involve

a journal of mathematics

Integer solutions to $x^2 + y^2 = z^2 - k$ for a fixed integer value k

Wanda Boyer, Gary MacGillivray, Laura Morrison,
C. M. (Kieka) Mynhardt and Shahla Nasserasr

msp

2017 vol. 10, no. 5

INVOLVE 10:5 (2017)
dx.doi.org/10.2140/involve.2017.10.881

Integer solutions to $x^2 + y^2 = z^2 - k$ for a fixed integer value k

Wanda Boyer, Gary MacGillivray, Laura Morrison,
C. M. (Kieka) Mynhardt and Shahla Nasserasr

(Communicated by Chi-Kwong Li)

For a given integer k, general necessary and sufficient conditions for the existence of integer solutions to an equation of the form $x^2 + y^2 = z^2 - k$ are given. It is shown that when there is a solution, there are infinitely many solutions. An elementary method for finding the solutions, when they exist, is described.

1. Introduction

Finding solutions to quadratic Diophantine equations in three or more variables has been of interest since ancient times. One example is *Pythagoras' equation* $x^2 + y^2 = z^2$, which was studied at least 3500 years ago by the Babylonians. Another example is its generalization $x^2 + y^2 + w^2 = z^2$, which was completely solved by Catalan [1885] (also see [Ayoub 1984]). A further generalization is the equation $x^2 + y^2 = z^2 - k$ for a given integer $k \neq 0$. Frink [1987] gave a complete solution to the equations of the form $x^2 + y^2 = z^2 + 1$. Moreover, solutions to the equation $x^2 + y^2 = z^2 - k$ with $k = 1, 2$ were crucial in finding the minimum number of arcs in primitive digraphs with smallest large exponent; see [MacGillivray et al. 2008]. When k is a perfect square, the solution set can be found using Catalan's method. In the previous reference, the solution set is described when $k = 1, 2$.

We study the equation $x^2 + y^2 = z^2 - k$ for any fixed integer value of k. It is advantageous to write $z = x + t$ for some integer t. Hence we seek solutions x, y, t to the Diophantine equation

$$x^2 + y^2 = (x + t)^2 - k. \tag{1}$$

We give conditions on k and t for which the equation has no solution, and describe an elementary method for finding all solutions to the equation in the cases when

MSC2010: primary 11D09; secondary 11A07, 11A15.
Keywords: Diophantine equations, congruences, residue systems, Pythagorean triples.

they exist. If $t = 0$ then (1) becomes $y^2 = -k$, which has a solution if and only if $-k$ is a perfect square. Thus in the sequel we consider only nonzero integers t.

2. Background

In an attempt to make this article self-contained, we review some relevant background from elementary number theory. The results and proofs in this section can be found in standard number theory books; for example, see [Apostol 1976; Kumanduri and Romero 1998].

We shall make use of quadratic congruences, that is, congruences of the form $x^2 \equiv a \pmod{m}$, for integers a and m. The integer a is a *quadratic residue* modulo m if the congruence $x^2 \equiv a \pmod{m}$ has a solution, and a *quadratic nonresidue* modulo m otherwise.

Suppose p is an odd prime and p does not divide a. The *Legendre symbol*, denoted by (a/p), is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

Theorem 1 [Kumanduri and Romero 1998, p. 216]. *Suppose p is an odd prime which divides neither a nor b. Then*:

(1) $\left(\frac{a^2}{p}\right) = 1.$

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$

(3) *Euler's criterion*: $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$

Proposition 2 [Apostol 1976, p. 181; Kumanduri and Romero 1998, p. 414]. *Suppose p is an odd prime with $p \neq 3$. Then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \pmod{4}, \\ -1 & \textit{if } p \equiv 3 \pmod{4}, \end{cases} \tag{2}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1, 7 \pmod{8}, \\ -1 & \textit{if } p \equiv 3, 5 \pmod{8}, \end{cases} \tag{3}$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1, 11 \pmod{12}, \\ -1 & \textit{if } p \equiv 5, 7 \pmod{12}. \end{cases} \tag{4}$$

Proposition 3 [Kumanduri and Romero 1998, p. 428]. *For every odd prime $p \neq 5$,*

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1, 4 \pmod{5}, \\ -1 & \textit{if } p \equiv 2, 3 \pmod{5}. \end{cases}$$

We use the notation (a, b) to denote the *greatest common divisor* of integers a and b.

