A Theorem of Fermat
on
Congruent Number Curves

Lorenz Halbeisen

Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland

lorenz.halbeisen@math.ethz.ch

Norbert Hungerbühler

Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland

norbert.hungerbuehler@math.ethz.ch

key-words: congruent numbers, Pythagorean triples

2010 Mathematics Subject Classification: **11G05** 11D25

Abstract

A positive integer A is called a *congruent number* if A is the area of a right-angled triangle with three rational sides. Equivalently, A is a *congruent number* if and only if the congruent number curve $y^2 = x^3 - A^2x$ has a rational point $(x, y) \in \mathbb{Q}^2$ with $y \neq 0$. Using a theorem of Fermat, we give an elementary proof for the fact that congruent number curves do not contain rational points of finite order.

1 Introduction

A positive integer A is called a **congruent number** if A is the area of a right-angled triangle with three rational sides. So, A is congruent if and only if there exists a rational Pythagorean tripel (a, b, c) (*i.e.*, $a, b, c \in \mathbb{Q}$, $a^2 + b^2 = c^2$, and $ab \neq 0$), such that $\frac{ab}{2} = A$. The sequence of integer congruent numbers starts with

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, \ldots$$

For example, $A = 7$ is a congruent number, witnessed by the rational Pythagorean triple

$$\Big(\frac{24}{5}, \frac{35}{12}, \frac{337}{60}\Big).$$

It is well-known that A is a congruent number if and only if the cubic curve

$$C_A: \; y^2 = x^3 - A^2x$$

has a rational point (x_0, y_0) with $y_0 \neq 0$. The cubic curve C_A is called a **congruent number curve**. This correspondence between rational points on congruent number curves and rational Pythagorean triples can be made explicit as follows: Let

$$C(\mathbb{Q}) := \{(x, y, A) \in \mathbb{Q} \times \mathbb{Q}^* \times \mathbb{Z}^* : y^2 = x^3 - A^2x\},$$

where $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}, \mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$, and

$$P(\mathbb{Q}) := \{(a,b,c,A) \in \mathbb{Q}^3 \times \mathbb{Z}^* : a^2 + b^2 = c^2 \textit{ and } ab = 2A\}.$$

Then, it is easy to check that

$$\begin{array}{rrcl} \psi : & P(\mathbb{Q}) & \to & C(\mathbb{Q}) \\ & (a,b,c,A) & \mapsto & \Big(\dfrac{A(b+c)}{a}, \dfrac{2A^2(b+c)}{a^2}, A\Big) \end{array} \tag{1}$$

is bijective and

$$\begin{array}{rrcl} \psi^{-1} : & C(\mathbb{Q}) & \to & P(\mathbb{Q}) \\ & (x,y,A) & \mapsto & \Big(\dfrac{2xA}{y}, \dfrac{x^2 - A^2}{y}, \dfrac{x^2 + A^2}{y}, A\Big). \end{array} \tag{2}$$

For positive integers A, a triple (a,b,c) of non-zero rational numbers is called a **rational Pythagorean A-triple** if $a^2 + b^2 = c^2$ and $A = \left|\frac{ab}{2}\right|$. Notice that if (a,b,c) is a rational Pythagorean A-triple, then A is a congruent number and $|a|, |b|, |c|$ are the lengths of the sides of a right-angled triangle with area A. Notice also that we allow a, b, c to be negative.

