Pell Equations and Pythagorean Triples with Constant Difference of Two Legs

By

Toru Ishihara

Professor Emeritus, The University of Tokushima

e-mail address: tostfeld@mb.pikara.ne.jp

(Received October 6, 2015. Revised October 8, 2015)

Abstract

A Pythagorean triple is composed of a pair of legs $a, b$ and a hypotenuse $c$, where $a, b, c$ are positive integers. For a given positive integer $q$, the group of Pythagorean triples whose legs have difference $q$ is called the $d_q$ group by H. Hosoya [3]. In the present paper, using some results about Pell equation, we investigate extensively the structure of $d_q$ group.

2000 Mathematics Subject Classification. Primary 11D09; Secondary 11R11.

1 Pythagorean Triples

If the lengths of the legs and hypotenuse of a rectangular triangle are respectively $a, b, c$, then $a^2 + b^2 = c^2$. When $a, b, c$ are integers, we say $(a, b, c)$ is a Pythagorean triple (briefly, Py-triple). If $a, b, c$ have no common factor, $(a, b, c)$ is called a primitive Py-triple (briefly, pPy-triple). In this paper, we mainly treat pPy-triples. A triple $(a, b, c)$ is a pPy-triple if and only if there are positive integers $m, n$ such that $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$, $m - n (= \ell)$ is a positive odd integer and $m, n$ have no common factor. We consider $(\ell, n)$ as a code of $(a, b, c)$.

For a given pPy-triples $(a, b, c)$, the difference of two legs is $|a - b| = |m^2 - n^2 - 2mn| = |\ell^2 - 2n^2|$. Put $q = |a - b|$, we have
$f^2 - 2n^2 = \pm q.$

pPy-triples whose two legs have difference $q$ form a family, which is called $d_q$ group by H. Hosoya [3].

F. Barning [1] and A. Hall [2] introduced three matrices generating pPy-triples. One of them is the following

(1.2) $A = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 3 & 3 \end{pmatrix}.$

Let $(a_0, b_0, c_0)$ be a pPy-triple and set $q_0 = a_0 - b_0$. By operating $A$ on the column vector $(a_0, b_0, c_0)^T$, we get $(a_1, b_1, c_1)^T = A(a_0, b_0, c_0)^T$. Then, $(a_1, b_1, c_1)$ is also a pPy-triple and $q_1 = a_1 - b_1 = -q_0$. In general, put $(a_k, b_k, c_k)^T = A^k(a_0, b_0, c_0)^T$ and $q_k = a_k - b_k$ for each integer $k(\geq 0)$. Then, $(a_k, b_k, c_k)$ is a pPy-triple and $q_k = -q_{k-1} = (-1)^kq_0$. Hence, each $(a_k, b_k, c_k)$ belongs to $d_{|q_0|}$ group. Moreover, we have

(1.3) $\begin{pmatrix} \ell_k \\ n_k \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}^k \begin{pmatrix} \ell_0 \\ n_0 \end{pmatrix}.$

2 Pell equations

Since the expression (1.1) can be regarded as a Pell equation $x^2 - 2y^2 = \pm q$, we need some facts about this equation. Firstly, we begin with a general Pell equation

(2.1) $x^2 - ay^2 = \pm q,$

where $a$ is a positive integer, not a square and $q$ is a positive integer. We deal with numbers of the form $x + y\sqrt{a}$, where $x, y$ are integers. The set of these numbers is denoted as $Z[\sqrt{a}]$. The conjugate of number $z = x + y\sqrt{a}$ is defined as $\bar{z} = x - y\sqrt{a}$, and its norm as $N(z) = z\bar{z} = x^2 - ay^2$. In terms of these concepts, the equation (2.1) can be rewritten