Proposition 4. *Suppose $a, b \in \mathbb{N}$ and p is a prime, and assume $k = k_1 p^b$ with $(k_1, p) = 1$. Consider the congruence*

$$y^2 \equiv -k \pmod{p^a}. \tag{5}$$

(1) *If $b < a$, then the congruence (5) has an integer solution if and only if b is even and $-k_1$ is a quadratic residue modulo p^{a-b}.*

(2) *If $b \geq a$, then the congruence (5) always has a solution.*

Proof. (1) The congruence $y^2 \equiv -k \pmod{p^a}$ has a solution if and only if there exists an integer m such that $m^2 = -k + p^a q = p^b(-k_1 + p^{a-b}q)$. Since p does not divide $-k_1 + p^{a-b}q$, we have $p^b \mid m^2$ but p^{b+1} does not divide m^2, thus b is even. Now, divide both sides of $m^2 = p^b(-k_1 + p^{a-b}q)$ by p^b. Then $m_1^2 = -k_1 + p^{a-b}q$, for some integer m_1, which implies $x^2 \equiv -k_1 \pmod{p^{a-b}}$ has a solution. The converse is trivial.

(2) If $b \geq a$, then $y^2 \equiv -k \pmod{p^a}$ has a solution if and only if there exists an integer m such that $m^2 = -k + p^a q = p^a(-k_1 p^{b-a} + q)$. If a is even, say $a = 2\beta$ for some integer β, then for any integer u, any number of the form $m = \pm u p^\beta$ satisfies $m^2 = (\pm p^\beta)^2(-k_1 p^{b-a} + u^2 + k_1 p^{b-a})$. So any such m with $0 \leq m \leq p^a - 1$ is a solution to the congruence $y^2 \equiv -k \pmod{p^a}$. If $a = 2\beta + 1$ is odd, then by a similar argument $m = \pm u p^{\beta+1}$, with $0 \leq m \leq p^a - 1$, is a solution to the congruence $y^2 \equiv -k \pmod{p^a}$. □

For any integer $n > 1$, and given congruence $f(x) \equiv 0 \pmod{n}$, let $N(n)$ denote the number of solutions to the congruence $f(x) \equiv 0 \pmod{n}$.

Lemma 5 [Apostol 1976, p. 118]. *Suppose $f(x)$ is a polynomial with integer coefficients. Let $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ be the prime factorization of t.*

(1) *The congruence $f(x) \equiv 0 \pmod{t}$ has a solution if and only if each of the congruences $f(x) \equiv 0 \pmod{p_i^{e_i}}$, $i = 1, 2, \dots, r$, has a solution.*

(2) $N(t) = \prod_i^r N(p_i^{e_i})$.

The following results will also be used in solving (1).

Lemma 6 [Apostol 1976, p. 178]. *If p is an odd prime and p does not divide k, then $y^2 \equiv -k \pmod{p}$ has either exactly two distinct solutions or no solution.*

Lemma 7 [Nasserasr 2007, p. 38]. *If p is an odd prime and $(k, p) = 1$, then every solution to the congruence $y^2 \equiv -k \pmod{p^e}$, $e \geq 2$, generates a solution to the congruence $y^2 \equiv -k \pmod{p}$ and conversely.*

If the modulus in Lemma 6 is a composite number, we have the following result.

Lemma 8. *If $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, where $p_1, p_2, \dots, p_r$ are distinct odd primes, $r, e_i \in \mathbb{N}$, and $(k, t) = 1$, then $y^2 \equiv -k \pmod{t}$ has 2^r distinct solutions y if $-k$*

is a quadratic residue modulo p_i for each p_i, $i = 1, 2, \ldots, r$, and no solution otherwise.

Proof. Suppose for each p_i, $i = 1, 2, \ldots, r$ there is a solution to $y^2 \equiv -k \pmod{p_i}$. Using Lemma 6, there are exactly two solutions for each congruence. Lemma 5 implies that $s^2 \equiv -k \pmod{t}$ has exactly 2^r distinct solutions. If one of the congruences $s^2 \equiv -k \pmod{p_i}$, $i = 1, 2, \ldots, r$, has no solution, then by Lemma 5, the congruence $y^2 \equiv -k \pmod{t}$ has no solution. □

The following is a special case of $y^2 \equiv -k \pmod{p}$ when k is a perfect square.

Lemma 9. *Let p be an odd prime, and a be an integer such that p does not divide a. Then the congruence $y^2 \equiv -a^2 \pmod{p}$ has exactly two distinct solutions if $p \equiv 1 \pmod{4}$ and no solution otherwise.*

Proof. The congruence $y^2 \equiv -a^2 \pmod{p}$ has exactly two distinct solutions if and only if

$$\left(\frac{-a^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a^2}{p}\right) = 1. \tag{6}$$

Since $(a^2/p) = 1$, (6) holds if and only if $(-1/p) = 1 = (-1)^{(p-1)/2}$ (using Euler's criterion). The last equation holds if and only if $p \equiv 1 \pmod{4}$. □

3. General results

We give solutions to the equation

$$x^2 + y^2 = (x+t)^2 - k.$$

First, we show that it is possible to remove common divisors of k and t.

