) = \left(-\frac{31}{467}, \frac{30731278}{467^2}\right);$$

retracing our changes of variable we then recover the rational solutions

$$(r, s, t) = \left(-\frac{18796760}{20615673}, \frac{2682440}{20615673}, \frac{15365639}{20615673}\right) \tag{10}$$

for (5). Clearing denominators we obtain our first counterexample

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

to Euler's conjecture.

4. More Rational Solutions of (5). From our single solution to (9) we may now compute arbitrarily many others:

PROPOSITION. *There are infinitely many rational X that make the right-hand side*

$$-31790X^4 + 36941X^3 - 56158X^2 + 28849X + 22030$$

of (9) *a square. These yield infinitely many rational solutions* (r, s, t) *of* (5).

Proof. We know two rational points

$$P_\pm : (X, Y) = \left(-\frac{31}{467}, \pm\frac{30731278}{467^2}\right)$$

on the elliptic curve (8), so we need only show that the difference $Q = P_+ - P_-$ between them is of infinite order in the group of the Jacobian of that curve, i.e., is not a torsion point. By [8, Theorem 2], there are only finitely many groups that can occur as the rational torsion subgroup of an elliptic curve, and in particular no torsion point can have index greater than 12; this reduces the proof to a finite, if tedious, computation to show $n \cdot Q \neq 0$ for $n = 2, 3, \ldots, 12$. (Actually, we need not invoke Mazur's deep theorem here; we may instead compute the Néron-Tate canonical height of Q and find it positive, or show directly that Q is not a torsion point in the p-adic completion of (9) for some p. But Mazur's theorem later simplifies considerably our proof that the rational points on (5) are dense

in its real locus, so it seems natural to use that theorem here as well.) We can reduce the tedium by noting that the Jacobian of (9) has a rational point of order 2, corresponding to $(x, y, t) \mapsto (x, -y, -t)$ in (6b,c)—this does not depend on our choice $u = -16/5$—or

$$(X, Y) \mapsto \left(\frac{323 - 535X}{535 + 17X}, -\frac{291716}{17X + 535} Y \right)$$

in (9). Thus by Mazur's theorem we need only check that $n \cdot Q$ gives neither 0 nor a 2-torsion point for $n = 2, \ldots, 6$; and this indeed turns out to be the case. □

A note on the addition law on (9), or generally an elliptic curve E given in the form $Y^2 = \text{quartic}(X)$ with a known pair of rational points $P_\pm = (X_0, \pm Y_0)$: Take the point P_- to be the origin of our addition law, so P_+ is identified with $Q = P_+ - P_-$. It is then possible to find coordinate functions on E which put it in Weierstrass form, and then compute the addition law in the usual way by "chords and tangents", but these coordinate functions tend to have monstrously large coefficients even when the coefficients of E's defining quartic are only moderately large as in (9). It is more convenient to compute the addition law directly in terms of the given coordinates X, Y, using secant and tangent parabolas $Y = aX^2 + bX + c$. Indeed, if such a parabola meets E in four points P_1, P_2, P_3, P_4 counting multiplicity, then $P_1 + P_2 + P_3 + P_4 = 2Q$ in E's group law, because

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

is a rational function on E with divisor $P_1 + P_2 + P_3 + P_4 - 2(P_+ + P_-)$. Given P_1, P_2 and P_3, we can then solve the linear equations for a, b, c to make the parabola go through P_1, P_2, P_3, and find the X-coordinate of P_4 as the fourth zero of a quartic with three known roots, and the Y-coordinate as a known quadratic in X. So, for instance, to compute the coordinates of $-Q$, find a, b, c such that the parabola $Y = aX^2 + bX + C$ has a point of triple contact with E at P_+ (i.e., take

