Far East Journal of Mathematical Sciences (FJMS)

http://www.pphmj.com
http://dx.doi.org/10.17654/MS103020467
Volume 103, Number 2, 2018, Pages 467-481 **ISSN: 0972-0871**

ON INTEGER PARTITIONS DETERMINED BY IN-PLACE TRANSPOSITIONS OF MATRICES

Nirutt Pipattanajinda and Yangkok Kim

Program of Mathematics
Faculty of Sciences and Technology
Kamphaeng Phet Rajabhat University
Kamphaeng Phet, Thailand
e-mail: nirutt.p@gmail.com

Department of Mathematics
Dongeui University
Busan 614-714, Korea
e-mail: ykkim@deu.ac.kr

Abstract

In-place transpositions of rectangular matrices naturally produce partitions of integers. In this note, we investigate the pattern and the number of partitions determined by in-place transposition of matrices in terms of the sizes of matrices.

1. Introduction

In-place matrix transposition is the problem of transposing an $n \times m$ matrix in-place in computer memory, with papers being published on the subject from 1959 [1]. In this note, we investigate in-place matrix transpositions from algebraic and number theoretic aspect. We consider two

Received: September 14, 2017; Accepted: November 11, 2017
2010 Mathematics Subject Classification: 05A17, 11P81.
Keywords and phrases: integer partition, in-place transposition, Sophie Germain prime.

4×2 matrices A and B, which are column-major and row-major ordered, respectively, as follows:

$$A = \begin{bmatrix} 1 & 5 \\ 2 & 6 \\ 3 & 7 \\ 4 & 8 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 7 & 8 \end{bmatrix}.$$

We now move A to B by rearranging numbers. We do not have to change two entries, 1 and 8. If we take 2 out, then we can move 3 to the original spot of 2. Now the spot of 3 is empty and so we can move 5. Then the spot of 5 is for 2. We are done. We do the same procedure for the rest to get two moving sequences $2 \to 3 \to 5$ and $4 \to 7 \to 6$ of length 3. The lengths of all procedures are 1, 1, 3 and 3, which can be regarded as a partition of 8. We express this procedure by matrices. For natural numbers $k, m, n \in \mathbb{N}$, we write $\mathbb{N}_k = \{1, 2, 3, ..., k\}$, and $mn = m \cdot n$.

Definition 1.1. An $m \times n$ matrix $[a_{(i, j)}]$ is called a *natural matrix* if

(i) all $a_{(i, j)}$ are distinct,

(ii) $a_{(i, j)} \in \mathbb{N}_{mn}$.

For an $m \times n$ matrix $A = [a_{(i, j)}]$, we write $e(A)$ for the set of all entries $a_{(i, j)}$ of A. In particular, for an $m \times n$ natural matrix A, $e(A) = \mathbb{N}_{mn}$. From now on every matrix is a natural matrix unless otherwise stated.

Definition 1.2. Let $A = [a_{(i, j)}]$ and $B = [b_{(i, j)}]$ be two $m \times n$ natural matrices. The $(m \times n)\hat{B}A$-move is a function $\hat{B} : e(A) \to e(A)$ defined by

$$\hat{B}(a_{(i, j)}) = a_{(i', j')},$$

where $a_{(i', j')} = b_{(i, j)}$.

Example 1.1. For a natural matrix A, the $\hat{A}A$-move is an identity function on $e(A)$.