Proposition 10. *Suppose t has prime factorization of the form $t = \prod_{i=1}^{r} p_i^{e_i}$ and let $k = k_1 p_{i_0}^{f_{i_0}}$, where $1 \le i_0 \le r$ and $p_{i_0} \nmid k_1$. Then the equation $x^2 + y^2 = (x+t)^2 - k$ is equivalent to $x_1^2 + y_1^2 = (x_1 + t_1)^2 - k_1$, where $p_{i_0}^2 \nmid (k_1, t_1)$.*

Proof. We prove the statement for the case $f_{i_0} \le e_{i_0}$. The case $f_{i_0} > e_{i_0}$ is similar. Depending on whether f_{i_0} is even or odd we have $f_{i_0} = 2\alpha + \beta$ with $\beta = 0, 1$. Since $p_{i_0}^{2\alpha} \mid (k, t)$, if the equation has a solution, then $p_{i_0}^{2\alpha} \mid y^2$. Thus, dividing both sides of the equation $y^2 = 2xt + t^2 - k$ by $p_{i_0}^{2\alpha}$ implies

$$\left(\frac{y}{p_{i_0}^{\alpha}}\right)^2 = 2\left(\frac{x}{p_{i_0}^{\alpha}}\right)\left(\frac{t}{p_{i_0}^{\alpha}}\right) + \left(\frac{t}{p_{i_0}^{\alpha}}\right)^2 - \left(\frac{k}{p_{i_0}^{2\alpha}}\right).$$

This is equivalent to $x_1^2 + y_1^2 = (x_1 + t_1)^2 - k_1 p_{i_0}^{\beta}$, and the result follows. □

In Proposition 10, if $\alpha = 1$, in solving the equation we can consider $k/p_{i_0}^2$ and t/p_{i_0} instead of k and t, respectively. By repeating this process on each common prime factor p of k and t such that $p^2 \mid k$ and $p \mid t$, we arrive to an equation of the form $x^2+y^2=x^2+2xt+t^2-k$ with a few possibilities for common divisors of k and t listed below.

Lemma 11. *For every common prime factor p of k and t, (1) can be reduced to an equation of a similar form where k and t satisfy one of the following conditions*:

(1) $(k,t)=1$.

(2) $(k,t)=sp$ *where p does not divide s, p^2 does not divide k and $p^2 \mid t$.*

(3) $(k,t)=sp$ *where p does not divide s, p^2 does not divide k, and p^2 does not divide t.*

Therefore, without loss of generality, in solving (1) we may assume that k and t satisfy one of the conditions in Lemma 11.

We consider the cases for t odd and t even separately.

3.1. *Solutions to $x^2+y^2=(x+t)^2-k$ when t is odd.*

If t is odd and y is a variable, the solutions to $y^2 \equiv t^2-k \pmod{2t}$ and $y^2 \equiv -k \pmod{t}$ are related.

Lemma 12. *Suppose t is odd and k is an even integer. Then m is a solution to $y^2 \equiv t^2-k \pmod{2t}$ if and only if it is an odd solution to $y^2 \equiv -k \pmod{t}$.*

Proof. If m is a solution to $y^2 \equiv t^2-k \pmod{2t}$, then there exists $q \in \mathbb{Z}$ such that $m^2=-k+t(2q+t)$. Since t is odd and k is even, m is an odd solution to $y^2 \equiv -k \pmod{t}$. For the converse, note that if m is an odd solution to $y^2 \equiv -k \pmod{t}$, then m is a solution to $y^2 \equiv t^2-k \pmod{t}$. Since m^2-t^2+k is even and t is odd, m is a solution to $y^2 \equiv t^2-k \pmod{2t}$. □

In this case, if all solutions to $y^2 \equiv -k \pmod{t}$ are odd, then they all generate distinct solutions to $y^2 \equiv t^2-k \pmod{2t}$. However, if $y^2 \equiv -k \pmod{t}$ has an even solution v, then $v+t$ is an odd solution to $y^2 \equiv -k \pmod{t}$ and thus it is a solution to $y^2 \equiv t^2-k \pmod{t}$. That is, for $t=\prod_{i=1}^r p_i^{e_i}$, we can choose 2^r distinct solutions to the congruence $y^2 \equiv -k \pmod{t}$ to be odd, and they will generate 2^r distinct solutions to the congruence $y^2 \equiv t^2-k \pmod{2t}$.