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

to be the beginning of the Taylor expansion of Y at $X = X_0$), then substitute $aX^2 + bX + c$ for Y in the equation of E to obtain a quartic in X with a known triple root at X_0, so the remaining zero is easily computed. For instance, for our curve (9), we compute

$$\begin{aligned}
\alpha &= \frac{937766474523}{467 \cdot 15365639}, \\
\beta &= -\frac{2096569897386251210893331}{2 \cdot 15365639^3}; \\
a &= -\frac{2096569897386251210893331}{2 \cdot 15365639^3}, \\
b &= \frac{334937219677623362815466}{15365639^3}, \\
c &= \frac{1076124066222818157529571}{2 \cdot 15365639^3},
\end{aligned}$$

from which we find that $-Q$ has X-coordinate

$$\frac{1274739344939668202218656423135632 83}{1297595594858724312829527106686985 69},$$

and eventually recover our second solution

$$A = 14399657106489544922685067718331752678502014266153004422182923363366633,$$
$$B = 44172646989945384969435974897549528458546724971790478988641242093469 20,$$
$$C = 90339645774825323880594824293984572910049479250057430281474657326458 80,$$
$$D = 91617818300354368478324523982672660382270029622572436620703708887221 69$$

to $A^4 + B^4 + C^4 = D^4$ in coprime integers A, B, C, D. Likewise, we can compute $n \cdot Q$ for $n = 2, \ldots, 6$ to verify that Q is not a torsion point of (9); fortunately, this requires only the coordinates of these points as single-precision real numbers, since the corresponding integer solutions to $A^4 + B^4 + C^4 = D^4$ are too huge to be profitably displayed even in a *Math. Comp.* article!

While we now have infinitely many rational points on the surface (5), they all lie on the same curve. We proceed to show how to produce rational points off that curve, and indeed enough rational points to comprise a dense subset of the real locus of (5). It will be convenient to henceforth drop the requirement that u be of the form $2m/n$; instead of choosing between u and $2/u$, we may choose the sign in (6c), and will use the minus sign (the reason for this choice will appear later). Our curve (9) then corresponds to $u = 2/(-16/5) = -5/8$. We now combine two observations: we have already seen that any rational solution of (5) necessarily comes from a rational

$$u = \frac{-1 + (r+s)^2 - t^2}{r^2 + rs + s^2 + r + s} \tag{11}$$

in the parametrization (6), and we have implicitly used the 48 linear symmetries of the surface (5) generated by replacing each of r, s, t by their negatives and permuting them. Of these, only four (generated by $(r, s, t) \mapsto (r, s, -t)$ and $(r, s, t) \mapsto (s, r, t)$) preserve the value of u in (11). This leaves us with $48/4 = 12$ different curves for each of our solutions to (5), only one of which corresponds to $u = -5/8$. Thus, from each of our infinitude of solutions to (5) with $u = -5/8$ we obtain a few new values of u for which we know a rational solution to (6), and for each such u we can expect to find infinitely more as in our proof of the above Proposition. With a little more work we find that these solutions suffice to prove:

THEOREM. *The rational solutions of* (5) *are dense in the set of real solutions.*

Remark. In particular, it follows that there are infinitely many admissible u, so infinitely many pairs (m, n) of relatively prime integers with n odd and $R(2m^2 - \kappa mn + n^2)$ a product of primes congruent to 1 mod 8 for $\kappa = -2, 0, 2, 4$; and in fact $u = 2m/n$ can be taken arbitrarily close to any real number outside $(2 - \sqrt{2}, 2 + \sqrt{2})$. This result is hardly surprising, for on probabilistic grounds one expects the number of admissible (m, n) with $|m|, |n| < N$ to be asymptotically proportional to $(N/\log N)^2$ for large N, but I cannot see how to simply prove the infinitude of admissible u, let alone obtain their asymptotic distribution.

Proof. First note that, for any real solution (r, s, t) of (5) with $rst \neq 0$, at least one of the twelve possible values of u is negative or infinite: by replacing r or s by their negatives if necessary, we can make $r > 0$ and $s < 0$ with $r + s \geqslant 0$, when the denominator

$$r^2 + rs + s^2 + r + s = r^2 + (1 + s)(r + s)$$

in (11) is positive and the numerator

$$-1 + (r+s)^2 - t^2 < -t^2$$

is negative (this is why we chose the minus sign in (6c)!). Next we show that, by replacing s by $-s$ in the family of rational solutions of (5) described in our proof of the Proposition, we can obtain values of u arbitrarily close to any given negative real number. Indeed, the real locus of (9) is connected, because the right-hand side is positive only for X between its two real roots, $-.3828\ldots$ and $.9987\ldots$, so its infinite rational subgroup is dense; and the new value