$$N(z) = \pm q, \quad z = x + y\sqrt{a} \in Z[\sqrt{a}].$$

We use often this expression and $z$ is considered as a solution of the equation. If, for a solution $z = x + y\sqrt{a}$ of Pell equation, $x, y$ have no common factor, the solution is called primitive. If $x > 0, y > 0$, $z = x + y\sqrt{a}$ is called positive. The Pell equation $N(z) = 1$ has always solutions and the trivial solution is $z = 1$. 
The minimum solution \( z_1 = x_1 + y_1 \sqrt{a} \) with \( x_1 > 0, y_1 > 0 \) is said to be its fundamental solution. Any solution of \( N(z) = 1 \) is expressed as \( \pm z_1^k \) or \( \pm z_1^k \). As the equation \( N(z) = -1 \) do not always have solutions, in the sequel, we always consider the case when \( N(z) = -1 \) has solutions. The minimum solution \( z_0 = x_0 + y_0 \sqrt{a} \) with \( x_0 > 0, y_0 > 0 \) of \( N(z) = -1 \) is also called as its fundamental solution. It is known that \( z_0^2 = z_1 \). When \( a = 2 \), \( N(z) = -1 \) has solutions, and \( z_0 = 1 + \sqrt{a} \), \( z_1 = z_0^2 = 3 + 2 \sqrt{a} \). Any solution of \( N(z) = -1 \) is expressed as \( \pm z_0^k \) or \( \pm z_0^k \).

Moreover, we assume that the equation (2.1) has solutions. If \( z \) is a solution of (2.1), for any integer \( k \), \( z z_0^k \) is also its solution. We introduce an equivalent relation on all of solutions of (2.1) as follows. When \( \alpha, \beta \) are solutions of (2.1), \( \alpha \) is equivalent with \( \beta \) if and only if \( \alpha = \beta z \) for some solution \( z \) of \( N(z) = -1 \). All solutions of (2.1) are divided into classes under this equivalent relation. We call these classes \( z_0-\text{classes} \). Similarly, another equivalent relation is defined by \( \alpha = \beta z \) for some solution \( z \) of \( N(z) = 1 \), and this relation gives equivalent classes, which are called \( z_1-\text{classes} \). A \( z_0-\text{class} \) \( S \) is divided into two \( z_1-\text{classes} \), a set \( S_+ \) of solutions of \( N(z) = q \) and a set \( S_- \) of solutions of \( N(z) = -q \). Each \( z_0-\text{class} \) contains a solution \( \alpha = x_\alpha + y_\alpha \sqrt{a} \) with least possible \( y_\alpha \geq 0 \) in the class. We call it minimal in the class. Each \( z_1 \) class has a solution with similar property, which we call \( z_1-\text{minimal} \) in the class. The minimal solution of a \( z_0-\text{class} \) \( S \) is the smaller \( z_1-\text{minimal} \) solution of two \( z_1-\text{classes} \) \( S_+, S_- \). Let \( \beta = x_\beta + y_\beta \sqrt{a} \) be a solution in a \( z_0-\text{class} \) with \( x_\beta > 0 \) and least possible \( y_\beta > 0 \). We call \( \beta \) the fundamental solution of the class. The following is well known (for example, [5] p299-300).

**Theorem A.** Let \( \alpha = x_\alpha + y_\alpha \sqrt{a} \) be the \( z_1-\text{minimal} \) solution of a \( z_1-\text{class} \). We have

\[
\sqrt{q} \leq |x_\alpha| \leq \sqrt{\frac{(x_1 + 1)q}{2}}, \quad 0 \leq y_\alpha \leq y_1 \sqrt{\frac{q}{2(x_1 + 1)}},
\]

if \( N(\alpha) = q \), and

\[
0 \leq |x_\alpha| \leq \sqrt{\frac{(x_1 - 1)q}{2}}, \quad \sqrt{\frac{q}{a}} \leq y_\alpha \leq y_1 \sqrt{\frac{q}{2(x_1 - 1)}},
\]

if \( N(\alpha) = -q \), where \( z_1 = x_1 + y_1 \sqrt{a} \) is the fundamental solution of \( N(z) = 1 \).

