# ON A DIOPHANTINE EQUATION RELATED TO SYMMETRIC DESIGN

H. W. Lu, Harold Bowman, and Peter J.–S. Shiue

We investigate the following Diophantine equation

$$k(k-1) = \lambda(v-1), \tag{1}$$

where $\lambda$, $k$ and $v$ are positive integers, and $0 < \lambda < k < v-1$. This Diophantine equation arises in cyclic difference set and symmetric design ([1, 3]). We prove a result which allows us to efficiently determine solutions of the equation (Theorem 1). We also provide some applications.

Lemma 1. There is a simple parametric representation for the solutions of (1). For all positive integers $n \geq 2$ and all divisors $\lambda$ of $n(n-1)$ we have

$$\lambda \mid n(n-1), \text{ and let } k-\lambda = n, \text{ and } v = 2n + \lambda + \frac{n(n-1)}{\lambda}. \tag{2}$$

Proof. See Assmus and Key [1].

Theorem 1. There exists a one–to–one mapping from the set

$$C = \{(v,k,\lambda) \mid k^2 = k + \lambda(v-1),\ 0 < \lambda < k < v-1,\ v,k,\lambda \in \mathbb{N}\} \tag{3}$$

onto the set

$$SL_2(\mathbb{N}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, ad - bc = 1,\ a,b,c,d \in \mathbb{N} \right\}. \tag{4}$$

Proof. For $(v,k,\lambda) \in C$, with $n = k - \lambda \geq 2$. The mapping $\phi: C \to SL_2(\mathbb{N})$ is defined in the following manner. Let

$$a = \gcd(\lambda, k-\lambda),\ b = \gcd(\lambda, k-\lambda-1),\ d = \frac{k-\lambda}{a},\ c = \frac{k-\lambda-1}{b} \tag{5}$$

then we have

$$a, b, c, d \in \mathbb{N} \text{ and } ad - bc = 1, \tag{6}$$

i.e. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{N})$ is the image of $(v, k, \lambda) \in C$ in $SL_2(\mathbb{N})$ under the mapping $\phi$.

Now let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{N})$. Since $\gcd(k - \lambda, k - \lambda - 1) = 1$, using Lemma 1, we get

$$\lambda = ab,\ k = a(b+d) = b(a+c) + 1,\ v = 2ad + ab + cd = (a+c)(b+d) + 1. \tag{7}$$

Thus showing that $(v, k, \lambda)$ is determined uniquely by its image in $SL_2(\mathbb{N})$. Therefore, the mapping $\phi$ is one–to–one. On the other hand, for a given $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{N})$, let $(v, k, \lambda)$ be given by (7), then we have $\lambda(v - 1) - k(k - 1) = ab(a+c)(b+d) - a(b+d)b(a+c) = 0$, which shows that $(v, k, \lambda)$ is a solution of (1). Therefore, the mapping $\phi$ is from $C$ onto $SL_2(\mathbb{N})$.

Remark. Theorem 1 gives a very effective way to find solutions of (1). We first take any pair of relatively prime natural numbers $a$ and $b$. Since $(a, b) = 1$, there exists $c$ and $d \in \mathbb{N}$ such that $ad - bc = 1$. By substituting $a$, $b$, $c$ and $d$ into (7), we have a solution $(\lambda, k, v)$ of (1). Another approach for the solutions of (1) can be found in Assmus [2].

Example. Let $a = 5$, $b = 3$. Then there exists $d = 2$, $c = 3$ such that $5 \cdot 2 - 3 \cdot 3 = 1$.

Thus,

$$\begin{aligned} \lambda &= ab = 15 \\ k &= a(b+d) = 5 \cdot (3+2) = 25 \\ v &= 2ad + ab + cd = 2 \cdot 5 \cdot 2 + 5 \cdot 3 + 3 \cdot 2 = 41 \end{aligned}$$

is a solution of (1).

The following simple corollary is an immediate consequence of Theorem 1.

