ON THE EQUATION $a(a+d)(a+2d)(a+3d) = x^2$

Tamás Erdélyi

Finding all three-term arithmetic progressions of squares is easy. We are led to the equation $a^2+c^2=2b^2$, which is equivalent to $(a+c)^2+(a-c)^2=(2b)^2$, so the family of all three-term arithmetic progressions of squares can be given by using the known formula for the Pythagorean triples [4, p. 396].

In [3, p. 199] Erdős and Surányi remark that Euler proved that four squares cannot make an arithmetic progression with positive difference. They also mention that it can also be proved that the equation $a(a+d)(a+2d)(a+3d)=x^2$ cannot be solved in positive integers (which obviously implies Euler's result). I was not able to get a reference for either of these results. After communicating with a few experts in number theory, I learned that the stronger result can be obtained from some known results on elliptic curves. For example, an expert gave me the following outline: If $y^2=a(a+d)(a+2d)(a+3d)$, then dividing both sides by a^4 and setting $y'=y/a^2$ and $x'=d/a$ yields ${y'}^2=(1+x')(1+2x')(1+3x')$, a nice elliptic curve. We can rewrite this as ${y'}^2=6(x'+1)(x'+1/2)(x'+1/3)$. If we multiply both sides by 6^2 and set $u=6y'$ and $v=6x'$, we get $u^2=(v+2)(v+3)(v+6)$. Finally, if we replace v by $v-4$, we get $u^2=(v-1)(v^2-4)$, which is curve number 24B of the Antwerp tables [1]. There or from John Cremona' tables [2] we learn that it has rank 0. Reducing mod 5 and mod 7, we see that the only torsion points are the points of order 2 (the conductor is 24) and we can deduce that the original equation has only trivial rational solutions.

This argument is comprehensible only to specialists in elliptic curves and is far from being self-contained. The purpose of this note is to present a totally elementary proof of the fact that the equation $a(a+d)(a+2d)(a+3d)=x^2$ cannot be solved in positive integers. The method of proof is an infinite descent with respect to $(a+d)(a+2d)$. This is a proof that Fermat could have found, but there is no trace of this in the literature. The canonical example that textbooks present as an application of the method of infinite descent is Fermat's proof of the fact that $x^4+y^4=z^2$ is not solvable in positive integers. In fact, it is hard to find non-trivial applications of infinite descent; the current proof is one.

Theorem. *The equation $a(a+d)(a+2d)(a+3d)=x^2$ cannot be solved in positive integers.*

Proof. Assume that (a,d,x) satisfies $a(a+d)(a+2d)(a+3d)=x^2$ for some positive integers for which $(a+d)(a+2d)$ is minimal. We show that there exists a triple (A,D,X) of positive integers for which $A(A+D)(A+2D)(A+3D)=X^2$ and

Typeset by $\mathcal{AMS}$-TEX

$(A+D)(A+2D) < (a+d)(a+2d)$, which implies that $a(a+d)(a+2d)(a+3d) = x^2$ cannot be solved in positive integers.

We may assume that a and d are relative primes, otherwise we may divide by $(a;d)^4$, where, and in what follows, $(m;n)$ denotes the greatest common divisor of the nonnegative integers m and n. Observe that $a(a+d)(a+2d)(a+3d) = x^2$ can be written as

$$(a^2 + 3ad + d^2)^2 = x^2 + d^4\,,$$

so by the well-known formula for the Pythagorean triples [4, p. 396] we have one of the following two cases.

Case 1. $a^2 + 3ad + d^2 = u^2 + v^2$; $\quad d^2 = 2uv$; $\quad u$ and v are positive integers, $(u;v) = 1$, and uv is even.

Case 2. $a^2 + 3ad + d^2 = u^2 + v^2$; $\quad d^2 = u^2 - v^2$; $\quad u$ and v are positive integers, $(u;v) = 1$, and uv is even.