Firstly, we show

**Lemma 1.** Let \( S \) be a \( z_0-\text{class} \) with \( S = S_+ \cup S_- \) such that \( \alpha = x_\alpha + y_\alpha \sqrt{a} \) with \( x_\alpha > 0, y_\alpha \geq 0 \) is \( z_1-\text{minimal} \) in \( S_+ \). Put \( \beta = x_\beta + y_\beta \sqrt{a} = z_0 \bar{\alpha} \), where \( z_0 \) is the fundamental solution of \( N(z) = -1 \). Then, \( x_\beta \geq 0, \ y_\beta > 0 \) and \( -\bar{\beta} \) is \( z_1-\text{minimal} \) in \( S_- \). If \( \alpha \) and \( \bar{\alpha} \) belong the same class, the class is called
ambiguous. If $S$ is not ambiguous, there is another $z_0$–class $S = \bar{S}_+ \cup \bar{S}_-$ such that $-\bar{\alpha}$ is $z_1$–minimal in $\bar{S}_+$ and $\beta$ is $z_1$–minimal in $\bar{S}_-$.

$y_\alpha$ and $y_\beta$ satisfy

$$(2.2) \quad y_\alpha \leq y_\beta \iff 0 \leq y_\alpha \leq y_0 \sqrt{\frac{q}{2x_0}}$$

Conversely, let $S$ be a $z_0$–class with $S = S_+ \cup S_-$ such that $\beta = x_\beta + y_\beta \sqrt{a}$ with $x_\beta \geq 0$, $y_\beta > 0$ is $z_1$–minimal in $S_-$. Put $\alpha = x_\alpha + y_\alpha \sqrt{a} = -z_0 \bar{\beta}$. Then, $x_\alpha > 0$, $y_\beta \geq 0$ and $-\bar{\alpha}$ is $z_1$–minimal in $\bar{S}_+$. If the class is not ambiguous, there is another $z_0$–class $S = S_+ \cup S_-$ such that $\alpha$ is $z_1$–minimal in $S_+$ and $-\bar{\beta}$ is $z_1$–minimal in $\bar{S}_-$.

Proof. Firstly, we show $y_\beta = y_0 x_\alpha - x_0 y_\alpha > 0$. As

$$y_0^2 x_\alpha^2 = a y_0^2 y_\alpha^2 + q y_0^2 > y_\alpha^2 (a y_0^2 - 1) = x_0^2 y_\alpha^2$$

we get $y_0 x_\alpha - x_0 y_\alpha > 0$. Next, we show $x_\beta = x_0 x_\alpha - a y_0 y_\alpha \geq 0$. From

$$0 \leq y_\alpha \leq \frac{x_0 y_0 \sqrt{q}}{\sqrt{x_0^2 + 1}},$$

it follows

$$y_\alpha^2 \leq \frac{x_0^2 y_0^2 q}{x_0^2 + 1}.$$ 

Hence, we get

$$x_0^2 x_\alpha^2 = (ay_0^2 - 1)(ay_\alpha^2 + q)$$

$$\geq a^2 y_0^2 y_\alpha^2 + q y_0^2 - a \frac{y_0^2 y_\alpha^2 q}{x_0^2 + 1} - q$$

$$= a^2 y_0 y_\alpha y_\alpha^2 + q \left( \frac{a y_0^2}{x_0^2 + 1} - 1 \right) = a^2 y_0^2 y_\alpha^2,$$

which shows $x_\beta = x_0 x_\alpha - a y_0 y_\alpha \geq 0$.

Next, we show $-\bar{\beta}$ is $z_1$–minimal in $\bar{S}_-$. If this is true, $\bar{\beta}$ is also $z_1$–minimal in $\bar{S}_-$, when $S$ is not ambiguous. Assume $-\bar{\beta}$ is not $z_1$–minimal. Then, there is a solution $\gamma = x_\gamma + y_\gamma \sqrt{a}$ with $0 < y_\gamma < y_\beta$ such that $\gamma = \pm z_0^k(\bar{\beta})$ or $\gamma = \pm z_0^{2k}(-\beta)$ for some $k \geq 1$, where $\pm$ means $+$ or $-$. When $\gamma = \pm z_0^{2k}(\bar{\beta})$, as $z_0(-\beta) = \alpha$, we have $\gamma = \pm z_0^{2k-2} z_0(-\beta) = \pm z_0^{2k-2} z_0 \alpha$. In this case, $\pm$ must be $+$, and we get $y_\gamma \geq y_0 x_\alpha + x_0 y_\alpha \geq y_0 x_\alpha - x_0 y_\alpha = y_\beta$, a contradiction. Hence, it holds $\gamma = \pm z_0^{2k}(-\bar{\beta})$. Put $z_0^{2k} = X - Y \sqrt{a}$. Then, we have $\gamma = \pm (X - Y \sqrt{a})(-x_\beta + y_\beta \sqrt{a}) = \pm (-X x_\alpha + a Y y_\alpha) + (Y x_\alpha + X y_\alpha) \sqrt{a})$. This means $\pm = +$, and we get $y_\gamma = X x_\beta + X y_\beta > y_\beta$, a contradiction.

