Florian Luca; László Szalay

Congruent numbers with higher exponents

Acta Mathematica Universitatis Ostraviensis, Vol. 14 (2006), No. 1, 49--55

Persistent URL: http://dml.cz/dmlcz/137483

Congruent numbers with higher exponents

Florian Luca[1] *and László Szalay*[2]

Abstract. This paper investigates the system of equations

$$x^2 + ay^m = z_1^2, \qquad x^2 - ay^m = z_2^2$$

in positive integers x, y, z_1, z_2, where a and m are positive integers with $m \geq 3$. In case of $m = 2$ we would obtain the classical problem of congruent numbers. We provide a procedure to solve the simultaneous equations above for a class of the coefficient a with the condition $\gcd(x, z_1) = \gcd(x, z_2) = \gcd(z_1, z_2) = 1$. Further, under same condition, we even prove a finiteness theorem for arbitrary nonzero a.

1. Introduction

A natural number a is called congruent if the system of equations

$$x^2 + ay^2 = z_1^2, \tag{1}$$
$$x^2 - ay^2 = z_2^2 \tag{2}$$

is solvable in positive integers x, y, z_1, z_2. The history of congruent numbers dates back to the tenth century when an anonymous Arab manuscript posed the following problem. If c is an integer, find a square x^2 such that $x^2 \pm c$ both are squares. Since then a lot of mathematicians, among others Fibonacci, Fermat, Euler, investigated the problem of congruent numbers. For more details, see Dickson [4].

It was showed by Roberts [8] that if $x^2 \pm ay^2 = \square$, then ay^2 is of the form $D\alpha\beta(\alpha - \beta)(\alpha + \beta)$, where $D = 1$ or $D = 4$ depending on the parity of α and β. Likely, this result had already been known before. Our present work also uses a similar type of argument. In the paper [1], Alter, Curtz and Kubota proposed the following conjecture.

Conjecture 1. *If* $a \equiv 5,\ 6$ *or* $7 \pmod 8$*, then* a *is congruent number.*

Received: January 20, 2006.

1991 *Mathematics Subject Classification:* 11D09, 11D41.

Key words and phrases: congruent numbers, quadratic equations, higher degree equations.

[1] Research supported by grant SEP-CONACyT 46755 and a Guggenheim Fellowship.

[2] Research supported by the Hungarian National Foundation for Scientific Research Grant No. T 048954 MAT and by the Eötvös Scholarship of Hungary.

Tunnell [9], applied the theory of formal power series and modular forms to gain conditions for congruent and noncongruent numbers. His work is an important contribution to understanding their nature. Here, we look at the following question.

Question 1. *If a is a positive integer, what can one say about the positive integer solutions (x, y, z_1, z_2) of the system*

$$\begin{aligned} x^2 + ay^m &= z_1^2, & (3)\\ x^2 - ay^m &= z_2^2, & (4) \end{aligned}$$

where $m \geq 3$ is a fixed integer?

A *primitive solution* of the system of equations (3) and (4) will be just a solution (x, y, z_1, z_2) in positive integers such that $\gcd(x, z_1) = \gcd(x, z_2) = \gcd(z_1, z_2) = 1$. We start with the following result.

Theorem 1. *Given any integers $a \neq 0$ and $m \geq 3$, the system of equations (3) and (4) has only finitely many primitive positive integer solutions (x, y, z_1, z_2).*

We now address the issue of determining all such finitely many primitive solutions to the system of equations (3) and (4) once a is given. While we are unable to determine all such solutions in general, we do so for certain values of the parameter a, namely when $a = 2^u \cdot p^v$ with nonnegative integers u and v and an odd prime p. Our algorithm to determine all such solutions mainly relies on results of Ribet [7], and Darmon and Merel [3], which allow us to find all the integer solutions of the Fermat-type Diophantine equations $X^n + 2^\gamma Y^n = Z^n$. We use the method to find all the primitive solutions of the system of equations (3) and (4) for $a = 3$. We have the following result.