Lemma 13. *Suppose t and k are odd integers. Then m is a solution to $y^2 \equiv t^2-k \pmod{2t}$ if and only if it is an even solution to $y^2 \equiv -k \pmod{t}$.*

Proof. If m is a solution to $y^2 \equiv t^2-k \pmod{2t}$, then m is even and there exists $q \in \mathbb{Z}$ such that $m^2=-k+t(2q+t)$. Since t and k are odd, m is an even solution to $y^2 \equiv -k \pmod{t}$. If m is an even solution to $y^2 \equiv -k \pmod{t}$, then m is a solution to $y^2 \equiv t^2-k \pmod{t}$. Now, m^2-t^2+k is even and t is odd, so m is a solution to $y^2 \equiv t^2-k \pmod{2t}$. □

Similarly, in this case, if all solutions to $y^2 \equiv -k \pmod{t}$ are even, then they all generate distinct solutions to $y^2 \equiv t^2-k \pmod{2t}$. However, if $y^2 \equiv t^2-k \pmod{t}$

has an odd solution v, then $v+t$ is an even solution to $y^2 \equiv -k \pmod{t}$ and thus is a solution to $y^2 \equiv t^2 - k \pmod{2t}$. Similar to the previous case, we can generate 2^r distinct solutions to the congruence $y^2 \equiv t^2 - k \pmod{2t}$ by choosing enough even solutions to $y^2 \equiv -k \pmod{t}$.

Therefore, when t is odd, solving the congruence $y^2 \equiv -k \pmod{t}$ is critical in solving (1). We study the cases of $(k,t) \neq 1$ and $(k,t) = 1$ separately.

Lemma 14. *Let $t = \prod_{i=1}^{r} p_i^{e_i}$ be the prime factorization of t. Consider the equation $x^2 + y^2 = (x+t)^2 - k$:*

(1) *If $(k,t) = sp$ and p does not divide s, p^2 does not divide k, and $p^2 \mid t$, for some common prime factor p of k and t, then the equation has no solution.*

(2) *If the above case does not hold for any common prime factor of k and t, and there exists a prime p such that $(k,t) = sp$, p does not divide s, p^2 does not divide k, and p^2 does not divide t, then the equation has a solution if and only if every congruence $y^2 \equiv -k \pmod{p_i^{e_i}}$ with $p_i \neq p$ has a solution of the form $y \equiv 0 \pmod{p}$.*

Proof. (1) In this case, one of the congruences obtained from the congruence $y^2 \equiv -k \pmod{t}$ is equivalent to $y^2 \equiv -k_1 p \pmod{p^2}$, where $(k_1, p) = 1$. Using Proposition 4, this congruence has no solution, which implies that (1) has no solution.

(2) In this case, one of the congruences obtained from the congruence $y^2 \equiv -k \pmod{t}$ is equivalent to $y^2 \equiv -k_1 p \pmod{p}$. Using Proposition 4, this congruence always has a solution, namely $y \equiv 0 \pmod{p}$. Since $y^2 \equiv -k \pmod{t}$ has a solution if and only if each of the congruences $y^2 \equiv -k \pmod{p_i^{e_i}}$ with $p_i \neq p$ for all other prime divisors of t has a solution, the result follows. □

Now consider the case where $(k,t) = 1$ and t is odd.

Using Lemma 5, if $t = \prod_{i=1}^{r} p_i^{e_i}$ is an odd integer, then the congruence $y^2 \equiv -k \pmod{t}$ is equivalent to the system of congruences

$$\begin{aligned} y^2 &\equiv -k \pmod{p_1^{e_1}}, \\ y^2 &\equiv -k \pmod{p_2^{e_2}}, \\ &\vdots \\ y^2 &\equiv -k \pmod{p_r^{e_r}}. \end{aligned}$$

That is, if one of the above congruences does not have a solution, then the congruence $y^2 \equiv -k \pmod{t}$ has no solution. Now, if all of the above congruences have solutions, then each congruence can be replaced by a linear congruence, and the resulting system of congruences can be solved using the Chinese remainder theorem.

The following is a consequence of Lemmas 8, 12, and 13.

Corollary 15. *If $t=p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$, where $p_1,p_2,\dots,p_r$ are distinct odd primes and $r,e_i\in\mathbb{N}$, then $y^2\equiv t^2-k \pmod{2t}$ has 2^r distinct solutions for y if $-k$ is a quadratic residue modulo p_i for each p_i, $i=1,2,\dots,r$, and no solution otherwise.*

Theorem 16. *Suppose t is odd and k is an integer with $(k,t)=1$. The equation $x^2+y^2=(x+t)^2-k$ has integer solutions x, y, t if and only if $-k$ is a quadratic residue modulo p_i for every prime divisor p_i of t. For any such t, there are infinitely many solutions.*

Proof. Suppose $x^2+y^2=(x+t)^2-k$ has integer solutions x, y, t. Then, $y^2\equiv t^2-k \pmod{2t}$, so by Corollary 15, $-k$ is a quadratic residue modulo every prime divisor of t.