We get (2.2) from the following
\[ y_\alpha \leq y_\beta = y_0 x_\alpha - x_0 y_\alpha \]
\[ \Leftrightarrow (1 + x_0) y_\alpha \leq y_0 x_\alpha \]
\[ \Leftrightarrow (x_0 + 1)^2 y_\alpha^2 \leq y_0^2 x_\alpha^2 = y_0^2 (a y_\alpha^2 + q) \]
\[ \Leftrightarrow (x_0^2 + 1)^2 y_\alpha^2 \leq (x_0^2 + 1) y_\alpha^2 + y_0^2 q \]
\[ \Leftrightarrow 2 x_0 y_\alpha^2 \leq y_0^2 q. \]

Now, we prove the converse statement. From

\[ a^2 y_\alpha^2 y_\beta^2 = (x_0^2 + 1)(x_\beta^2 + q) > x_0^2 x_\beta^2 \]

if follows \( x_\alpha = a y_0 y_\beta - x_1 x_\beta > 0 \). We know, from Theorem A

\[ y_\beta \leq y_1 \sqrt{\frac{q}{2(x_1 - 1)}} = y_0 \sqrt{q}. \]

The following calculation

\[ x_0^2 y_\beta^2 - y_0^2 x_\beta^2 = (a y_0^2 - 1) y_\beta^2 - y_0^2 x_\beta^2 \]
\[ = y_0^2 (a y_\beta^2 - x_\beta^2) - y_\beta^2 \]
\[ = y_0^2 q - y_\beta^2 \geq 0 \]

implies \( y_\alpha = x_0 y_\beta - y_0 x_\beta \geq 0 \).

Next, we show \(-\alpha\) is \(z_1\)-minimal in \(S_+\). If this is true, \(\alpha\) is also \(z_1\)-minimal in \(\bar{S}_+\), when \(S\) is not ambiguous. Assume \(-\alpha\) is not \(z_1\)-minimal. Then, there is a solution \(\gamma = x_\gamma + y_\gamma \sqrt{a}\) with \(0 < y_\gamma < y_\alpha\), such that \(\gamma = \pm z_0^{2k} (-\alpha)\) or \(\gamma = \pm z_0^{2k} (-\bar{\alpha})\) for some \(k \geq 1\). If \(\gamma = \pm z_0^{2k} (-\bar{\alpha})\), as \(z_0(\bar{\alpha}) = \beta\), we have \(\gamma = \pm z_0^{2k} (-\beta)\). In this case, \(\pm\) must be \(-\), and we get \(y_\gamma \geq y_0 x_\beta + x_0 y_\beta \geq x_0 y_\beta - y_0 x_\beta = y_\alpha\), a contradiction. Hence, it holds \(\gamma = \pm z_0^{2k} (-\alpha)\). But, as before, this also leads to a contradiction.

From Lemma 1, we obtain

**Theorem 1.** Let \(S\) be a \(z_0\)-class with \(S = S_+ \cup S_-\) such that \(\alpha = x_\alpha + y_\alpha \sqrt{a}\) with \(x_\alpha > 0, y_\alpha \geq 0\) is \(z_1\)-minimal in \(S_+\). Put \(\beta = x_\beta + y_\beta \sqrt{a} = z_0 \bar{\alpha}\).

(1) If \(y_\alpha = 0\), then, \(\alpha = \bar{\alpha}\) and \(S\) is ambiguous. \(\alpha = \sqrt{q}\) is minimal in \(S\) and \(\beta = \sqrt{q} x_0 + \sqrt{q} y_0 \sqrt{a}\) is the fundamental solution of \(S\). If \(q > 1\), \(\beta\) is not primitive.

