A Theorem of Congruent Primes

Jorma Jormakka

Contact by: jorma.o.jormakka@gmail.com

Abstract. The paper presents a theorem when a prime number is not a congruent number. This theorem does not add to the present knowledge of congruent primes since all primes fulfilling the conditions of the theorem can already be classified into congruent and noncongruent numbers, but the proof of the theorem has certain own interest and this is why I decided to write it into a paper.

Key words: Congruent numbers, elliptic curves, number theory.

1 Introduction

Consider an elliptic curve of the form:

$$y^2 = x^3 - d^2 x \tag{1}$$

where d is an integer. A rational solution (x, y) to the elliptic curve (1) is a solution where x and y are rational numbers.

The substitution $x = d(a+b)/b$, $y = 2d^2(a+c)/b^2$ changes $y^2 = x^3 - d^2x$ to $a^2 + b^2 = c^2$ with $ab = 2d$. Then $4d^2 = a^2(c^2 - a^2)$. Integers d that give rational number solutions to $a^2 + b^2 = c^2$, $ab = 2d$ are called congruent numbers. If d is a congruent number the elliptic curve (1) has a rational solution where y is not zero. In that case it has infinitely many rational solutions.

If there is a solution for $d = s^2$, then there is a solution for $d = 1$ because the substitution $y = s^3 y'$, $x = s^2 x'$ changes $y^2 = x^3 - d^2x$ to $y'^2 = x'^3 - x'$. It is known that every $d = s^2$ is a congruent number. The case where d is a prime number is amost solved.

For notations the following concepts suffice: The condition that the integer a divides integer b is written as $a|b$. If $p > 2$ is a prime, the cyclic group of integers modulo p is denoted by Z_p and $Z_p^* = \{1, \ldots, p-1\}$. The set of quadratic residues modulo p is the set

$$QR_p = \{x \in Z_p^* | \exists y \in Z_p^* \text{ such that } y^2 \equiv x \pmod{p}\}.$$

The set of quadratic nonresidues modulo p is the set

$$QNR_p = \{x \in Z_p^* | x \notin QR_p\}.$$

Let us start by two very simple lemmas.

Lemma 1. *Let $c^2 = a^2 + b^2$, $a, b, c \in Z$, then $\exists h, m, e \in \mathbb{N}$ such that*

$$a = \pm hem \ , \ b = \pm\frac{1}{2}h(m^2 - e^2) \ , \ c = \pm\frac{1}{2}h(m^2 + e^2).$$

Proof. Without loss of generality we can assume that $a, b, c \in N$. We can write $c^2 - b^2 = (c-b)(c+b) = a^2$. Let $h = gcd(c+b, c-b)$. Then there exists m and e, $m > e$, $gcd(m, e) = 1$, such that $c + b = hm^2$, $c - b = he^2$. The claim follows. □

With Lemma 1 we can characterize congruent numbers.

Lemma 2. *Let $d \in Z$, $d > 0$. Rational solutions (x, y) with $x \neq 0, y \neq 0$ to*

$$y^2 = x^3 - d^2 x$$

are of the form

$$(x_1, y_1) = \left(d\frac{m+e}{m-e}, \pm\frac{k}{j}d\frac{m+e}{m-e}\right),$$

$$(x_2, y_2) = \left(d\frac{m-e}{m+e}, \pm\frac{k}{j}d\frac{m-e}{m+e}\right),$$

where $k, j, e, m \in N$, $m > e$, $gcd(m, e) = 1$, $gcd(k, j) = 1$, *satisfy*

$$d = \left(\frac{k}{2j}\right)^2 \frac{m^2 - e^2}{em}. \tag{2}$$

Proof. Let $x, y \in Q$, $x \neq 0, y \neq 0$. Let us write $\alpha = \frac{d}{x} + 1 \in Q$, $\beta = \frac{y}{x} \in Q$. Solving (10) for x and solving x from the definition of α yields

$$x = \frac{\beta^2}{2\alpha - \alpha^2} = \frac{d}{\alpha - 1}.$$

Writing $\beta = \frac{k}{j}$ for some $k, j \in N$ gives

$$\alpha_{1,2} = 1 - \frac{k^2}{j^2 2d} \pm \frac{\sqrt{(2dj^2)^2 + (k^2)^2}}{j^2 2d}.$$