For $\mathbf{a}$ in $e(A)$, the $(m \times n)\hat{B}A$-move naturally produces a finite cycle as follows:

$$\mathbf{a} \to \hat{B}(\mathbf{a}) \to \hat{B}(\hat{B}(\mathbf{a})) = \hat{B}^2(\mathbf{a}) \to \cdots \to \hat{B}^{k-1}(\mathbf{a}), \tag{1.1}$$

where $\hat{B}^k(\mathbf{a}) = \mathbf{a}$ and $\hat{B}^s(\mathbf{a}) \neq \mathbf{a}$ for $0 < s < k$. When this is the case, we say $\mathbf{a}$ generates a cycle $(\mathbf{a} \quad \hat{B}(\mathbf{a}) \quad \hat{B}^2(\mathbf{a}) \quad \cdots \quad \hat{B}^{k-1}(\mathbf{a}))$ of length k, or shortly k-cycle, under the $(m \times n)\hat{B}A$-move. By this way we can express $\hat{B}$ as the product of disjoint cycles. Moreover, the sum of all lengths of all disjoint cycles is mn.

Definition 1.3. Let A, B be two $m \times n$ natural matrices, and let $\hat{B}$ be the product of disjoint cycles $\alpha_1, \alpha_2, ..., \alpha_k$ of length $m_1, m_2, ..., m_k$, respectively. Then $m_1 + m_2 + \cdots + m_k$ is called the $(m \times n)\hat{B}A$-*partition* of mn. In particular, $\underbrace{1 + 1 + \cdots + 1}_{mn}$ is called a *trivial partition* and $1 + 1 + (mn - 2)$ is called an *improper partition*.

We note that two sums that differ only in the order of their summands are considered the same partition.

Example 1.2. The $(m \times n)\hat{B}A$-partition of mn is a trivial partition if and only if $A = B$.

Solution. Every entry of an $m \times n$ natural matrix A generates a 1-cycle under the $(m \times n)\hat{A}A$-move and so the $(m \times n)\hat{A}A$-partition of mn is a trivial partition. For the converse, we assume $A \neq B$ and $a_{(i,j)} \neq b_{(i,j)}$. Then $\hat{B}$ satisfies $\hat{B}(a_{(i,j)}) = a_{(i',j')} = b_{(i,j)} \neq a_{(i,j)}$ and so $a_{(i,j)}$ generates a cycle of length $k > 1$.

Theorem 1.1. *Every partition of each positive integer is a* $\hat{B}A$*-partition of two natural matrices A and B.*

Proof. Let $n_1 + n_2 + \cdots + n_k = n$ be a partition of *n*. We consider two $1 \times n$ natural matrices $A = [a_{(1,i)}]$ and $B = [b_{(1,i)}]$ with $a_{(1,i)} = i$ and

$$b_{(1,i)} = \begin{cases} 1 & \text{if } i = n_1 \\ 1 + n_1 + n_2 + \cdots + n_{j-1} & \text{if } i = n_1 + n_2 + \cdots + n_j \\ i + 1 & \text{if not.} \end{cases}$$

Then the $(1 \times n)\hat{B}A$-move is

$$(1 \;\; 2 \;\; \cdots \;\; n_1)(n_1 + 1 \;\; n_1 + 2 \;\; \cdots \;\; n_2)\cdots(n_{k-1} + 1 \;\; n_{k-1} + 2 \;\; \cdots \;\; n_k)$$

and so the $(1 \times n)\hat{B}A$-partition of *n* is $n_1 + n_2 + \cdots + n_k$.

In this note, we consider problems related to $\hat{B}A$-partitions of a given integer with a special class of natural matrices, which include (i) how many different partitions for a given integer exist? (ii) which integer has only one nontrivial partition? and (iii) which integer has improper partition?

2. Natural Matrices

Definition 2.1. We define an $m \times n$ *vertical natural matrix* or simply *v-matrix* by

$$\begin{bmatrix} 1 & m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & \cdots & (n-1)m+2 \\ \vdots & \vdots & & \vdots \\ m & 2m & \cdots & mn \end{bmatrix}$$

and an $m \times n$ *horizontal natural matrix* or simply *h-matrix* by

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ n+1 & n+2 & \cdots & 2n \\ \vdots & \vdots & & \vdots \\ (m-1)n+1 & (m-1)n+2 & \cdots & mn \end{bmatrix}.$$

In particular, if $n = 1$, then the *h*-matrix and *v*-matrix are same. Moreover, for an $m \times 1$ *v*-matrix V and an $m \times 1$ *h*-matrix H, the $(m \times 1)\hat{H}V$ -partition of m is a trivial partition. We note that for an $m \times n$ *v*-matrix $[v_{(i,\,j)}]$ and an $m \times n$ *h*-matrix $[h_{(i,\,j)}]$, $v_{(i,\,j)} = (j-1)m + i$ and $h_{(i,\,j)} = (i-1)n + j$.