(2) If \(0 < y_\alpha \leq y_0 \sqrt{\frac{q}{2 x_0}}\), \(\alpha\) is minimal in \(S\) and also its fundamental solution. If \(S\) is not ambiguous, \(-\bar{\alpha}\) is minimal in \(\bar{S}\) and \(\beta\) is its fundamental solution.
(3) If \( y_0 \sqrt{\frac{q}{2x_0}} < y_\alpha \leq y_1 \sqrt{\frac{q}{2(x_1 + 1)}} = \frac{x_0 y_0 \sqrt{q}}{x_0^2 + 1} \), \( y_\beta \) is minimal in \( S \) and \( \alpha \) is its fundamental solution. If \( S \) is not ambiguous, \( y_\beta \) is minimal in \( \bar{S} \) and also its fundamental solution.

When \( a = 2 \), as we have \( z_0 = 1 + \sqrt{2} \), \( z_1 = 3 + 2\sqrt{2} \), it holds \( y_0 \sqrt{\frac{q}{2x_0}} = \sqrt{\frac{q}{2}} = y_1 \sqrt{\frac{q}{2(x_1 + 1)}} \). Hence, only the case (2) in Theorem 1 occurs. Thus, we get

**Corollary.** Let \( S \) be a \( z_0 \)-class of the solutions of Pell equation \( x^2 - 2y^2 = \pm q \). Let \( \alpha = x_\alpha + y_\alpha \sqrt{q} \) be minimal in \( S \). Then we have

\[
\sqrt{q} \leq |x_\alpha| \leq \sqrt{2q}, \quad 0 \leq y_\alpha \leq \frac{\sqrt{q}}{2}.
\]

If \( x_\alpha > 0 \), \( \alpha \) is also the fundamental solution of \( S \). If \( x_\alpha < 0 \), the fundamental solution of \( S \) is \( -x_\alpha + y_\alpha \sqrt{q} \) or \( x_\alpha - 2y_\alpha + (x_\alpha - y_\alpha) \sqrt{q} \) according as \( S \) is ambiguous or not.

It is well known that a prime \( p \) completely decomposes in \( \mathbb{Q}(\sqrt{2}) \) if and only if \( p \equiv \pm 1(\mod 8) \). Since the class number of \( \mathbb{Q}(\sqrt{2}) \) is one, the ideal \( (p) \) of \( \mathbb{Q}(\sqrt{2}) \) decomposes into \( (p) = \varphi \bar{\varphi} \), where \( \varphi \) is a principal ideal \( \varphi = (a + b\sqrt{2}) \) with some integer \( a \) and \( b \). Since the norm function is multiplicative, the following is well known.

**Theorem B.** There exist primitive \( x, y \) such that \( x^2 - 2y^2 = \pm q \) if and only if each prime factor \( p \) of \( q \) satisfies \( p \equiv \pm 1(\mod 8) \).

**Lemma 2.** Let \( q \) satisfy the condition in Theorem B. A \( z_0 \)-class of the solutions of \( x^2 - 2y^2 = \pm q \) is ambiguous only when \( q \) is a square and \( \alpha = \sqrt{q} \) is contained in the class.

**Proof.** Let \( \alpha = x_\alpha + y_\beta \sqrt{2} \) be a solution in a \( z_0 \)-class \( S \). Assume that \( \bar{\alpha} \) is also contained in \( S \). As it does not occur that \( \bar{\alpha} = \pm z_0^k \alpha \), we have \( \bar{\alpha} = \pm \bar{z}_0^k \alpha \).

We can put \( k = 2m \) or \( k = 2m + 1 \). Set \( \pm z_0^k \alpha = X + Y \sqrt{2} \), which is also in \( S \). When \( k = 2m \), we have \( \pm (X + Y \sqrt{2}) = X - Y \sqrt{2} \). Hence, we get \( X = 0 \) or \( Y = 0 \). But as \( X \neq 0 \), we obtain \( Y = 0, X = \pm \sqrt{q} \). Thus, \( q \) must be a square and \( \sqrt{q} + 0\sqrt{2} \) is the minimal solution in \( S \).