Now, suppose $t=p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$ where $-k$ is a quadratic residue of every p_i. By Corollary 15, $y^2\equiv t^2-k \pmod{2t}$ has 2^r distinct solutions. Let m be such a solution that is also a least residue of y modulo $2t$. Now, x, y, t with $y=m+2tq$, $x=(y^2-t^2+k)/(2t)$, is a solution to the equation $x^2+y^2=(x+t)^2-k$ for all $q\in\mathbb{Z}$. Therefore, for any such t, there are infinitely many solutions. □

The above results give an algorithm for computing the solutions to the equation $x^2+y^2=(x+t)^2-k$ when t is odd. To illustrate this algorithm, we present an example for each of the cases $k\equiv 0,1,2,3 \pmod 4$. For this we consider $k=12,5,6,15$, respectively.

3.1.1. *Examples for $k\equiv 0,1,2,3 \pmod 4$.* For the case $k\equiv 0 \pmod 4$, consider the example $k=12$. That is, we want to solve $x^2+y^2=(x+t)^2-12$ when t is odd and has a prime factorization $t=\prod_{i=1}^r p_i^{e_i}$. Since t is odd, the only possibilities for $(12,t)$ are 3 and 1. First we consider $(12,t)=3$. Using Lemma 14, if $9\mid t$, then there is no solution to the equation; if 9 does not divide t, then there is a solution to the equation if and only if $y\equiv 0 \pmod 3$ and $y^2\equiv -12 \pmod{p_i^{e_i}}$ has a solution for each $p_i\neq 3$, $i=1,2,\dots,r$. Since $(12,p_i)=1$ for $p_i\neq 3$, the latter congruence is equivalent to finding whether or not -12 is a quadratic residue modulo each $p_i^{e_i}$; this can be done using Euler's criterion or quadratic reciprocity. The result for each congruence will be a linear congruence and then the Chinese remainder theorem can be used. Now, consider the case $(12,t)=1$.

The parity of t depends on the parity of x and the parity of y as follows:

- If both x and y are even, then $x^2+y^2\equiv 0 \pmod 4$. This leads to $(x+t)^2\equiv 0 \pmod 4$, which implies that t is even.
- If x and y are both odd, then $x^2+y^2\equiv 2 \pmod 4$. Then $(x+t)^2\equiv 2 \pmod 4$, which is a contradiction since no square is congruent to 2 modulo 4.
- If x and y are of opposite parity, then $x^2+y^2\equiv 1 \pmod 4$. This implies that $(x+t)^2\equiv 1 \pmod 4$, meaning that x and t are of opposite parity.

Proposition 17. (i) *If $p \neq 3$ is an odd prime, then $s^2 \equiv -12 \pmod{p}$ has exactly two distinct solutions if $p \equiv 1 \pmod{6}$ and no solution otherwise.*

(ii) *If $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, where $p_1, p_2, \dots, p_r$ are distinct odd primes, all greater than 3, and $r, e_i \in \mathbb{N}$, then $s^2 \equiv -12 \pmod{t}$ has 2^r distinct solutions if $p_i \equiv 1 \pmod{6}$ for each $i = 1, 2, \dots, r$, and no solution otherwise.*

Proof. (i) First suppose $s^2 \equiv -12 \pmod{p}$ has exactly two distinct solutions. Since $(4/p) = (2^2/p) = 1$,

$$\left(\frac{-12}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{4}{p}\right)=1 \quad\Longrightarrow\quad \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=1.$$

We consider the two cases $(-1/p) = (3/p) = 1$ and $(-1/p) = (3/p) = -1$:

(1) $(-1/p) = (3/p) = 1$. Then, using (2) and (4), we get one of the following:

- (i) $p \equiv 1 \pmod{4}$ and $p \equiv 1 \pmod{12}$. These congruences imply $p \equiv 1 \pmod{2}$ and $p \equiv 1 \pmod{3}$, respectively. By the Chinese remainder theorem $p \equiv 1 \pmod{6}$.
- (ii) $p \equiv 1 \pmod{4}$ and $p \equiv 11 \pmod{12}$, which is impossible.

(2) $(-1/p) = (3/p) = -1$. Then, using (2) and (4), we get one of the following:

- (i) $p \equiv 3 \pmod{4}$ and $p \equiv 5 \pmod{12}$, which is impossible.
- (ii) $p \equiv 3 \pmod{4}$ and $p \equiv 7 \pmod{12}$. These congruences imply $p \equiv 1 \pmod{2}$ and $p \equiv 1 \pmod{3}$, respectively. By the Chinese remainder theorem, $p \equiv 1 \pmod{6}$.