As $y \neq 0$, $k \neq 0$. By Lemma 1, $\alpha_{1,2} \in Q$ if and only if there exist $h, e, m \in N$, $gcd(e, m) = 1$, $m > e$, such that

$$k^2 = hem \ , \ 2dj^2 = \frac{1}{2}h(m^2 - e^2) \ , \ c = \frac{1}{2}h(m^2 + e^2).$$

If $em = 0$, then $k = 0$ and $y = 0$. This solution gives $j = 2dj^2$

$$\alpha_{1,2} = 1 \pm \frac{2dj^2}{2dj^2} = 1 \pm 1 \ , \ \alpha_1 = 2, \alpha_2 = 0,$$

$$x_1 = \frac{d}{\alpha - 1} = d \ , \ x_2 = -d \ , y = 0$$

but we have excluded this case in the assumptions. Since $em \neq 0$, let us write $h = \frac{k^2}{em}$. Eliminating h yields

$$d = \left(\frac{k}{2j}\right)^2 \frac{m^2 - e^2}{em},$$

$$c = \frac{k^2}{2}(m^2 + e^2).$$

Simplifying $\alpha_{1,2}$ yields

$$\alpha_{1,2} = \frac{1}{m^2 - e^2}\left(m^2 - e^2 - 2em \pm (m^2 + e^2)\right),$$

i.e.,

$$\alpha_1 = \frac{2m}{m+e} \ , \ \alpha_2 = -\frac{2e}{m-e}$$

$$x_1 = \frac{d}{\alpha_1 - 1} = d\frac{m+e}{m-e} \ , \ x_2 = -d\frac{m-e}{m+e},$$

$$y = \beta x \ , \beta^2 = \left(\frac{k}{j}\right)^2 = 4d\frac{em}{m^2 - e^2}.$$

This gives the claim. □

As two examples of Lemma 2

$$d = 5 = \left(\frac{3}{2\cdot 2}\right)^2 \frac{9^2 - 1^2}{9\cdot 1}$$

$$d = 7 = \left(\frac{24}{2\cdot 5}\right)^2 \frac{16^2 - 9^2}{16\cdot 9}$$

are both congruent numbers. Notice that $gcd(k, j) = 1$ but it is allowed that $2|k$.

If d is a square, there are no rational solutions to (1) with $y \neq 0$. There are the three solutions $(0, 0), (d, 0), (-d, 0)$ to (1), so the number of rational solutions of (1) is finite, the rank of the elliptic curve is zero.

In the next theorem gives a set of values where d is a prime number and (1) has no rational solutions, i.e., the elliptic curve has rank zero. The case of prime numbers d is rather well known: if $p \equiv 5 \pmod{d}$ or $p \equiv 7 \pmod{d}$ the number d is a congruent number and there are solutions to (1). If $p \equiv 3 \pmod{d}$ there are no solutions and d is not a congruent number. The only case remaining is $p \equiv 1 \pmod{d}$. For that case it is known that e.g. $p = 41$ is a congruent number, while e.g. $p = 17$ is not.

The next theorem does not solve the problem for any prime p that is one modulo eight because if $p \equiv 1 \pmod{8}$ it is necessarily true that $-1 \in QR_p$, i.e.,

$-1 \in QR_p$ is equivalent with the condition that $4|(p-1)$ and if $p \equiv 1 \pmod{d}$, then $8|(p-1)$. The theorem does prove e.g. that $p = 19$ is not a congruent number, but as $19 \equiv 3 \pmod{d}$ this is known. Yet, the method of this proof seemed interesting enough to me in order to be written down. The method may generalize to other numbers than primes. The primality condition is used only in a few places. The main idea is to exclude branches from a recursion.

Theorem 1. *Let $d > 3$ be a prime such that $-1 \in QNR_d$ and $2 \in QRN_d$. The equation (2) in Lemma 2 does not have solutions $k, j, m, e \in \mathbb{N}$ where $gcd(m, e) = 1$, $gcd(k, j) = 1$, $m > e > 0$.*

Proof. We write (2) with m_1, e_1

$$d = \left(\frac{k}{2j}\right)^2 \frac{m_1^2 - e_1^2}{e_1 m_1} \tag{3}$$

If $d|m_1$ then $d|e_1$ and $gcd(m_1, e_1) \neq 1$, thus $d \not| m_1$ and $d \not| e_1$. If $d|k^2$ then since d is a prime $d|k$. It follows that $k = dk_1$ and as $gcd(k, 2j) = 1$ holds $d \not| 2j$. Thus

$$(2j)^2 m_1 e_1 = dk_1^2(m_1^2 - e_1^2)$$

which is not possible as the left side is not divisible by d. Thus $d \not| k^2$. Therefore $d|m_1^2 - e_1^2$.