First we study Case 1. Since $(2u;v) = 1$, we have $2u = (2u_1)^2$ and $v = v_1^2$ with some positive integers u_1 and v_1. These lead to

$$a^2 + 3ad + d^2 = u^2 + v^2 = 4u_1^4 + v_1^4 \qquad \text{and} \qquad d = 2u_1v_1\,.$$

Hence the discriminant of the quadratic equation

$$f(a) = a^2 + 6u_1v_1a + 4u_1^2v_1^2 - 4u_1^4 - v_1^4 = 0$$

is a square, so

$$36u_1^2v_1^2 - 16u_1^2v_1^2 + 16u_1^4 + 4v_1^4 = y^2\,,$$

that is

$$4u_1^4 + v_1^4 + 5u_1^2v_1^2 = y_1^2$$

with some positive integers y and $y_1 := y/2$. We conclude

$$(u_1^2 + v_1^2)(4u_1^2 + v_1^2) = y_1^2\,. \tag{1}$$

Observe that

$$\big((u_1^2 + v_1^2);\,(4u_1^2 + v_1^2)\big) = 1\,. \tag{2}$$

Indeed, if $q \mid u_1^2 + v_1^2$ and $q \mid 4u_1^2 + v_1^2$, then $q \mid 3u_1^2$ and $q \mid 3v_1^2$. As $(u_1;v_1) = 1$, we have $q = 1$ or $q = 3$. However, $q \mid u_1^2 + v_1^2$ implies $q \neq 3$, otherwise $3 \mid u_1$ and $3 \mid v_1$, which is impossible. Hence $q = 1$, indeed. Now (1) and (2) imply that

$$u_1^2 + v_1^2 = e^2 \quad \text{and} \quad (2u_1)^2 + v_1^2 = f^2$$

with some positive integers e and f. Using the formula for the Pythagorean triples [4, p. 396] again, and using also that v_1 is odd and $(u_1;v_1) = 1$, we obtain

$$u_1 = 2u_2v_2 \quad \text{and} \quad v_1 = u_2^2 - v_2^2$$

and

$$2u_1 = 2u_3v_3 \quad \text{and} \quad v_1 = u_3^2 - v_3^2$$

with some positive integers u_3 and v_3. That is,

$$u_3v_3 = 2u_2v_2 \quad \text{and} \quad u_3^2 - v_3^2 = u_2^2 - v_2^2\,,$$

so

$$\left(u_3^2 - v_3^2\right)^2 + u_3^2v_3^2 = \left(u_2^2 - v_2^2\right)^2 + 4u_2^2v_2^2 = \left(u_2^2 + v_2^2\right)^2\,. \tag{3}$$

It is easy to see that the solutions of the equation

$$x^2 + y^2 - xy = z^2 \tag{4}$$

in positive integers can be expressed by the formulae

$$x = \tfrac{1}{3}tb_1(2a_1 - b_1) \quad \text{and} \quad y = \tfrac{1}{3}ta_1(2b_1 - a_1)\,, \tag{5}$$

where a_1 and b_1 are positive integers. This can be obtained by rewriting (4) as

$$z^2 - (x - y/2)^2 = 3(y/2)^2$$

and modifying the proof of the well-known formula giving all the Pythagorean triples [4, p. 396]. From (3) and (5) we obtain

$$\frac{9}{t^2}u_3^2v_3^2 = a_1b_1(2a_1 - b_1)(2b_1 - a_1) = a_2(a_2 + b_2)(a_2 + 2b_2)(a_2 + 3b_2)\,,$$

where $a_2 = 2a_1 - b_1$ and $b_2 = b_1 - a_1$. Observe that $b_2 \neq 0$, otherwise $a_1 = b_1$, that is $x = y$, $u_3 = v_3$, $v_1 = 0$, and $d^2 = 0$. Also,

$$\begin{aligned}(a_2 + b_2)(a_2 + 2b_2) &< \tfrac{1}{2}a_2(a_2 + b_2)(a_2 + 2b_2)(a_2 + 3b_2) \\ &= \frac{9}{2t^2}u_3^2v_3^2 = \frac{9}{2t^2}u_1^2 = \frac{9}{8t^2}4u_1^2 \leq \frac{9}{8t^2}4u_1^2v_1^2 \\ &\leq \frac{9}{8}4u_1^2v_1^2 = \frac{9}{8}d^2 < 2d^2 < a^2 + 3ad + 2d^2 = (a + d)(a + 2d)\,.\end{aligned}$$

By this the proof is finished in Case 1.