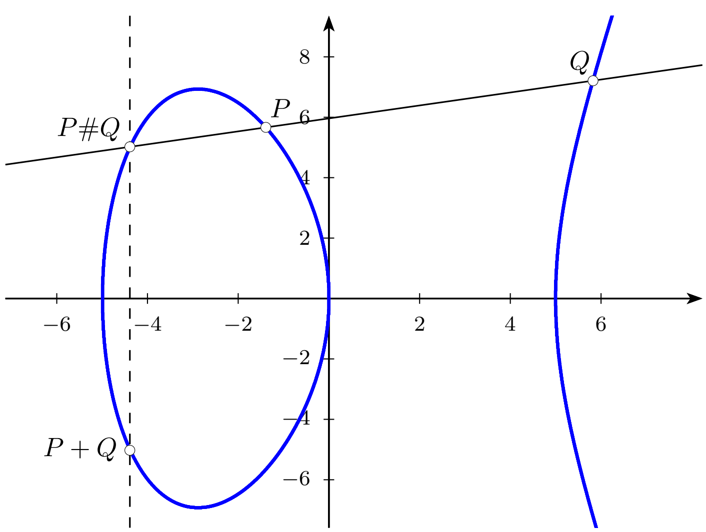
It is convenient to consider the curve C_A in the projective plane $\mathbb{R}P^2$, where the curve is given by

$$C_A : \; y^2 z = x^3 - A^2 x z^2.$$

On the points of C_A, one can define a commutative, binary, associative operation "+", where $\mathscr{O}$, the neutral element of the operation, is the projective point $(0,1,0)$ at infinity. More formally, if P and Q are two points on C_A, then let $P\#Q$ be the third intersection point of the line through P and Q with the curve C_A. If $P = Q$, the line through P and Q is replaced by the tangent in P. Then $P + Q$ is defined by stipulating

$$P + Q \; := \; \mathscr{O}\#(P\#Q),$$

where for a point R on C_A, $\mathscr{O}\#R$ is the point reflected across the x-axis. The following figure shows the congruent number curve C_A for $A = 5$, together with two points P and Q and their sum $P + Q$.



More formally, for two points $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ on a congruent number curve C_A, the point $P + Q = (x_2, y_2)$ is given by the following formulas:

- If $x_0 \neq x_1$, then

$$x_2 = \lambda^2 - x_0 - x_1, \qquad y_2 = \lambda(x_0 - x_2) - y_0,$$

  where

$$\lambda := \frac{y_1 - y_0}{x_1 - x_0}.$$

- If $P = Q$, *i.e.*, $x_0 = x_1$ and $y_0 = y_1$, then

$$x_2 = \lambda^2 - 2x_0, \qquad y_2 = 3x_0\lambda - \lambda^3 - y_0, \tag{3}$$

  where

$$\lambda := \frac{3x_0^2 - A^2}{2y_0}. \tag{4}$$

  Below we shall write $2 * P$ instead of $P + P$.

- If $x_0 = x_1$ and $y_0 = -y_1$, then $P + Q := \mathscr{O}$. In particular, $(0, 0) + (0, 0) = (A, 0) + (A, 0) = (-A, 0) + (-A, 0) = \mathscr{O}$.

- Finally, we define $\mathscr{O} + P := P$ and $P + \mathscr{O} := P$ for any point P, in particular, $\mathscr{O} + \mathscr{O} = \mathscr{O}$.

With the operation "+", $(C_A, +)$ is an abelian group with neutral element $\mathscr{O}$. Let $C_A(\mathbb{Q})$ be the set of rational points on C_A together with $\mathscr{O}$. It is easy to see that $\big(C_A(\mathbb{Q}), +\big)$. is a subgroup of $(C_A, +)$. Moreover, it is well known that the group $\big(C_A(\mathbb{Q}), +\big)$ is finitely generated. One can readily check that the three points $(0, 0)$ and $(\pm A, 0)$ are the only points on C_A of order 2, and one easily finds other points of finite order on C_A. But do we find also rational points of finite order on C_A? This question is answered by the following

THEOREM 1. *If A is a congruent number and (x_0, y_0) is a rational point on C_A with $y_0 \neq 0$, then the order of (x_0, y_0) is infinite. In particular, if there exists one rational Pythagorean A-triple, then there exist infinitely many such triples.*

The usual proofs of THEOREM 1 are quite involved. For example, Koblitz [4, Ch. I, § 9, Prop. 17] gives a proof using Dirichlet's theorem on primes in an arithmetic progression, and in Chahal [1, Thm. 3], a proof is given using the Lutz-Nagell theorem, which states that rational points of finite order are integral. However, both results, Dirichlet's theorem and the Lutz-Nagell theorem, are quite deep results, and the aim of this article is to provide a simple proof of THEOREM 1 which relies on an elementary theorem of Fermat.