If $2 \not| k$ we convert (3) into the form

$$d = \left(\frac{k}{j}\right)^2 \frac{st}{m^2 - e^2} \tag{4}$$

by the substitution $m_1 = m + e$, $e_1 = m - e$, i.e., $2m = m_1 + e_1$, $2e = m_1 - e_1$. As $m_1 e_1 = (m+e)(m-e) = m^2 - e^2$ holds $em = \frac{1}{4}(m_1 + e_1)(m_1 - e_1)$. As $4|(m_1^2 - e_1^2)$ in (3) if $2 \not| k$ it follows that one of $m_1 + e_1$ or $m_1 - e_1$ is even. If so, they are both even and $2|m_1 + e_1$, $2|m_1 - e_1$ and m, e are integers. As $gcd(m_1, e_1) = 1$,

$gcd(m_1+e_1, m_1-e_1) = 2$. Then $gcd(m,e) = gcd(((m_1+e_1)/2)((m_1-e_1)/2)) = 1$. Since $m_1 > e_1 > 0$ holds $m > e > 0$.

If $2|k$ then the substitution is $m = m_1+e_1$, $e = m_1-e_1$. Then m, e are integers and $m > e > 0$. In this case $2 \not| j$ gecause $gcd(k,j) = 1$. Therefore $2 \not| (m_1^2 - e_1^2$. It follows that $gdc(m,e) = gcd(m_1+e_1, m_1-e_1) = 1$. We get the same form (4) since $me = m_1^2 - e_1^2$ and $m^2 - e^2 = 4m_1e_1$.

Then $d|em$ and $j^2|em$. Let us write (4) as

$$j^2(m+e)(m-e)d = k^2me. \tag{5}$$

Since $gcd(m,e) = 1$ it follows that $gcd(m \pm e, m) = 1$. Indeed, if $m \pm e = c_1r$, $m = c_2r$ for some $r, c_1, c_2 \in \mathbb{N}$, then

$$c_1c_2r = c_2m \pm c_2e = c_1m \Rightarrow (c_1 - c_2)m = \pm c_2e$$

$$\Rightarrow m|c_2 \Rightarrow \exists \alpha \in \mathbb{N} \text{ such that } c_2 = \alpha m$$

$$\Rightarrow m = \alpha mr \ \ \Rightarrow \alpha r = 1 \Rightarrow r = 1.$$

Similarly, $gcd(m \pm e, e) = 1$.

Since $gcd(k,j) = 1$ it follows from (4) that $k^2 = m^2 - e^2$. Therefore (4) implies that $dj^2 = em$. As $dj^2 = em$ and $gcd(e,m) = 1$ there is one of the cases: either $m = ds^2$, $e = t^2$ for some $s, t > 0$ or $m = s^2$, $e = dt^2$.

As $k^2 = (m+e)(m-e)$ and $gcd((m+e)(m-e)) \leq 2$ we have two cases cases: either $m+e = c_1^2$ and $m-e = c_2^2$ for some $c_1, c_2 > 0$ or $m+e = 2c_1^2$ and $m-e = 2c_2^2$.

We have four cases in total.

Case 1. $m = ds^2$, $e = t^2$, $m+e = c_1^2$, $m-e = c_2^2$. Then

$$m - e = s^2d - t^2 = c_2^2.$$

The equation yields $-1 \equiv (c_2 t^{-1})^2 \pmod{d}$ which is impossible since $-1 \in QNR_d$.

Case 2. $m = ds^2$, $e = t^2$, $m + e = 2c_1^2$, $m - e = 2c_2^2$. Then

$$s^2 d + t^2 = 2c_1^2 \ , \ s^2 d - t^2 = 2c_2^2.$$

Multiplying the modular equations

$$t^2 \equiv 2c_1^2 \pmod{d} \ , -t^2 \equiv 2c_2^2 \pmod{d}$$

yields $-1 \equiv (2c_1c_2t^{-2})^2 \pmod{d}$ which is impossible since $-1 \in QNR_d$.