Lemma 2.1. *For an $m \times n$ v-matrix V and an $m \times n$ h-matrix H, the $\hat{H}V$-move is a function $\hat{H} : e(V) \to e(V)$ with $\hat{H}(x) \equiv n(x-1) + 1 \bmod(nm-1)$. In particular, $\hat{H}^k(x) \equiv n^k(x-1) + 1 \bmod(nm-1)$.*

Proof. Let $V = [v_{(i,\,j)}]$ and $H = [h_{(i,\,j)}]$, and $x = v_{(i,\,j)} = i + (j-1)m$. Then

$$\hat{H}(x) = \hat{H}(v_{(i,\,j)}) = h_{(i,\,j)} = (i-1)n + j = (i-1)n + (j-1) + 1$$

$$\equiv (j-1)nm + (i-1)n + 1 \bmod(nm-1)$$

$$\equiv (x-i)n + (i-1)n + 1 \bmod(nm-1) \equiv nx - n + 1 \bmod(nm-1)$$

and

$$\hat{H}^k(x) = H(\hat{H}^{k-1}(x)) = H(n^{k-1}(x-1) + 1) \equiv n^k(x-1) + 1 \bmod(nm-1).$$

For an $m \times n$ *v*-matrix V and an $m \times n$ *h*-matrix H, we determine $x \in e(V)$ which generates a 1-cycle under the $(m \times n)\hat{H}V$ -move. By Lemma 2.1, $x \equiv \hat{H}(x) \equiv n(x-1) + 1 \bmod(nm-1)$. That is,

$$(n-1)(x-1) \equiv 0 \bmod(nm-1) \quad \text{or} \quad (nm-1) \mid (n-1)(x-1).$$

Let $(n-1,\, nm-1) = d_1$ be the greatest common divisor of $n-1$ and $nm-1$. Then $\dfrac{(nm-1)}{d_1} \mid (x-1)$ and so there are $d_1 + 1$ elements in $e(V)$, namely,

$$x = 1,\ 1 \cdot \frac{(nm-1)}{d_1} + 1,\ 2 \cdot \frac{(nm-1)}{d_1} + 1,\ \ldots,\ d_1 \cdot \frac{(nm-1)}{d_1} + 1.$$

Hence, we have $d_1 + 1$ disjoint 1-cycles in the $(m \times n)\hat{H}V$ -partition of *mn*. We now determine $x \in e(V)$ which generates a 2-cycle under the $(m \times n)\hat{H}V$ -move. By applying the above argument, we get $d_2 + 1$ elements in $e(V)$ such that $\hat{H}^2(x) \equiv x \bmod(nm - 1)$, namely,

$$x = 1,\ 1 \cdot \frac{(nm-1)}{d_2} + 1,\ 2 \cdot \frac{(nm-1)}{d_2} + 1,\ \ldots,\ d_2 \cdot \frac{(nm-1)}{d_2} + 1,$$

where $(n^2 - 1,\ nm - 1) = d_2$. We note that if $x \equiv \hat{H}(x)$, then $x \equiv \hat{H}^2(x)$. Hence, there are $d_2 - d_1$ elements in $e(V)$ which determine 2-cycles under the $(m \times n)\hat{H}V$ -move. Moreover, there are $\frac{d_2 - d_1}{2}$ disjoint 2-cycles in the $(m \times n)\hat{H}V$ -partition of $m \cdot n$. In general, if we write by e_k the number of elements in $e(V)$ which determine *k*-cycles under the $(m \times n)\hat{H}V$ -move, then we have the following.