2 A Theorem of Fermat

In [2], Fermat gives an algorithm to construct different right-angled triangles with three rational sides having the same area (see also Hungerbühler [3]). Moreover, Fermat claims that his algorithm yields infinitely many distinct such right-angled triangles. However, he did not provide a proof for this claim. In this section, we first present Fermat's algorithm and then we show that this algorithm delivers infinitely many pairwise distinct rational right-angled triangles of the same area.

FERMAT'S ALGORITHM 2. *Assume that A is a congruent number, and that (a_0, b_0, c_0) is a rational Pythagorean A-triple, i.e., $A = \left|\frac{a_0 b_0}{2}\right|$. Then*

$$a_1 := \frac{4c_0^2 a_0 b_0}{2c_0(a_0^2 - b_0^2)}, \quad b_1 := \frac{c_0^4 - 4a_0^2 b_0^2}{2c_0(a_0^2 - b_0^2)}, \quad c_1 := \frac{c_0^4 + 4a_0^2 b_0^2}{2c_0(a_0^2 - b_0^2)}, \tag{5}$$

is also a rational Pythagorean A-triple. Moreover, $a_0 b_0 = a_1 b_1$, i.e., if $(a_0, b_0, c_0, A) \in P(\mathbb{Q})$, then $(a_1, b_1, c_1, A) \in P(\mathbb{Q})$.

Proof. Let $m := c_0^2$, let $n := 2a_0 b_0$, and let

$$X := 2mn, \quad Y := m^2 - n^2, \quad Z := m^2 + n^2,$$

in other words,

$$X = 4c_0^2 a_0 b_0, \quad Y = c_0^4 - 4a_0^2 b_0^2, \quad Z = c_0^4 + 4a_0^2 b_0^2.$$

Then obviously, $X^2 + Y^2 = Z^2$, and since $a_0, b_0, c_0 \in \mathbb{Q}$, $\big(|X|, |Y|, |Z|\big)$ is a rational Pythagorean triple, where the area of the corresponding right-angled triangle is

$$\tilde{A} = \left|\frac{XY}{2}\right| = \left|2a_0 b_0 c_0^2 (c_0^4 - 4a_0^2 b_0^2)\right|.$$

Since $a_0^2 + b_0^2 = c_0^2$, we get $c_0^4 = (a_0^2 + b_0^2)^2 = a_0^4 + 2a_0^2 b_0^2 + b_0^4$ and therefore

$$c_0^4 - 4a_0^2 b_0^2 \;=\; a_0^4 - 2a_0^2 b_0^2 + b_0^4 \;=\; (a_0^2 - b_0^2)^2 > 0.$$

So, for

$$a_1 = \frac{X}{2c_0(a_0^2 - b_0^2)}, \quad b_1 = \frac{Y}{2c_0(a_0^2 - b_0^2)}, \quad c_1 = \frac{Z}{2c_0(a_0^2 - b_0^2)},$$

we have $a_1^2 + b_1^2 = c_1^2$ and

$$\frac{a_1 b_1}{2} \;=\; \frac{XY}{2 \cdot 4c_0^2 (a_0^2 - b_0^2)^2} \;=\; \frac{2a_0 b_0 c_0^2 (c_0^4 - 4a_0^2 b_0^2)}{4c_0^2 (a_0^2 - b_0^2)^2} \;=\; \frac{2a_0 b_0 c_0^2 (a_0^2 - b_0^2)^2}{4c_0^2 (a_0^2 - b_0^2)^2} \;=\; \frac{a_0 b_0}{2}.$$

q.e.d.