Corollary 1. Let $(v_i, k_i, \lambda_i)$ $(i = 1, 2)$ be two solutions of the following Diophantine equation

$$(8) \qquad k^2 = k + \lambda(v-1),\ 0 < \lambda < k < v-1,\ v, k, \lambda \in \mathbb{N}.$$

Then we can generate a third solution $(v, k, \lambda)$ of (1) from $(v_i, k_i, \lambda_i)$ $(i = 1, 2)$ by the following method. Let

$$a_i = \gcd(\lambda_i, k_i - \lambda_i),\ b_i = \gcd(\lambda_i, k_i - \lambda_i - 1),$$

$$(9) \qquad d_i = \frac{k_i - \lambda_i}{a_i},\ c_i = \frac{k_i - \lambda_i - 1}{b_i},\quad i = 1, 2,$$

then $a_i$, $b_i$, $c_i$, $d_i \in \mathbb{N}$ and $a_i d_i - b_i c_i = 1$, $i = 1, 2$. Let

$$(10) \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} d_2 & b_2 \\ c_2 & a_2 \end{pmatrix}.$$

Define:

$$(11)\ \lambda = ab,\ k = a(b+d) = b(a+c) + 1,\ v = (a+c)(b+d) + 1 = 2ad + ab + cd.$$

This gives a third solution $(v, k, \lambda)$ of (1).

Proof. Since $a_i d_i - b_i c_i = 1$ for $i = 1, 2$. Then $ad - bc = 1$. $k^2 = a^2b^2 + 2a^2bd + a^2d^2$ and $\lambda(v-1) = ab(ab + ad + cb + cd)$ by direct substitution we can see this is a solution for (1).

Definition 1. We call the solution $(v, k, \lambda)$ of (1) generated by $(v_i, k_i, \lambda_i)$ $(i = 1, 2)$ according to Corollary 1 as the multiplication of $(v_1, k_1, \lambda_1)$ and $(v_2, k_2, \lambda_2)$, and is denoted by

$$(v, k, \lambda) = (v_1, k_1, \lambda_1) \circ (v_2, k_2, \lambda_2).$$

Corollary 2.

$$(v,k,\lambda)^2 = (v,k,\lambda)\circ(v,k,\lambda) =$$

$$(2(v-1)(2(k-\lambda)-1),\ (2k-1)(2(k-\lambda)-1),\ 2\lambda(2(h-\lambda)-1)) \tag{12}$$

is also a solution of (1).

Proof. In this case, $a_2 = a_1 = a$, $b_2 = b_1 = b$, $c_2 = c_1 = c$, $d_2 = d_1 = d$. So we get

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} d_2 & b_2 \\ c_2 & a_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & b \\ c & a \end{pmatrix} = \begin{pmatrix} ad+bc & 2ab \\ 2cd & ad+bc \end{pmatrix},$$

which yields

$$(v,k,\lambda)^2 = (v,k,\lambda)\circ(v,k,\lambda) = (\hat{v},\hat{k},\hat{\lambda}).$$

Using (11), we have

$$\begin{aligned}
\hat{\lambda} &= 2ab(ad+bc) = 2ab(2ad-1) = 2\lambda(2(k-\lambda)-1),\\
\hat{k} &= (ad+bc)(ad+bc+2ab) = (2(k-\lambda)-1)(2(k-\lambda)-1+2\lambda)\\
&= (2(k-\lambda)-1)(2k-1),\\
\hat{v} &= 2(ad+bc)^2 + (ad+bc)(2ab+2cd)\\
&= 2(ad+bc)(ad+bc+ab+cd)\\
&= 2(2ad-1)(2ad-1+ab+cd) = 2(2(k-\lambda)-1)(v-1).
\end{aligned}$$

Thus, we have proved the corollary.

Examples.

1. $(4t-1,\ 2t-1,\ t-1)^2 = (4(2t-1)^2,\ (4t-3)(2t-1),\ 2(t-1)(2t-1)),\ 2 \le t \in \mathbb{N}$.
2. $(4s-1,\ 2s-1,\ s-1)\circ(4t-1,\ 2t-1,\ t-1) = (4(T-1)^2,\ (T-1)(2T-3),\ (T-1)(T-2))$, $T = s+t,\ 2 \le s,t \in \mathbb{N}$.
3. $(n^2+n+1,\ n+1,\ 1)^2 = (2(2n-1)(n+1)n,\ 4n^2-1,\ 4n-2),\ 2 \le n \in \mathbb{N}$.

4. $(n^2+n+1,\ n+1,\ 1)\circ(m^2+m+1,\ m+1,\ 1) = (m(2n+1)^2-(2n+3)n,\ (2m-1)(2n+1),\ 2(2m-1))$.