Theorem 2. *Let the pairwise relatively prime positive integers x, z_1 and z_2 satisfy the equations $x^2 + 3y^3 = z_1^2$ and $x^2 - 3y^3 = z_2^2$ for some positive integer y. Then, $(x, y, z_1, z_2) = (5, 2, 7, 1)$.*

2. The Finiteness Theorem

Here, we prove Theorem 1. Multiplying equations (3) and (4), we get the equation

$$x^4 - a^2 y^{2m} = z^2,$$

where $z = z_1 z_2$. Since $1/2 + 1/4 + 1/2m < 1$ for any fixed $m \geq 3$, the fact that the above equation has only finitely many integer solutions (x, y, z) follows immediately from a result of Darmon and Granville from [2], which asserts that if A, B and C are given nonzero integers and ℓ, m and n and given positive integers with $1/\ell + 1/m + 1/n < 1$, then the equation

$$Ax^\ell + By^m = Cz^n$$

has only finitely many integer solutions (x, y, z) with $\gcd(Ax, By) = 1$.

3. Preparation for the Proof of Theorem 2

In this section, we establish the basic equations which have a crucial role in our arguments for the proof of Theorem 2.

We start by recalling a useful result of Legendre dealing with the integer solutions (x, y, z) of the Diophantine equation

$$ax^2 + by^2 + cz^2 = 0. \tag{5}$$

Here a, b and c are pairwise coprime square-free integers with $a > 0$, $b < 0$ and $c < 0$. Under the presentation below, Lemma 1 appears [6].

Lemma 1. *Assume that (x_0, y_0, z_0) is an integer solution of equation (5) with $z_0 \neq 0$. Then, all integer solutions (x, y, z) with $z \neq 0$ of equation (5) are of the form*

$$\begin{aligned} x &= \pm\frac{D}{d}\left(-ax_0s^2 - 2by_0rs + bx_0r^2\right), \\ y &= \pm\frac{D}{d}\left(ay_0s^2 - 2ax_0rs - by_0r^2\right), \\ z &= \pm\frac{D}{d}\left(az_0s^2 + bz_0r^2\right), \end{aligned}$$

where $s > 0$ and r are coprime integers, D is a nonzero integer, and the positive integer d divides $2a^2bcz_0^3$.

Furthermore, the number D above is the greatest common divisor of any two numbers from the set $\{x, y, z\}$.

Let c denote a positive integer. Consider, like in the Arab manuscript, the system of two Diophantine's equations

$$\begin{aligned} x^2 + c &= z_1^2, \quad (6) \\ x^2 - c &= z_2^2, \quad (7) \end{aligned}$$

in positive integers x, z_1 and z_2. Equations (6) and (7) lead to

$$2x^2 - z_1^2 - z_2^2 = 0. \tag{8}$$

Take $(x_0, z_{10}, z_{20}) = (1, 1, 1)$ as a basic solution of equation (8). Then, by Lemma 1, it is possible to write any solution of equation (8) in the form

$$x = \pm\frac{D}{d}(2s^2 - 2sr + r^2)\,, \quad z_1 = \pm\frac{D}{d}(2s^2 - 4sr + r^2)\,, \quad z_2 = \pm\frac{D}{d}(2s^2 - r^2)\,, \tag{9}$$

where $s > 0$ and r are coprime integers, D is an arbitrary positive integer, and the positive integer d divides 8. It follows easily, from the proof of Lemma 1 in [6], that d does not necessarily run through all the divisors of 8, but only through the divisors of 8 of the form

$$d = \gcd(2s^2 - 2sr + r^2, 2s^2 - r^2) = \gcd(2s^2 - 4sr + r^2, 2s^2 - r^2). \tag{10}$$

Thus, we must analyze (10) in order to reduce the number of possibilities for d. If r is odd, then

$$d = \gcd(-2sr + 2r^2, 2s^2 - r^2) = \gcd(-s + r, 2s^2 - r) = \gcd(-s + r, r^2) = 1.$$

If $r = 2r_0$ is even, then s is necessarily odd, and

$$\begin{aligned} d &= 2\gcd(-2sr_0 + 2r_0^2, s^2 - 2r_0^2) = 2\gcd(-s + r_0, s^2 - 2r_0^2) = \\ &= 2\gcd(-s + r_0, -r_0^2) = 2. \end{aligned}$$

Thus, $d = 1$ or 2 depending on the parity of r.