Case 3. $m = s^2$, $e = dt^2$, $m + e = c_1^2$, $m - e = c_2^2$. Then

$$s^2 + t^2 d = c_1^2 \ , \ s^2 - t^2 d = c_2^2.$$

Thus

$$2s^2 = c_1^2 + c_2^2 \tag{6}$$

so

$$4s^2 = c_1^2 + 2c_1c_2 + c_2^2 + c_1^2 - 2c_1c_2 + c_2^2$$

$$(2s)^2 = (c_1 + c_2)^2 + (c_1 - c_2)^2. \tag{7}$$

It follows from Lemma 1 that $\exists h', e', m' \in \mathbb{N}$, $gcd(m', e') = 1$ such that

$$c_1 + c_2 = h'e'm' \ , c_1 - c_2 = \frac{1}{2}h'(m'^2 - e'^2),$$

$$2s = \frac{1}{2}h'(m'^2 + e'^2).$$

Solving c_1, c_2, s yields

$$c_1 = \frac{1}{4}h'(2e'm' + m'^2 - e'^2),$$

$$c_2 = \frac{1}{4}h'(2e'm' + e'^2 - m'^2),$$

$$s = \frac{1}{4}h'(m'^2 + e'^2).$$

Since

$$2t^2 d = c_1^2 - c_2^2 = (c_1 - c_2)(c_1 + c_2)$$

we get

$$d = \frac{1}{4t^2}h'^2 e'm'(m'^2 - e'^2)$$

i.e.

$$d = \left(\frac{h'e'm'}{2t}\right)^2 \frac{(m'^2 - e'^2)}{e'm'}.$$

Removing the greatest common divisor of $h'e'm'$ and t this equation can be written as

$$d = \left(\frac{k_{i+1}}{2j_{i+1}}\right)^2 \frac{(m_{i+1}^2 - e_{i+1}^2)}{e_{i+1}m_{i+1}}. \tag{8}$$

As $gcd(m', e') = 1$ and we made $gcd(k, j) = 1$, equation (8) is is of the same form as (3)

$$d = \left(\frac{k_i}{2j_i}\right)^2 \frac{(m_i^2 - e_i^2)}{e_i m_i} = \left(\frac{k}{2j}\right)^2 \frac{(m_1^2 - e_1^2)}{e_1 m_1}.$$

We have a recursion that in each step reduces the numbers m_i, e_i to numbers m_{i+1}, e_{i+1} that are of the order of square root of m_i, e_i.

Case 4. $m = s^2$, $e = dt^2$, $m + e = 2c_1^2$, $m - e = 2c_2^2$. We can select $c_1 > c_2 \geq 0$. Then

$$s^2 + t^2 d = 2c_1^2 \ , \ s^2 - t^2 d = 2c_2^2.$$

Thus

$$s^2 = c_1^2 + c_2^2 \ \ dt^2 = c_1^2 - c_2^2 = (c_1 - c_2)(c_1 + c_2). \tag{9}$$

Let us notice that $m + e = 2c_1^2$ and

$$1 = gcd(m + e, e) = gcd(2c_1^2, dt^2) \Rightarrow gcd(c_1, t) = 1, gcd(2, t) = 1$$

$$1 = gcd(m-e,e) = gcd(2c_2^2, dt^2) \Rightarrow gcd(c_2,t) = 1.$$

First we exclude one case in the second equation of (9). If $t > 1$ and $c_1 + c_2 = \alpha_1 t$ and $c_1 - c_2 = \alpha_2 t$ for some $\alpha_1, \alpha_2 \in \mathbb{N}$, then

$$2c_1 = (\alpha_1 + \alpha_2)t \Rightarrow t = 1, 2c_1 = \alpha_1 + \alpha_2,$$

$$2c_2 = (\alpha_1 - \alpha_2)t \Rightarrow t = 1, 2c_1 = \alpha_1 - \alpha_2.$$

Thus, $dt^2 = c_1^2 - c_2^2 = \alpha_1\alpha_2 t^2$. It follows that $d = \alpha_1\alpha_2$ and as d is prime and necessarily $\alpha_1 > \alpha_2$ it follows that $\alpha_1 = d$, $\alpha_2 = 1$. Then $c_1 = d+1$ and $c_2 = d-1$. Consequently $s^2 = c_1^2 + c_2^2 = 2(d^2 - 1)$ is even, so m is even. Since $s^2 + dt^2 = 2c_1^2$ it would follow that t is also even as d is odd, but $t = 1$ in this case. We have a contradiction.