Theorem 2.2. *The number of elements in $e(V)$ which determine a k-cycle under the $(m \times n)\hat{H}V$ -move is*

$$e_k = d_k + 1 - \sum_{c \mid k,\, c \neq k} e_c,$$

where $d_k = (n^k - 1,\ nm - 1)$.

Corollary 2.3. *The number of disjoint k-cycles in the $(m \times n)\hat{H}V$ -partition of $m \cdot n$ is $\frac{e_k}{k}$.*

In a ring $\mathbb{Z}_n$ the order $o(x)$ of an element x with $(x,\ n) = 1$ is the smallest positive integer *k* such that $x^k = 1 \bmod n$.

Corollary 2.4. *The order $o(n)$ in $\mathbb{Z}_{mn-1}$ is the largest length of cycles in the $(m \times n)\hat{H}V$ -partition of mn. Moreover, the length of every cycle in the $(m \times n)\hat{H}V$ -partition of mn is a divisor of $o(n)$.*

Proof. We note that for every element x in $\mathbb{Z}_{mn-1}$,

$$\hat{H}^{o(n)}(x) \equiv n^{o(n)}(x-1)+1 \equiv (x-1)+1 \equiv x \bmod(mn-1).$$

Theorem 2.5. *The* $(m \times n)\hat{HV}$ *-partition of mn is the same as the* $(n \times m)\hat{HV}$ *-partition of mn*:

Proof. We note that for an $m \times n$ v-matrix V and an $m \times n$ h-matrix H, the transpose V^T and H^T are an $n \times m$ h-matrix and an $n \times m$ v-matrix, respectively. Moreover, the $\hat{HV}$-move and the $\hat{VH}$-move are inverse functions each other.

Definition 2.2. A partition of an integer is called an $\hat{HV}$ *-partition* when it is an $(m \times n)\hat{HV}$-partition of mn for the $m \times n$ v-matrix V and the $m \times n$ h-matrix H.

How many $\hat{HV}$-partitions we have for a given integer? It is clear that a prime number has only one $\hat{HV}$-partition which is trivial. In general we suppose an integer t has k distinct divisors, $u_1, u_2, ..., u_k$, then we have k different $\left(u_i \times \frac{t}{u_i}\right)\hat{HV}$-partitions. By Theorem 2.5 without loss of generality we can assume that $u_i \le \frac{t}{u_i}$. Hence, there are at most $\left\lceil \frac{k}{2} \right\rceil$ different $\hat{HV}$-partitions of t. For example, $12 = 2^2 \cdot 3$ has 3 different $\hat{HV}$-partitions, namely,

$$\underbrace{1+1+\cdots+1}_{12}, \; 1+1+10 \text{ and } 1+1+5+5$$

corresponding to $(12 \times 1), (6 \times 2), (4 \times 3)\hat{HV}$-partitions, respectively. We also note that two different $\hat{HV}$-moves for a fixed number can produce the same partition. For example, $24 = 2^3 \cdot 3$ has 4 different $\hat{HV}$-moves but it has only two different $\hat{HV}$-partitions, a trivial partition and a nontrivial

partition $1+1+11+11$. Then which integer has only one nontrivial partition? It is clear that for two primes *p*, *q*, there are only two $\hat{H}V$-partitions of *pq*, corresponding to $(pq \times 1)$, $(p \times q)\hat{H}V$-partitions. Thus, an integer *pq* has only one nontrivial partition.