Using formulas (9), together with the fact that $2c = z_1^2 - z_2^2$, we get $2c = D^2/d^2(-16s^3r + 24s^2r^2 - 8sr^3)$, and we so have

$$\frac{cd^2}{4D^2} = s(-r)(s-r)(2s-r). \tag{11}$$

The right hand side of the above equation is a product of four coprime numbers, except when $\gcd(r, 2s - r) = 2$. This happens only if r is even. Further, the right hand side of the above equation is the product of three consecutive terms of an arithmetic progression and the difference of the progression.

Hence, the system consisting of equations (6) and (7) is solvable for some c, if and only if either $c = 4D^2s(-r)(s - r)(2s - r)$ (when r is odd), or $c = D^2s(-r)(s - r)(2s - r)$ (when r is even).

The fact that the unknowns x, z_1 and z_2 are positive leads to the following conditions. The left hand side of equation (11) is positive therefore either $r < 0$, or $s < r < 2s$. Further, since $2s^2 - 2sr + r^2$ is a positive definite quadratic form, we see that $x = D/d(2s^2 - 2sr + r^2)$. If $r < 0$, then $2s^2 - 4sr + r^2 > 0$ for all possible pairs (s, r), so $z_1 = D/d(2s^2 - 4sr + r^2)$. On the other hand, if $s < r < 2s$, then $z_1 = D/d(-2s^2 + 4sr - r^2)$. Finally, if $|r| < \sqrt{2}s$, then $z_2 = D/d(2s^2 - r^2)$, and otherwise $z_2 = D/d(-2s^2 + r^2)$.

We conclude this section by providing two examples, the first one leading to the solution appearing in Theorem 2.

1. Let $s = 2$, $r = 3$, $D = 1$. Since r is odd, we get that $c = 4s(-r)(s-r)(2s-r) = 24 = 3 \cdot 2^3$. Further, $x = 5$, $z_1 = 7$ and $z_2 = 1$. Consequently, $(x, y, z_1, z_2) = (5, 2, 7, 1)$ gives a solution of the system of equations

$$x^2 + 3y^3 = z_1^2, \tag{12}$$

$$x^2 - 3y^3 = z_2^2. \tag{13}$$

2. It is easy to see that for any positive integer $m \geq 3$, there exists a positive integer a such that

$$x^2 + ay^m = z_1^2, \tag{14}$$

$$x^2 - ay^m = z_2^2. \tag{15}$$

Indeed, suppose that m is fixed. Put $r = -1$ and $s = 2^b$ for some positive integer b. Then $d = 1$, and

$$c = 4 \cdot 2^b(2^b + 1)(2^{b+1} + 1) = 2^{b+2} \cdot (2^b + 1)(2^{b+1} + 1).$$

Taking $b = m - 2$, we see that the choice $a = (2^b + 1)(2^{b+1} + 1)$ is suitable for the system of equations (14) and (15).

4. The Structure of the Primitive Solutions of $x^2 \pm 2^u p^v y^m = z_i^2$

In this section, we give a procedure to determine all the primitive solutions of the equation $x^2 \pm 2^u p^v y^m = z_i^2$ in positive integers $x,\ y,\ z_1,\ z_2$, where p is an odd prime, u and v are nonnegative integers, and $m \geq 3$. Without loss of generality, we may assume that the exponents u and v are less then m. Thus, in the sequel, we suppose that $0 \leq u,\ v < m$. By the results from Section 3, we have $D = 1$, and so we must solve the equations

$$2^u p^v y^m = s(-r)(s-r)(2s-r), \quad r \text{ even}, \tag{16}$$

and

$$2^u p^v y^m = 4s(-r)(s-r)(2s-r), \quad r \text{ odd}, \tag{17}$$

with $y > 0$, $\gcd(s, r) = 1$ and $s > 0$.