Proposition 1. The complement of $(v,k,\lambda)$ denoted by $(v',k',\lambda')$ is defined to be

$$v'=v,\ k'=v-k,\ \lambda'=v-2k+\lambda\ \ (k'-\lambda'=k-\lambda),$$

and when

$$(v,k,\lambda)\overset{\phi}{\mapsto}\begin{pmatrix} a & b\\ c & d\end{pmatrix}\quad\text{with}\quad\det\begin{pmatrix} a & b\\ c & d\end{pmatrix}=M,$$

then

$$(v',k',\lambda')\overset{\phi}{\mapsto}\begin{pmatrix} d & c\\ b & a\end{pmatrix}=\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix}M\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix}.$$

Proof. It is easy to see that

$$\begin{aligned} a' &= \gcd(\lambda',k'-\lambda')=\gcd(cd,ad)=d,\\ b' &= \gcd(\lambda',k'-\lambda'-1)=\gcd(cd,bc)=c,\\ c' &= b,\quad\text{and}\quad d'=a,\end{aligned}$$

which proves Proposition 1.

Proposition 2. Let

$$(v,k,\lambda)\overset{\phi}{\mapsto}\begin{pmatrix} a & b\\ c & d\end{pmatrix}.$$

For a design $(v,k,\lambda)$, if $b=c$, then $v$ is odd.

Proof. We know that for a design $(v,k,\lambda)$ and an even $v$, $k-\lambda$ must be a perfect square. If $b=c$ and $v$ is even, then there is a positive integer $A$ such that $ad=A^2$, hence we get

$$A^2-b^2=1,$$

so we have $A=1$ and $b=0$, it is impossible.

Proposition 3. If $(v_i', k_i', \lambda_i')$ are the complements of $(v_i, k_i, \lambda_i)$, $(i = 1, 2)$, then $(v_1', k_1', \lambda_1') \circ (v_2', k_2', \lambda_2')$ is the complement of $(v_1, k_1, \lambda_1) \circ (v_2, k_2, \lambda_2)$.

Proof. Let

$$(v_i, k_i, \lambda_i) \overset{\phi}{\mapsto} \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}, \quad (i = 1, 2), \quad \text{with} \quad \det \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} = M.$$

Then, using Proposition 1, we get

$$(v_i', k_i', \lambda_i') \overset{\phi}{\mapsto} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} M_i \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad i = 1, 2.$$

So we have

$$(v_1, k_1, \lambda_1) \circ (v_2, k_2, \lambda_2) \overset{\phi}{\mapsto} M_1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} M_2^T \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$(v_1', k_1', \lambda_1') \circ (v_2', k_2', \lambda_2') \overset{\phi}{\mapsto} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} M_1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$M_2^T \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} M_1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} M_2^T, \tag{13}$$

but $\phi$ maps the complement of $(v_1, k_1, \lambda_1) \circ (v_2, k_2, \lambda_2)$ to

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} M_1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} M_2^T \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} M_1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} M_2^T. \tag{14}$$

Hence, from (13) and (14), the proposition is proved.

Applying Proposition 3, we have

Corollary 1. If $(v', k', \lambda')$ is the complement of $(v, k, \lambda)$, then $(v', k', \lambda')^2$ is the complement of $(v, k, \lambda)^2$.

Proof. Obvious.

## *References*


1. E. F. Assmus, Jr. and D. D. Key, *Designs and Their Codes*, Cambridge Univ. Press, Cambridge, 1992.
2. E. F. Assmus, Jr., "On the Theory of Designs," *Surveys in Combinatorics, London Mathematical Society Lecture Note Series 141*, J. Siemons, editor, Cambridge University Press, Cambridge, 1989, 1–21.
3. M. Hall, Jr., *Combinatorial Theory*, 2nd edition, Wiley–Interscience, 1986.



H. W. Lu
Department of Mathematics
Tongji University
Peoples Republic of China

Harold Bowman
Department of Mathematical Sciences
University of Nevada
Las Vegas, NV 89154–4020
email: bowman@nevada.edu

Peter J.–S. Shiue
Department of Mathematical Sciences
University of Nevada
Las Vegas, NV 89154–0001
email: shiue@nevada.edu


æ