THEOREM 3. *Assume that A is a congruent number, that (a_0, b_0, c_0) is a rational Pythagorean A-triple, and for positive integers n, let (a_n, b_n, c_n) be the rational Pythagorean A-triple we obtain by* FERMAT'S ALGORITHM *from $(a_{n-1}, b_{n-1}, c_{n-1})$. Then for any distinct non-negative integers n, n', we have $|c_n| \neq |c_{n'}|$.*

Proof. Let n be an arbitrary but fixed non-negative integer. Since $A = \left|\frac{a_n b_n}{2}\right|$, we have $2A = |a_n b_n|$, and consequently

$$a_n^2 b_n^2 = 4A^2. \tag{6}$$

Furthermore, since $a_n^2 + b_n^2 = c_n^2$, we have

$$(a_n^2 + b_n^2)^2 = a_n^4 + 2a_n^2 b_n^2 + b_n^4 = a_n^4 + 8A^2 + b_n^4 = c_n^4,$$

and consequently we get

$$c_n^4 - 16A^2 = a_n^4 - 8A^2 + b_n^4 = a_n^4 - 2a_n^2 b_n^2 + b_n^4 = (a_n^2 - b_n^2)^2 > 0.$$

Therefore,

$$\sqrt{(a_n^2 - b_n^2)^2} = |a_n^2 - b_n^2| = \sqrt{c_n^4 - 16A^2},$$

and with (5) and (6) we finally have

$$|c_{n+1}| = \frac{c_n^4 + 16A^2}{2c_n\sqrt{c_n^4 - 16A^2}}\,.$$

Now, assume that $c_n = \frac{u}{v}$ where u and v are in lowest terms. We consider the following two cases:

u is odd: First, we write $v = 2^k \cdot \tilde{v}$, where $k \geq 0$ and $\tilde{v}$ is odd. In particular, $c_n = \frac{u}{2^k \cdot \tilde{v}}$. Since c_{n+1} is rational, $\sqrt{c_n^4 - 16A^2} \in \mathbb{Q}$. So,

$$\sqrt{c_n^4 - 16A^2} = \sqrt{\frac{u^4 - 16A^2 v^4}{v^4}} = \frac{\tilde{u}}{v^2}$$

for a positive odd integer $\tilde{u}$. Then

$$|c_{n+1}| = \frac{\frac{u^4 + 16A^2 v^4}{v^4}}{\frac{2u\tilde{u}}{v^3}} = \frac{\bar{u}}{2u\tilde{u}v} = \frac{\bar{u}}{2u\tilde{u}2^k\tilde{v}} = \frac{\bar{u}}{2^{k+1}u\tilde{u}\tilde{v}} = \frac{u'}{2^{k+1}\cdot v'}$$

where $\bar{u}, u', v'$ are odd integers and $\gcd(u', v') = 1$. This shows that

$$c_n = \frac{u}{2^k \cdot \tilde{v}} \quad \Rightarrow \quad |c_{n+1}| = \frac{u'}{2^{k+1}\cdot v'}$$

where $u, \tilde{v}, u', v'$ are odd.

u is even: First, we write $u = 2^k \cdot \tilde{u}$, where $k \geq 1$ and $\tilde{u}$ is odd. In particular, $c_n = \frac{2^k \cdot \tilde{u}}{v}$, where v is odd. Similarly, $A = 2^l \cdot \tilde{A}$, where $l \geq 0$ and $\tilde{A}$ is odd. Then

$$c_n^4 \pm 16A^2 = \frac{2^{4k}\cdot \tilde{u}^4 \pm 2^{4+2l}\tilde{A}^2 v^4}{v^4},$$

where both numbers are of the form

$$\frac{2^{2m}\bar{u}}{v^4}\,,$$

where $\bar{u}$ is odd and $4 \leq 2m \leq 4k$, *i.e.*, $2 \leq m \leq 2k$. Therefore,

$$|c_{n+1}| = \frac{2^{2m}u_0 \cdot v^3}{2\cdot 2^k\tilde{u}\cdot v^4 \cdot 2^m u_1} = \frac{2^{m-k-1}\cdot u'}{v'},$$

where u_0, u_1, u', v' are odd. Since $m < 2k+1$, we have $m-k-1 < k$, and therefore we obtain

$$c_n = \frac{2^k \cdot \tilde{u}}{v} \quad \Rightarrow \quad |c_{n+1}| = \frac{2^{k'} \cdot u'}{v'}$$

where $\tilde{u}, v, u', v'$ are odd and $0 \leq k' < k$.