Lemma 2.6. *The* $(n \times n)\hat{H}V$*-partition of* n^2 *is*

$$n^2 = \underbrace{1+1+\cdots+1}_{n} + \underbrace{2+2+\cdots+2}_{\frac{n(n-1)}{2}}.$$

Proof. For an $n \times n$ *v*-matrix $V = [v_{(i,j)}]$ and an $n \times n$ *h*-matrix $H = [h_{(i,j)}]$, we note that the transpose H^T of *H* is *V*, that is, $v_{(i,j)} = h_{(j,i)}$. Hence, $\hat{H}(v_{(i,j)}) = v_{(j,i)}$ and so $\hat{H}^2(v_{(i,j)}) = v_{(i,j)}(i \neq j)$, which means that every diagonal entry produces a cycle of length 1 and every other entry produces a 2-cycle.

Lemma 2.7. *For an arbitrary integer* $t \geq 2$. *If any* $\hat{H}V$*-partition of* t^q *is a trivial partition or is of the form*

$$\underbrace{1+1+\cdots+1}_{t} + \underbrace{q+q+\cdots+q}_{\frac{t^q-t}{q}},$$

then q is a prime number.

Proof. If $q = rs$, where $1 < r, s < q$, then we consider the $(t^{(r-1)s} \times t^s)\hat{H}V$ - partition of t^q. For $2 \in e(V)$, we have

$$2 \equiv (t^s)^r(2-1)+1 \bmod(t^q-1),$$

which means that the $(t^{(r-1)s} \times t^s)\hat{H}V$-partition of t^q contains a cycle of length $0 \leq r < q$.

Theorem 2.8. *For a prime p, a positive integer q is a prime if and only if the* $\hat{H}V$*-partition of* p^q *is a trivial partition or is of the form*

$$\underbrace{1+1+\cdots+1}_{p}+\underbrace{q+q+\cdots+q}_{\frac{p^q-p}{q}}.$$

Proof. If $q = 2$, then there are only two $\hat{HV}$-partitions, namely, $(p^2 \times 1)\hat{HV}$-partition and $(p \times p)\hat{HV}$-partition. The former one produces a trivial partition of p^2 and the latter one determines $1+1+\cdots+1+2+2+\cdots+2$ by Lemma 2.6. Let $q \neq 2$ and $i > j$ with $i + j = q$. We find the $(p^i \times p^j)\hat{HV}$-partition of p^q. Since $(p^j - 1,\ p^q - 1) = p^{(j,q)} - 1 = p - 1$, there are p 1-cycles in the $\hat{HV}(p^i \times p^j)$ partition of p^q by Theorem 2.2. For $1 < k < q$, $((p^j)^k - 1,\ p^q - 1) = p^{(jk,q)} - 1 = p - 1$. Thus, there are $p - p = 0$ elements which determine *k*-cycles and so there are no *k*-cycles. Moreover, there are $p^q - p$ elements which determine q cycles. Indeed there are $\frac{p^q - p}{q}$ disjoint q-cycles. Further, we note that if $p \neq q$, then $p^{q-1} \equiv 1 \bmod q$ and so $p^q \equiv p \bmod q$ by Fermat's little theorem. The converse is a special case of Lemma 2.7.

Corollary 2.9. *A number p is prime if and only if any* $\hat{HV}$*-partition of* 2^p *is a trivial partition or is of the form*

$$1+1+\underbrace{p+p+\cdots+p}_{\frac{2^p-2}{p}}.$$

3. Determination of Partitions

We will determine $(m \times n)\hat{HV}$-partitions of *mn*. We will depict the cycles of the $(m \times n)\hat{HV}$-move on the unit circle and call it the $(m \times n)\hat{HV}$-figure. We simply arrange *mn* points evenly along the unit circle and impose

numbers 1, ..., *mn*, counterclockwise. We also define the mirror image of *x* by $x-(mn+1)$. The mirror image will be numbered by $-1, -2, ..., -mn$, clockwise (see Figure 1). Then we connect two numbers *v* and $\hat{H}(v)$ for all $v \in e(V)$.