For the converse, suppose $p \equiv 1 \pmod{6}$. Then either $p \equiv 1 \pmod{12}$, which implies $(-12/p) = (-1/p)(3/p)(4/p) = (1)(1)(1) = 1$, or $p \equiv 7 \pmod{12}$, which implies $(-12/p) = (-1/p)(3/p)(4/p) = (-1)(-1)(1) = 1$. In either case, $s^2 \equiv -12 \pmod{p}$ has exactly two distinct solutions.

(ii) If $r = 1$, then the result follows from the Case (1). For $r > 1$, suppose that for $i = 1, 2, \dots, r$, the prime p_i is congruent to 1 modulo 6. Then the result follows from the Case (1) and Lemma 8. For the converse, suppose $s^2 \equiv -12 \pmod{t}$ has exactly 2^r distinct solutions. Then each congruence $s^2 \equiv -12 \pmod{p_i}$, $i = 1, 2, \dots, r$, has a solution and by the Case (1), p_i is congruent to 1 modulo 6 for all $i = 1, 2, \dots, r$. □

Also, if $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ where $p_1, p_2, \dots, p_r$ are distinct odd primes and $r, e_i \in \mathbb{N}$, then $s^2 \equiv t^2 - 12 \pmod{2t}$ has 2^r distinct solutions if each $p_i \equiv 1 \pmod{6}$ and no solution otherwise.

Proposition 18. *Let t be an odd number with $(12, t) = 1$. The equation $x^2 + y^2 = (x + t)^2 - 12$ has integer solutions for x, y, t if and only if every prime divisor of t is congruent to 1 modulo 6. For any such t, there are infinitely many solutions.*

Proof. Note that $x^2+y^2=(x+t)^2-12$ implies that $y^2 \equiv t^2-12 \pmod{2t}$. Then by Lemma 12 and Proposition 17, every prime divisor of t is congruent to 1 modulo 6. For the converse, suppose $t=p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$ with $p_i \equiv 1 \pmod 6$ for all $i=1,2,\dots,r$. By Lemma 12 and Proposition 17, $y^2 \equiv t^2-k \pmod{2t}$ has 2^r distinct solutions. Let m be such a solution that is also a least residue of y modulo $2t$. Then, x, y, t with $y=m+2tq$, $x=(y^2-t^2+12)/(2t)$, is a solution to the equation $x^2+y^2=(x+t)^2-12$ for $q\in\mathbb{Z}$. Therefore, for any such t, there are infinitely many solutions. □

For the case $k\equiv 1 \pmod 4$, we consider $k=5$. In this case, $(5,t)$ equals 1 or 5. If $(5,t)=5$, and 25 does not divide t, then the equation has no solution. If $(5,t)=5$, and $25\mid t$, then the equation has a solution if and only if the following system of equations has a solution:

$$y\equiv 0 \pmod 5 \qquad\text{and}\qquad y^2\equiv -5 \pmod{p_i^{e_i}} \quad\text{for all } p_i\neq 5.$$

Similarly to the previous example, this system can be reduced to linear equations. We now consider the case $(5,t)=1$.

The next lemma can be obtained from Proposition 3.

Lemma 19. (i) *If $p\neq 5$ is an odd prime, then $s^2\equiv -5 \pmod p$ has exactly two distinct solutions if $p\equiv 1,3,7,9 \pmod{20}$ and no solution otherwise.*

(ii) *If $t=p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$ where $p_1,p_2,\dots,p_r$ are distinct odd primes, $p_i\neq 5$ for all $i=1,2,\dots,r$, and $r,e_i\in\mathbb{N}$, then $s^2\equiv -5 \pmod t$ has 2^r distinct solutions modulo t if each $p_i\equiv 1,3,7,9 \pmod{20}$ and no solution otherwise.*

We now have the following.

Proposition 20. *Suppose t is odd with $(5,t)=1$. The equation*

$$x^2+y^2=(x+t)^2-5$$

has integer solutions x, y, t if and only if every prime divisor of t is congruent to $1,3,7,9$ modulo 20. For any such t there are infinitely many solutions.

For the case $k\equiv 2 \pmod 4$ we consider $k=6$. In this case, since t is odd, we have either $(6,t)=3$ or $(6,t)=1$. If $9\mid t$, there is no solution; if 9 does not divide t, then the equation has a solution if and only if there is a solution to

$$y\equiv 0 \pmod 3 \quad\text{and}\quad y^2\equiv -6 \pmod{p_i^{e_i}} \text{ for all } p_i\neq 3.$$

Hence we consider the case when $(6,t)=1$. We shall use a lemma which follows from (3).