Both cases together show that whenever $c_n = 2^k \cdot \frac{u}{v}$, where $k \in \mathbb{Z}$ and u, v are odd, then $|c_{n+1}| = 2^{k'} \cdot \frac{u'}{v'}$, where u', v' are odd and $k' < k$. So, for any distinct non-negative integers n and n', $|c_n| \neq |c_{n+1}|$. *q.e.d.*

The proof of Theorem 3 gives us the following reformulation of Fermat's Algorithm:

Corollary 4. *Assume that A is a congruent number, and that (a_0, b_0, c_0) is a rational Pythagorean A-triple, i.e., $A = \left|\frac{a_0 b_0}{2}\right|$. Then*

$$a_1 = \frac{4Ac_0}{\sqrt{c_0^4 - 16A^2}}, \quad b_1 = \frac{\sqrt{c_0^4 - 16A^2}}{2c_0}, \quad c_1 = \frac{c_0^4 + 16A^2}{2c_0\sqrt{c_0^4 - 16A^2}},$$

is also a rational Pythagorean A-triple.

Proof. Notice that $c_0^4 - 4a_0^2 b_0^2 = c_0^4 - 16A^2$ and recall that $|a_0^2 - b_0^2| = \sqrt{c_0^4 - 16A^2}$. *q.e.d.*

3 Doubling points with Fermat's Algorithm

Before we prove Theorem 1 (*i.e.*, that congruent number curves do not contain rational points of finite order), we first prove that Fermat's Algorithm 2 is essentially doubling points on congruent number curves.

Lemma 5. *Let A be a congruent number, let (a_0, b_0, c_0) be a rational Pythagorean A-triple, and let (a_1, b_1, c_1) be the rational Pythagorean A-triple obtained by* Fermat's Algorithm *from (a_0, b_0, c_0). Furthermore, let (x_0, y_0) and (x_1, y_1) be the rational points on the curve C_A which correspond to (a_0, b_0, c_0) and (a_1, b_1, c_1), respectively. Then we have*

$$2 * (x_0, y_0) = (x_1, -y_1).$$

Proof. Let (a_0, b_0, c_0) be a rational Pythagorean A-triple. Then, according to (5), the rational Pythagorean A-triple (a_1, b_1, c_1) which we obtain by Fermat's Algorithm is given by

$$a_1 := \frac{4c_0^2 a_0 b_0}{2c_0(a_0^2 - b_0^2)}, \quad b_1 := \frac{c_0^4 - 4a_0^2 b_0^2}{2c_0(a_0^2 - b_0^2)}, \quad c_1 := \frac{c_0^4 + 4a_0^2 b_0^2}{2c_0(a_0^2 - b_0^2)}.$$

Now, by (1), the coordinates of the rational point (x_1, y_1) on C_A which corresponds to the rational Pythagorean A-triple (a_1, b_1, c_1) are given by

$$x_1 = \frac{a_0 b_0 \cdot (b_1 + c_1)}{2 \cdot a_1} = \frac{a_0 b_0 \cdot 2c_0^4}{2 \cdot 4c_0^2 a_0 b_0} = \frac{c_0^2}{4},$$

$$y_1 = \frac{2(\frac{a_0 b_0}{2})^2 (b_1 + c_1)}{a_1^2} = \frac{1}{8}(a_0^2 - b_0^2)c_0.$$