Consider now equation (16). Let $r = 2r_0$. Thus, s is odd, and either $r_0 < 0$ or $0 < s/2 < r_0 < s$. Assume first that $u = 0$ or 1. In these cases, y must be even. Put $y = 2y_0$. We then have

$$2^{m-2+u} p^v y_0^m = r_0(-s)(r_0 - s)(2r_0 - s). \tag{18}$$

If $u \geq 2$, we then simplify both sides of equation (16) by a factor of 4 and obtain

$$2^{u-2} p^v y^m = r_0(-s)(r_0 - s)(2r_0 - s). \tag{19}$$

Suppose now that r is odd. If $u \in \{0, 1\}$ in equation (17), then $y = 2y_0$ and we get

$$2^{m-2+u} p^v y_0^m = s(-r)(s-r)(2s-r), \tag{20}$$

while in case when $u \geq 2$, we get

$$2^{u-2} p^v y^m = s(-r)(s-r)(2s-r). \tag{21}$$

All the above four equations are of the type

$$2^U p^v Y^m = S(-R)(S-R)(2S-R), \tag{22}$$

where $U \geq 1$, and either $Y = y$ or $Y = y_0$. Further, the four factors on the right hand side of the above equation are coprime any two.

There are two possibilities for the unknowns S and R. If the equation (22) has been derived from (16), then either $S,\ -R,\ S-R,\ 2S-R$ are all are negative, or $-R < 0$ and $S - R < 0$, while $S > 0$ and $2S - R > 0$. Similarly, if the source of equation (22) is (17), then either all the four factors $S,\ -R,\ S-R,\ 2S-R$ are positive, or $-R < 0$ and $S - R < 0$, while $S > 0$ and $2S - R > 0$.

Since the factors on the right hand side of equation (22) are coprime, we get $S = \varepsilon_1 y_1^m$, $-R = \varepsilon_2 y_2^m$, $S - R = \varepsilon_3 y_3^m$, and $2S - R = \varepsilon_4 y_4^m$, where ε_i are positive integers for $i = 1, \ldots, 4$ with $\prod_{i=1}^4 \varepsilon_i = 2^U p^v$.

Eliminating the numbers R and S from the above relations, we get

$$\begin{aligned} \varepsilon_2 y_2^m + \varepsilon_4 y_4^m &= 2\varepsilon_3 y_3^m, && (23)\\ \varepsilon_1 y_1^m + \varepsilon_3 y_3^m &= \varepsilon_4 y_4^m, && (24)\\ 2\varepsilon_1 y_1^m + \varepsilon_2 y_2^m &= \varepsilon_4 y_4^m, && (25)\\ \varepsilon_1 y_1^m + \varepsilon_2 y_2^m &= \varepsilon_3 y_3^m. && (26) \end{aligned}$$

Since the factor p^v can only divide exactly one of ε_i's, we get that among the previous four equations there is one for which p^v does not divide any coefficient. In such an equation, all the three coefficients are powers of 2, and so the solutions can be determined as an easy application of the results of Ribet [7] and Darmon and Merel [3].

All the 16 possibilities for the coefficients ε_i for $i = 1, \dots, 4$ are enumerated in Table 1.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ε_1	2^Up^v	p^v	p^v	p^v	2^U	1	1	1	2^U	1	1	1	2^U	1	1	1
ε_2	1	2^U	1	1	p^v	2^Up^v	p^v	p^v	1	2^U	1	1	1	2^U	1	1
ε_3	1	1	2^U	1	1	1	2^U	1	p^v	p^v	2^Up^v	p^v	1	1	2^U	1
ε_4	1	1	1	2^U	1	1	1	2^U	1	1	1	2^U	p^v	p^v	p^v	2^Up^v

Table 1.