Thus, in (9) must be one of the three cases

$$t^2 | (c_1 + c_2) \Rightarrow (c_1 - c_2) | d \Rightarrow c_1 - c_2 = d \Rightarrow t^2 = c_1 + c_2,$$

or

$$t^2 | (c_1 - c_2) \Rightarrow (c_1 + c_2) | d \Rightarrow c_1 + c_2 = d \Rightarrow t^2 = c_1 - c_2,$$

or

$$t = 1.$$

In the first case

$$2c_1 = t^2 + d \geq 0 \ , \ 2c_2 = t^2 - d \geq 0.$$

In the second case

$$2c_1 = d + t^2 \geq 0 \ , \ 2c_2 = d - t^2 \geq 0.$$

In both of these two cases we can derive in a similar way:

$$s^2 = c_1^2 + c_2^2 \ \Rightarrow (2s)^2 = (2c_1)^2 + (2c_2)^2$$

yields

$$(2s)^2 = (d + t^2)^2 + (d - t^2)^2. \tag{10}$$

By Lemma 2 there exist $h', e', m' \in \mathbb{N}$ such that

$$d + t^2 = h'e'm' \ , \ d - t^2 = \frac{1}{2}h'(m'^2 - e'^2).$$

The first equation implies that $d \not| h'$. Thus

$$4d = h'((m' + e')^2 - 2e'^2)$$

i.e., as $h' \not\equiv 0 \pmod{d}$

$$2 \equiv (m'^2 + e'^2)^2 e'^{-2} \pmod{d} \tag{11}$$

which is a contradiction since $2 \in QNR_d$. There remains the case $t = 1$. Then $2c_1^2 = s^2 + d$, $2c_2^2 = s^2 - d$. Instead of (10) we get

$$(2s)^2 = (d + s^2)^2 + (d - s^2)^2.$$

The contradiction (11) comes in the same way with t replaced by s. This means that Case 4 is not possible.

Because Cases 1, 2 and 4 are not possible, only Case 3 is left. Case 3 gives a recursion formula. The values h', m', e' in Lemma 1 satisfy

$$\frac{e'}{m'} = \frac{a}{b + c} = \frac{c - b}{a}$$

$$h' = gcd(b+c, b-c)$$

giving $a^2 = c^2 - b^2$. The numbers h', m', e' can be chosen to be positive and on the order of a, b, c. Thus, h', m', e' in (8) are of the order c_1, c_2. The numbers c_1, c_2 are of the order $\sqrt{m}$, $\sqrt{e}$. Therefore in each step the numbers m_i, e_i get smaller, they are reduced to the order of their square roots. Consider the problem when the recursion stops.

Let us look at an example of $d = 5$. Then

$$d = 5 = \left(\frac{3}{2 \cdot 2}\right)^2 \frac{9^2 - 1^2}{9 \cdot 1}.$$

We have $m_1 = 9, e_1 = 1, k = 3, j = 2$. We can do the first step and find $m = 5, e = 4$ and

$$d = 5 = \left(\frac{3}{2}\right)^2 \frac{5 \cdot 4}{5^2 - 4^2}.$$

Identifying $k^2 = 3^2 = 5^2 - 4^2 = 9$, $j^2 d = 4 \cdot 5 = 20 = 5 \cdot 4 = me$, $m = ds^2 = 5 \cdot 1^2$, $e = t^2 = 2^2$, $m + e = 5 + 4 = 3^2 = c_1^2$ and $m - e = 5 - 4 = 1^2 = c_2^2$ shows that the logic in the lemma is correct. We have Case 1, but for $d = 5$ the conditions of the lemma are not fulfilled: $-1 \in QNR_5$. This is why Case 1 does not give a contradiction. What happens in Case 1 is that when we remove the term dt^2 in a case resembling (6) we do not get (6) but

$$2t^2 = c_1^2 - c_2^2$$

Therefore we do not get (7) which can be inserted to the equation to Lemma 1 for calculation of the numbers h', m', e'.

Let us look at another example, that of $d = 7$. Here $-1 \in QNR_7$ and the Case is not 1.

$$d = 7 = \left(\frac{24}{2 \cdot 5}\right)^2 \frac{16^2 - 9^2}{16 \cdot 9}.$$

We have $m_1 = 16, e_1 = 9, k = 24, j = 5$. We find $m = 16+9 = 25, e = 16-9 = 7$. Thus