$$-\frac{7480X^2 - 18500X + 6068}{357X^2 + 11286X + 1605}$$

of u ranges from $-\infty$ at $X = -\frac{1}{7}+$ to a positive value at $X = \frac{2}{5}$, and so attains every negative value for some real solution of (9). Given a real point on (5), we thus obtain from the rational points $P_m = m \cdot Q$ on (9) points $Q'(P_m)$ on elliptic curves $E'(P_m)$ that pass arbitrarily close to it. It remains to show that only all but a finite number of these have infinite order and that the real loci of these curves are connected. The former is easy: by Mazur's Theorem there are only eleven possible orders $n = 1, 2, \ldots, 10, 12$ for a rational torsion point of an elliptic curve over $\mathbf{Q}$; for each of these, either $n \cdot Q_m = 0$ on E_m for finitely many m, or $n \cdot Q(P) = 0$ on $E(P)$ identically for all P in (9), rational or not. Now for $n = 1$, the equality $n \cdot Q(P) = 0$ means $t = 0$ which certainly does not hold identically; however, it does hold for some (complex) P, and for P' sufficiently near P, the point $Q(P)$ is too close to zero to be an n-torsion point for any $n \leqslant 12$. Finally, to verify that the real locus of (6) is connected, we need only check that the values of the right-hand side of (6b) at the two (necessarily real) roots of the right-hand side of (6c) are of opposite sign, or equivalently that their product,

$$-\left[\frac{u^2+2}{4(u^2-2)}\right]^2 (7u^4 - 48u^3 + 100u^2 - 96u + 48),$$

is negative; but that is clearly true for all $u < 0$. □

Postscript. While our first counterexample

$$(A, B, C; D) = (2682440, 15365639, 18796760; 20615673)$$

to Euler's conjecture still seems beyond the range of reasonable exhaustive computer search, there remained the possibility that smaller solutions may be found by such a search. Shortly after hearing of the first solution, Roger Frye of Thinking Machines Corporation asked whether it was minimal; I did not know, but suggested how one might exhaustively search for smaller solutions: eliminating common factors and permuting A, B, C if necessary, we may take D odd and not divisible by 5, and $C < D$ such that $D^4 - C^4$ is divisible by 625 and satisfies several other congruence and divisibility properties, and for each such D and C look for a representation of $D^4 - C^4$ as $A^4 + B^4$ with A, B divisible by 5. Frye translated this into a computer program and ran it on various Connection Machines for about 100 hours to find the minimal counterexample to Euler's conjecture:

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

He continued the search and found that this solution is unique in the range $D < 10^6$. This solution appears on the parametrization (6) with $(m, n) = (20, -9)$. We include Frye's result with his permission.

Department of Mathematics
Harvard University
Cambridge, Massachusetts 02138

1. A. BREMNER, personal communication, Aug. 1987.
2. B. J. BIRCH & W. KUYK, Editors, *Modular Functions on One Variable* IV, Lecture Notes in Math., vol. 476, Springer-Verlag, New York, 1975.
3. V. A. DEMJANENKO, "L. Euler's conjecture," *Acta Arith.*, v. 25, 1973–74, pp. 127–135. (Russian)
4. L. E. DICKSON, *History of the Theory of Numbers*, Vol. II: *Diophantine Analysis*, G. E. Stechert & Co., New York, 1934.
5. R. K. GUY, *Unsolved Problems in Number Theory*, Springer-Verlag, New York, 1981.
6. K. IRELAND & M. ROSEN, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1982.
7. L. J. LANDER & T. R. PARKIN, "Counterexamples to Euler's conjecture on sums of like powers," *Bull. Amer. Math. Soc.*, v. 72, 1966, p. 1079.
8. B. MAZUR, "Rational isogenies of prime degree," *Invent. Math.*, v. 44, 1978, pp. 129–162.
9. J. SILVERMAN, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
10. D. ZAGIER, "On the equation $w^4 + x^4 + y^4 = z^4$," unpublished note, 1987.