5. Example: Primitive Solutions of $x^2 \pm 3y^3 = z_i^2$

In this section, we prove Theorem 2. Thus, we must solve the equations

$$3y^3 = s(-r)(s-r)(2s-r), \quad r \text{ even}, \tag{27}$$

and

$$3y^3 = 4s(-r)(s-r)(2s-r), \quad r \text{ odd}, \tag{28}$$

where $y > 0$, $\gcd(s,r) = 1$ and $s > 0$. Since y has to be even in both cases, we put $y = 2y_0$, and in the first case we also let $r = 2r_0$. We have

$$6y_0^3 = r_0(-s)(r_0 - s)(2r_0 - s), \quad \text{where } r_0 < 0 \text{ or } 0 < s/2 < r_0 < s, \tag{29}$$

and

$$6y_0^3 = s(-r)(s-r)(2s-r), \quad \text{if } r < 0 \text{ or } 0 < s < r < 2s. \tag{30}$$

Using the notations of the previous section, we have $U = 1$, $p = 3$, $v = 1$, $m = 3$ and

$$6Y^3 = S(-R)(S-R)(2S-R), \tag{31}$$

with $S = \varepsilon_1 y_1^3$, $-R = \varepsilon_2 y_2^3$, $S - R = \varepsilon_3 y_3^3$, $2S - R = \varepsilon_4 y_4^3$, and $\prod_{i=1}^4 \varepsilon_i = 6$.

Clearly, if $y_i = 0$ for some i, as in all the cases except for the fifth, seventh and fifteenth columns of Table 1, then there is no additional solution of the equation we are considering.

Consider now the equation $2y_1^3 + y_3^3 = y_4^3$, which is a particular instance of equation (24) and the fifth column of Table 1. The only nonzero integer solutions of this equation are

$$(y_1, y_3, y_4) = (1, -1, 1), \ (-1, 1, -1).$$

The first solution gives $S = 2$, $R = 3$, and both instances (29) and (30) give $y = 2$, $x = 5$, $z_1 = 7$, $z_2 = 1$. The second solution $(-1, 1, -1)$ gives only negative values for s if d is either 1 or 2.

In the case of the seventh column of Table 1, equation (24) is $y_1^3 + 2y_3^3 = y_4^3$. Each one of its two possible solutions

$$(y_1, y_3, y_4) = (1, -1, -1) \text{ and } (-1, 1, 1)$$

induce the impossible result $y = -2$.

Finally, in the fifteenth case of Table 1, equation (26) becomes $y_1^3 + y_2^3 = 2y_3^3$, and none of its nonzero solutions

$$(y_1, y_2, y_3) = (1, 1, 1),\ (-1, -1, -1)$$

leads to any additional solution of the equation we are considering.

The proof of Theorem 2 is complete.

References

[1] Alter, R., Curtz, T. B. and Kubota, K. K, 'Remarks and results on congruent numbers', Proc. 3rd S. E. Conf. Combin. Graph Theory Comput., *Congr. Num.*, **6** (1972), 27-35.

[2] Darmon, H. and Granville, A., 'On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$', *Bull. London Math. Soc.*, **27** (1995), 513–543.

[3] Darmon, H. and Merel, L., 'Winding quotients and some variants of Fermat's Last Theorem', *J. reine angew. Math.*, **490** (1997), 81-100.

[4] Dickson, L. E., *History of the theory of numbers*, Vol. 2, Diophantine analysis, Washington, 1920, 459-472.

[5] Guy, R. K., *Unsolved Problems in Number Theory*, (D27, p. 306,) Third Edition, Springer, 2004.

[6] Luca, F. and Szalay, L., 'Consecutive binomial coefficients satisfying a quadratic relation', *Publ. Math. Debrecen*, to appear.

[7] Ribet, K., 'On the equation $a^p + 2^\alpha b^p + c^p = 0$', *Acta Arith.*, **79** (1997), 7-16.

[8] Robert, S., 'Note on a problem of Fibonacci's', *Proc. London Math. Soc.*, **11** (1879), 35-44.

[9] Tunnel, J. B., 'A classical Diophantine's problem and modular forms of weight 3/2', *Invent. Math.*, **72** (1983), 323-334.

Author(s) Address(es):
Florian Luca, Instituto de Matemáticas, Universidad Nacional Autonoma de México, C.P. 58180, Morelia, Michoacan, México

E-mail address: fluca@matmor.unam.mx

László Szalay, Institute of Mathematics, Statistics and Informatics, University of West Hungary, H-9400, Sopron, Erzsébet utca 9., Hungary

E-mail address: laszalay@ktk.nyme.hu