$$d = 7 = \left(\frac{24}{5}\right)^2 \frac{25 \cdot 7}{25^2 - 7^2}.$$

Here $k^2 = 24^2 = 576 = 25^2 - 7^2 = m^2 - e^2$, $j^2 d = 25 \cdot 7 = 175 = 25 \cdot 7 = me$, $m = s^2 = 5^2$, $e = dt^2 = 7 \cdot 1^2$, $m + e = 25 + 7 = 32 = 2 \cdot 4^2 = 2c_1^2$ and $m - e = 25 - 7 = 18 = 2 \cdot 3^2 = 2c_2^2$. The Case is 4. We notice that $t^2 = 1$ and $c_1 = 4, c_2 = 3$, thus we have the case $t = 1$. Then $s^2 + d = 5^2 + 7 = 32 = 2 \cdot 4^2 = 2c_1^2$ and $s^2 - d = 5^2 - 7 = 18 = 2 \cdot 3^2 = 2c_2^2$. We get

$$(2s)^2 = 100 = 64 + 36 = (2c_1)^2 + (2c_2)^2 = (5^2 + 7)^2 + (5^2 - 7)^2$$

and therefore find the numbers h', m', e' for $10^2 = 8^2 + 6^2$. The numbers are $h' = gcd(10 + 6, 10 - 6) = 4$, $e' = 1$, $m' = 2$. Thus

$$d + t^2 = h'e'm' = 7 + 1 = 8 \ , \ d - t^2 = \frac{1}{2}h'(m'^2 - e'^2) = 6$$

are true and

$$4d = h'((m' + e')^2 - 2e'^2) = 28 = 4 \cdot (3^2 - 2).$$

We get the modular equation $3^2 \equiv 2 \bmod (7)$, which violates the assumption $2 \in QNR_d$, but indeed $2 \in QR_7$. Therefore for $d = 7$ we do not get a contradiction.

The way the lemma works is that in (2) the numbers m_1 and e_1 must be squares $m_1 = s_1^2$, $e_1 = t_1^2$ so that k^2 can cancel them. The condition $-1 \in QNR_d$ excludes the larger branch $(s_1^2 + t_1^2)$ of

$$m_1^2 - e_1^2 = (s_1^2 + t_1^2)(s_1^2 - t_1^2)$$

by $(s_1^2 + t_1^2) \equiv 0 \pmod{d}$ being impossible.

Therefore $4d|(m_1^2 - e_1^2)$ leads to $4d|(s_1^2 - t_1^2)$. The condition $2 \in QNR_d$ excludes Case 4 and leaves only Case 3 which gives a recursion. Thus, the numbers m_i, e_i get smaller.

If there is a congruent number d with $-1 \in QNR_d$, the recursion must continue until it stops in some way and not to a contradiction, but the recursion does not stop and continues to a contradiction. At each stage $4d|(m_i^2 - e_i^2)$ or $d|(m_i^2 - e_i^2)$ depending on if k_i is odd or even. The numbers m_i and e_i become smaller on each step. Finally we must have $4d = m_i^2 - e_i^2$ or $d = m_i^2 - e_i^2$.

Changing variables in (2) to $m = (m_i + e_i)/2$, $e = (m_i - e_i)/2$ if k is odd and $m = m_i + e_i$, $e = m_i - e_i$ if k is even we get

$$d = \frac{k^2}{j^2} \frac{me}{m^2 - e^2}. \tag{12}$$

When the recursion has reached $4d = m_i^2 - e_i^2$ or $d = m_i^2 - e_i^2$ the number $j = 1$. In (12) necessarily $k^2 = m_i^2 e_i^2$ and consequently $d = me$. As d is prime either $m = d$, $e = 1$ or $m = 1$, $e = d$. As in Cases 1 and 2 the choice $m = d$ leads to $-1 \in QR_d$ and is impossible. Thus $m = 1$ and $t = d$, but then $m^2 - e^2 < 0$ and $d > 0$ is negative. This is a contradiction. The recursion leads to a contradiction and the claim of the lemma follows. □

There are primes d filling the conditions of the lemma: for $d = 19$ holds $-1 \in QNR_{19}$ and $2 \in QNR_{19}$.

While working with the Birch and Swinnerton-Dyer conjecture in 2010 I derived in [1] a theorem of congruent primes. The theorem (Lemma 11) in [1] was never needed for the result it gives to primes, but as an easy case of the proof method that I hoped to generalize to other d. Now I have rewritten the 2010 paper and do not use the method of Lemma 11. Yet, it has some own interest in the proof method. Therefore I moved it into this short paper. There were some typos in [1] in the proof of Lemmas 10 and 11, which are Lemma 2 and Theorem 1 in this paper. Now the errors are fixed. The method of the proof does work. Maybe some application for the method will be found later.

References

1. J. Jormakka, On the rank of elliptic curves, arXiv:0806.4091, first version from 2010.