Lemma 21. (i) *If $p\neq 3$ is an odd prime, then $s^2\equiv -6 \pmod p$ has exactly two distinct solutions if $p\equiv 1,5,7,11 \pmod{24}$ and no solution otherwise.*

(ii) *If* $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, *where* $p_1, p_2, \dots, p_r$ *are distinct odd primes*, $(6, t) = 1$ *and* $r, e_i \in \mathbb{N}$, *then* $s^2 \equiv -6 \pmod{t}$ *has* 2^r *distinct solutions modulo* t *if each* $p_i \equiv 1, 5, 7, 11 \pmod{24}$ *and no solution otherwise.*

Proposition 22. *The equation* $x^2 + y^2 = (x + t)^2 - 6$ *with* $(t, 6) = 1$ *has integer solutions* x, y, t *if and only if every prime divisor of* t *is congruent to* $1, 5, 7, 11$ *modulo* 24. *For any such* t *there are infinitely many solutions.*

Finally, $k = 15$ is considered as an example for the case $k \equiv 3 \pmod{4}$. The cases when $(15, t) = 3, 5, 15$ are similar to the previous examples. We only consider the case when $(15, t) = 1$.

Lemma 23. (i) *If* $p \geq 7$ *is an odd prime, then* $s^2 \equiv -15 \pmod{p}$ *has exactly two distinct solutions if* $p \equiv 1, 7, 17, 19, 23, 31, 43, 47, 49, 53 \pmod{60}$ *and no solution otherwise.*

(ii) *If* $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ *where* $p_1, p_2, \dots, p_r$ *are distinct odd primes*, $(15, t) = 1$, *and* $r, e_i \in \mathbb{N}$, *then* $s^2 \equiv -15 \pmod{t}$ *has* 2^r *distinct solutions modulo* t *if each* p_i *is congruent to* $1, 7, 17, 19, 23, 31, 43, 47, 49, 53$ *modulo* 60, *and no solution otherwise.*

Proposition 24. *The equation* $x^2 + y^2 = (x + t)^2 - 15$ *with* $(15, t) = 1$ *has integer solutions* x, y, t *if and only if every prime divisor of* t *is congruent to* 1, 7, 17, 19, 23, 31, 43, 47, 49, 53 *modulo* 60. *For any such* t *there are infinitely many solutions.*

3.2. *Solutions to* $x^2 + y^2 = (x + t)^2 - k$ *when* t *is even.*

Now we consider the equation $x^2 + y^2 = (x + t)^2 - k$ when t is even.

Proposition 25. *Let* k, t *be integers and suppose* t *is even. Then* m *is a solution to the congruence* $y^2 \equiv t^2 - k \pmod{2t}$ *if and only if it is a solution to the congruence* $y^2 \equiv -k \pmod{2t}$.

Proof. Note that since t is even, $2t \mid t^2$. Now, m is a solution for $y^2 \equiv t^2 - k \pmod{2t}$ if and only if $2t \mid (m^2 - t^2 + k)$ if and only if $2t \mid (m^2 + k)$. □

Thus, in this section our focus is on congruences of the form $y^2 \equiv t^2 - k \pmod{2t}$. We first show that when $p = 2$, there is no solution to (1) in Case (2) or Case (3) of Lemma 11.

Lemma 26. *Consider integers* k, t:

(1) *If* $2 \mid (k, t)$ *but* 4 *does not divide* k, *and* $4 \mid t$, *then the congruence* $y^2 \equiv -k \pmod{2t}$ *has no solution.*

(2) *If* $2 \mid (k, t)$ *but* 4 *divides neither* k *nor* t, *then the congruence* $y^2 \equiv -k \pmod{2t}$ *has no solution.*

Proof. (1) Suppose $k=2\alpha$ and $t=4\beta$ for some integers α and β, where α is odd. The congruence $y^2\equiv -k \pmod{2t}$ has a solution if and only if there exist integers m, q such that $m^2=-2(\alpha+4\beta q)$. This is not possible since $\alpha+4\beta q$ is odd.

(2) Suppose $k=2\alpha$ and $t=2\beta$ for some odd integers α and β. As above, the congruence $y^2\equiv -k \pmod{2t}$ has a solution if and only if there exist integers m, q such that $m^2=-2(\alpha+2\beta q)$. This is not possible since $\alpha+2\beta q$ is odd. □

If 2 does not divide (k,t) but $(k,t)\neq 1$, the same argument as the case of t odd can be used. Thus, without loss of generality, we can assume that $(k,t)=1$. This implies that k is odd. Let $t=2^r s$ where $r\in\mathbb{N}$ and $s=\prod_{i=1}^{u} p_i^{e_i}$ is an odd integer. Since $(2^{r+1},s)=1$, using Lemma 5, the congruence $y^2\equiv -k \pmod{2t}$ can be reduced to two congruences:

$$y^2\equiv -k \pmod{2^{r+1}},\quad \text{and}\quad y^2\equiv -k \pmod{s}.$$

The congruence $y^2\equiv -k \pmod{s}$ can be solved using the results from the previous section. We now consider different cases for r for the remaining congruence $y^2\equiv -k \pmod{2^{r+1}}$.