From now on, we consider only positive solutions of Pell equation \( x^2 - 2y^2 = \pm q \). Let \( S \) be a \( z_0 \)-class of positive solutions and \( \alpha = x_\alpha + y_\alpha \sqrt{2} \) is the fundamental solution in \( S \). Any solution in \( S \) can be represented as \( z_0^k \alpha \). Put \( x_k + y_k \sqrt{2} = z_0^k \alpha \). Then we have
\[
\begin{pmatrix}
x_k \\
y_k
\end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}^k \begin{pmatrix} x_\alpha \\
y_\alpha
\end{pmatrix}
\]

This is the same relation as (1.3). Hence, if \((x_\alpha, y_\alpha)\) is primitive, each \((x_k, y_k)\) is primitive. When \((x_k, y_k)\) is primitive, \(x_k\) must be a odd. From Theorem B, Corollary and Lemma 2, we obtain

**Theorem 2.** There exists \(d_q\) group if and only if \(q \equiv \pm 1 \pmod{8}\), where any prime factor \(p\) of \(q\) satisfies \(p \equiv \pm 1 \pmod{8}\). Assume that \(q\) satisfies this condition. Let \((\ell_i, n_i),\ 1 \leq i \leq j\) be all pairs of positive integers such that

\[
\ell_i^2 - 2n_i^2 = \pm q, \quad \sqrt{q} \leq \ell_i \leq \sqrt{2q}, \quad 0 < n_i \leq \sqrt{q/2},
\]

and \(\ell_i\) is a odd and \(\ell_i\) and \(n_i\) have no common factor. Let \(P(2i - 1),\ P(2i)\) be the column vectors of the Pythagorean triples corresponding to \((\ell_i, n_i),\ (\ell_i - 2n_i, \ell_i - n_i)\) respectively. Then, we have

\[
d_q = \{ A^k P(i); \ 1 \leq i \leq 2j, \ 0 \leq k \},
\]

where \(A\) is the matrix of Barning and Hall given in (1.2).

**Remark.** We note this theorem covers the case \(q = 1\), because there exists no prime factor \(p\) for this case. For \(q = 1\), as \(\sqrt{1} \leq \ell \leq \sqrt{2}, \ 0 < n \leq \sqrt{2/2},\) we have \(\ell = 1, n = 1\). Hence, we get the Pythagorean triple \((5, 4, 3)\) corresponding to the pair \((1, 1)\).

**Examples.** We give some simple examples,

For \(q = 7\), as \(\sqrt{7} \leq \ell \leq \sqrt{14}, \ 0 < n \leq \sqrt{14}/2,\) we have \(\ell = 3, n = 1\). Hence, we get Pythagorean triples \((15, 8, 17), (5, 12, 13)\) corresponding to pairs \((3, 1), (1, 2)\) respectively.

For \(q = 17\), as \(\sqrt{17} \leq \ell \leq \sqrt{34}, \ 0 < n \leq \sqrt{34}/2,\) we have \(\ell = 5, n = 2\). Hence, we get \((45, 28, 53), (7, 24, 25)\) corresponding to pairs \((5, 2), (1, 3)\) respectively.

For \(q = 7 \times 17 = 119,\) as \(\sqrt{119} \leq \ell \leq \sqrt{238}, \ 0 < n \leq \sqrt{238}/2,\) we have \(\ell_1 = 11, n_1 = 1\) and \(\ell_2 = 13, n_2 = 5\). Hence, we get \((143, 24, 145), (261, 380, 461), (299, 180, 349), (57, 176, 185)\) corresponding to pairs \((11, 1), (9, 10), (13, 5), (3, 8)\) respectively.

For \(q = 161,\) as \(\sqrt{161} \leq \ell \leq \sqrt{322}, \ 0 < n \leq \sqrt{322}/2,\) we have \(\ell_1 = 13, n_1 = 2\) and \(\ell_2 = 17, n_2 = 8\). Hence, we get \((221, 60, 229), (279, 440, 521), (561, 400, 689), (19, 180, 181)\) corresponding to pairs \((13, 2), (9, 11), (17, 8), (1, 9)\) respectively.

**References**