Now we study Case 2, where we have

$$a^2 + 3ad + d^2 = u^2 + v^2 = \tfrac{1}{2}[(u + v)^2 + (u - v)^2] \tag{6}$$

and

$$d^2 = u^2 - v^2 = (u + v)(u - v)\,. \tag{7}$$

As $(u; v) = 1$ and uv is even, we have $(u + v; u - v) = 1$. This, together with $d^2 = (u + v)(u - v)$, gives

$$u + v = x_1^2 \quad \text{and} \quad u - v = x_2^2 \tag{8}$$

with positive integers x_1 and x_2. Also, $d = x_1x_2$. Combining (8) with (6) and (7) shows that the discriminant of the quadratic equation

$$f(a) = a^2 + 3x_1x_2a + x_1^2x_2^2 - \tfrac{1}{2}x_1^4 - \tfrac{1}{2}x_2^4 = 0$$

is a square, so

$$9x_1^2x_2^2 - 4x_1^2x_2^2 + 2x_1^4 + 2x_2^4 = y^2\,,$$

that is,

$$(2x_1^2 + x_2^2)(2x_2^2 + x_1^2) = y^2 \tag{9}$$

with a positive integer y. It is impossible that both $3 \mid x_1$ and $3 \mid x_2$, since $(x_1; x_2) = 1$. It is also impossible that both $3 \mid x_1$ and $3 \nmid x_2$ or both $3 \mid x_2$ and $3 \nmid x_1$ hold, since in these cases

$$(2x_1^2 + x_2^2)(2x_2^2 + x_1^2) \equiv 2 \pmod 3$$

which contradicts (9). We conclude that $3 \nmid x_1$ and $3 \nmid x_2$, hence

$$3 \mid 2x_1^2 + x_2^2 \qquad \text{and} \qquad 3 \mid 2x_2^2 + x_1^2\,.$$

We conclude that

$$x_2^2 \cdot \frac{2x_2^2 + x_1^2}{3} \cdot \frac{2x_1^2 + x_2^2}{3} \cdot x_1^2 = x_1^2x_2^2y^2 =: y_1^2\,,$$

that is,

$$a_2(a_2 + b_2)(a_2 + 2b_2)(a_2 + 3b_2) = y_1^2$$

with a positive integer y_1, where $a_2 := x_2^2$ and $b_2 := \frac{1}{3}(x_1^2 - x_2^2)$. Here $b_2 \neq 0$ otherwise $x_1 = x_2$, that is $u + v = u - v$, $v = 0$, $a^2 + 3ad + d^2 = d^2$, $a^2 + 3ad = 0$, and $a = d = 0$, which contradicts our assumption. Also

$$\begin{aligned}(a_2 + b_2)(a_2 + 2b_2) &= \frac{1}{9}(2x_1^4 + 2x_2^4 + 5x_1^2x_2^2)\\ &< \frac{1}{9}(4(a^2 + 3ad + d^2) + 5d^2) < \frac{1}{9}(9(a^2 + 3ad + d^2))\\ &= a^2 + 3ad + d^2 < (a + d)(a + 2d)\,.\end{aligned}$$

By this the proof is finished in Case 2 as well. □

References

1. Antwerp IV, *Lecture Notes in Mathematics* **476**, Springer-Verlag, New York, 1975.

2. J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, Cambridge, 1992.

3. P. Erdős and J. Surányi, *Válogatott Fejezetek a Számelméletből (Selected Topics from the Theory of Numbers)*, Tankönyvkiadó, Budapest, 1960. Second, revised edition: Polygon, Szeged, 1996.

4. K. H. Rosen, *Elementary Number Theory and Its Applications*, Addison-Wesley Publishing Company, Second Edition, New York, 1988.

Texas A&M University, College Station, Texas 77843

E-mail address: terdelyi@math.tamu.edu