The following result can be found in most number theory books; see [Kumanduri and Romero 1998, p. 231] for example. We restate it using the notation used in this work.

Lemma 27 [Kumanduri and Romero 1998, p. 231]. *Suppose k is odd and $r\geq 1$. Consider the congruence*

$$y^2\equiv -k \pmod{2^{r+1}}. \tag{7}$$

(1) *If $r=1$, the congruence* (7) *has exactly two distinct solutions if $-k\equiv 1 \pmod{4}$ and no solution otherwise.*

(2) *If $r\geq 2$, the congruence* (7) *has exactly four distinct solutions if $-k\equiv 1 \pmod{8}$ and no solution otherwise. If y_0 is a solution, then $-y_0$ and $\pm y_0+2^r$ are also solutions.*

An application of the above results can solve (1) when t is even, as follows.

Theorem 28. *Assume k is odd and consider* (1) *with $t=2^r s$, where s is an odd integer and $r>0$:*

(1) *If $r=1$, then* (1) *has a solution if and only if $-k\equiv 1 \pmod{4}$ and $y^2\equiv -k \pmod{s}$ has a solution.*

(2) *If $r\geq 2$, then* (1) *has a solution if and only if $-k\equiv 1 \pmod{8}$ and $y^2\equiv -k \pmod{s}$ has a solution.*

In each case, if there is one solution, there are infinitely many solutions.

Proof. Using Proposition 25, we know that $x^2+y^2=(x+t)^2-k$ has a solution if and only if $y^2 \equiv -k \pmod{2t}$ has a solution. The conditions for the existence of a solution in each case follow from Lemma 27 and the discussion preceding it. Now, suppose m is a solution to $y^2 \equiv -k \pmod{2t}$. Using Proposition 25, we see that it is also a solution to $y^2 \equiv t^2-k \pmod{2t}$. Thus, the triple (x, y, t) with $y=m+2tq$, $x=(y^2-t^2+k)/(2t)$, is a solution to the equation $x^2+y^2=(x+t)^2-k$ for all $q \in \mathbb{Z}$. Since q can be chosen arbitrarily, there are infinitely many solutions. □

References

[Apostol 1976] T. M. Apostol, *Introduction to analytic number theory*, Springer, 1976. MR Zbl

[Ayoub 1984] A. B. Ayoub, "Integral solutions to the equation $x^2+y^2+z^2=u^2$: a geometrical approach", *Math. Mag.* **57**:4 (1984), 222–223. MR Zbl

[Catalan 1885] E. Catalan, "Questions d'analyse indéterminée", *Bull. Acad. Roy. Sci. Belgique* (3) **9** (1885), 531–534. JFM

[Frink 1987] O. Frink, "Almost Pythagorean triples", *Math. Mag.* **60**:4 (1987), 234–236. MR Zbl

[Kumanduri and Romero 1998] R. Kumanduri and C. Romero, *Number theory with computer applications*, Prentice Hall, Upper Saddle River, NJ, 1998. Zbl

[MacGillivray et al. 2008] G. MacGillivray, S. Nasserasr, D. D. Olesky, and P. van den Driessche, "Primitive digraphs with smallest large exponent", *Linear Algebra Appl.* **428**:7 (2008), 1740–1752. MR Zbl

[Nasserasr 2007] S. Nasserasr, *Primitive digraphs with smallest large exponent*, master's thesis, University of Victoria, 2007, available at http://hdl.handle.net/1828/184.

Received: 2016-07-27 Accepted: 2016-09-25

wbkboyer@uvic.ca
Deparment of Mathematics and Statistics, University of Victoria, P.O. Box 1700 STN CSC, Victoria BC V8W 2Y2, Canada

gmacgill@uvic.ca
Department of Mathematics and Statistics, University of Victoria, P.O. Box 1700 STN CSC, Victoria BC V8W 2Y2, Canada

laura.may.morrison@gmail.com
Department of Mathematics and Statistics, University of Victoria, P.O. Box 1700 STN CSC, Victoria BC V8W 2Y2, Canada

kieka@uvic.ca
Department of Mathematics and Statistics, University of Victoria, P.O. Box 3060 STN CSC, Victoria BC V8W 3R4, Canada

snasserasr@nova.edu
Department of Mathematics, Nova Southeastern University, Fort Lauderdale, FL 33324, United States

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

PRODUCTION

Silvio Levy, Scientific Editor

Cover: Alex Scorpan

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2017 is US $175/year for the electronic version, and $235/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2017 vol. 10 no. 5