Let still (a_0, b_0, c_0) be a rational Pythagorean A-triple. Then, again by (1), the corresponding rational point (x_0, y_0) on C_A is given by

$$x_0 = \frac{b_0(b_0 + c_0)}{2}, \qquad y_0 = \frac{b_0^2(b_0 + c_0)}{2}.$$

Now, as we have seen in (3) and (4), the coordinates of the point $(x_1', y_1') := 2 * (x_0, y_0)$ are given by $x_1' = \lambda^2 - 2x_0$, $y_1' = 3x_0\lambda - \lambda^3 - y_0$, where

$$\lambda = \frac{3x_0^2 - (\frac{a_0 b_0}{2})^2}{2y_0} = \frac{\frac{3b_0^2(b_0+c_0)^2 - a_0^2 b_0^2}{4}}{b_0^2(b_0 + c_0)} = \frac{3(b_0 + c_0)^2 - a_0^2}{4(b_0 + c_0)} = \frac{3(b_0 + c_0)^2 + (b_0^2 - c_0^2)}{4(b_0 + c_0)} =$$

$$\frac{(3b_0^2 + 6b_0c_0 + 3c_0^2) + (b_0^2 - c_0^2)}{4(b_0 + c_0)} = \frac{4b_0^2 + 6b_0c_0 + 2c_0^2}{4(b_0 + c_0)} = \frac{2b_0^2 + 3b_0c_0 + c_0^2}{2(b_0 + c_0)} =$$

$$\frac{(2b_0 + c_0)(b_0 + c_0)}{2(b_0 + c_0)} = \frac{(2b_0 + c_0)}{2}.$$

Hence,

$$x_1' = \lambda^2 - 2x_0 = \frac{(2b_0 + c_0)^2}{4} - b_0(b_0 + c_0) = \frac{(4b_0^2 + 4b_0c_0 + c_0^2) - (4b_0^2 + 4b_0c_0)}{4} = \frac{c_0^2}{4}$$

and

$$y_1' = 3x_0\lambda - \lambda^3 - y_0 = \frac{1}{8}(2b_0^2c_0 - c_0^3) = \frac{1}{8}(b_0^2 - a_0^2)c_0,$$

i.e., $x_1 = x_1'$ and $y_1 = -y_1'$, as claimed. *q.e.d.*

With LEMMA 5, we are now able to prove THEOREM 1, which states that for a congruent number A, the curve $C_A : y^2 = x^3 - A^2x$ does not have rational points of finite order other than $(0, 0)$ and $(\pm A, 0)$.

Proof of Theorem 1. Assume that A is a congruent number, let (x_0, y_0) be a rational point on C_A which $y_0 \neq 0$, and let (a_0, b_0, c_0) be the rational Pythagorean A-triple which corresponds to (x_0, y_0) by (2). Furthermore, for positive integers n, let (a_n, b_n, c_n) be the rational Pythagorean A-triple we obtain by FERMAT'S ALGORITHM from $(a_{n-1}, b_{n-1}, c_{n-1})$, and let (x_n, y_n) be the rational point on C_A which corresponds to the rational Pythagorean A-triple (a_n, b_n, c_n) by (1).

By the proof of LEMMA 5 we know that the x-coordinate of $2 * (x_n, y_n)$ is equal to $\frac{c_n^2}{4}$, and by THEOREM 3 we have that for any distinct non-negative integers n, n', $|c_n| \neq |c_{n'}|$. Hence, for all distinct non-negative integers n, n' we have

$$(x_n, y_n) \neq (x_{n'}, y_{n'}),$$

which shows that the order of (x_0, y_0) is infinite. *q.e.d.*

References

[1] JASBIR S. CHAHAL, *Congruent numbers and elliptic curves*, ***American Mathematical Monthly***, vol. 113 (2006), 308–317.

[2] PIERRE DE FERMAT, *Fermat's Diophanti Alex. Arith., 1670*, *in* ***Œuvres III*** (Ministère de l'instruction publique, ed.), Gauthier-Villars et fils, Paris, 1896, pp. 254–256.

[3] NORBERT HUNGERBÜHLER, *A proof of a conjecture of Lewis Carroll*, ***Mathematics Magazine***, vol. 69 (1996), 182–184.

[4] NEAL KOBLITZ, ***Introduction to Elliptic Curves and Modular Forms***, 2nd ed., [Graduate Texts in Mathematics 97], Springer-Verlag, New York, 1993.