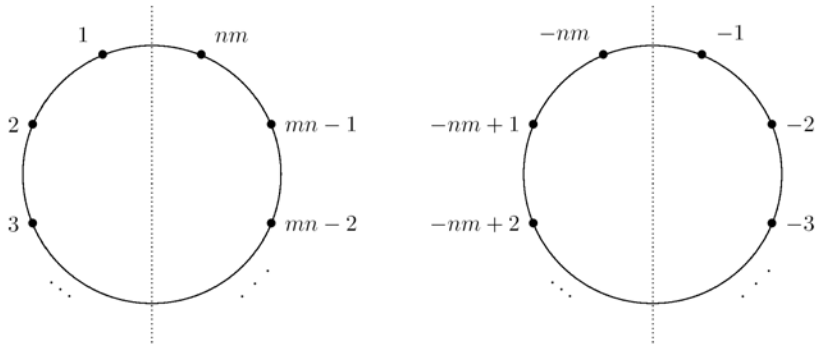

Figure 1. Arrangement of elements in $e(V)$.

We note that the number *i* is connected to the number $n(i-1)+1$ in the $(m \times n)\hat{H}V$ -figure because $\hat{H}(i) \equiv n(i-1)+1 \bmod(mn-1)$. We now show that the number $-i$ is connected to the number $-(n(i-1)+1)$. From the construction

$$-i \equiv -i + nm + 1 \bmod(mn-1)$$

and

$$-(n(i-1)+1) \equiv -(n(i-1)+1) + nm + 1 \equiv -n(i-1) + nm \bmod(mn-1).$$

We also note that

$$\hat{H}(-i) \equiv \hat{H}(-i + nm + 1) \equiv n(-i + nm) + 1 \bmod(nm-1).$$

Moreover,

$$n(-i + nm) + 1 - (-n(i-1) + nm) \equiv (n-1)(mn-1) \equiv 0 \bmod(mn-1)$$

and so

$$n(-i + nm) + 1 \equiv -n(i-1) + nm \equiv -(n(i-1)+1) \bmod(mn-1).$$

Thus,

$$\hat{H}(-i) \equiv -(n(i-1)+1) \bmod (mn-1)$$

which means that the number $-i$ is connected to the number $-(n(i-1)+1)$. The above argument shows that the $(m \times n)\hat{HV}$-figure is symmetric with respect to the central vertical dotted axis. For example, Figure 2 shows the $(4 \times 2)\hat{HV}$-figure for $4 \cdot 2 = 8$, where two triangles represent two 3-cycles, and two points 1, 8 mean two 1-cycles in the $(4 \times 2)\hat{HV}$-partition of 8.

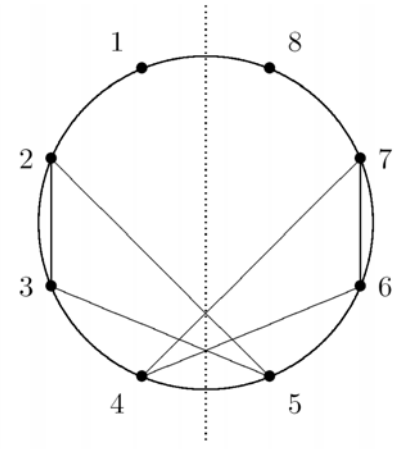

Figure 2. 4×2 moving.

Theorem 3.1. *The* $(m \times n)\hat{HV}$ *-partition of mn is of the form*:

$$\underbrace{1+\cdots+1}_{e_1} + \underbrace{2+\cdots+2}_{\frac{e_2}{2}} + (t_1+t_1) + \cdots + (t_k+t_k) + \delta_{ij}s_1 + s_2 + \cdots + s_\ell,$$

where δ_{ij} *is the Kronecker delta,* $t_i(>2)$, $s_j(>1)$ *are divisors of* $o(n)$, s_1 *is odd and the others are even.*

As simple applications of Theorem 3.1, we determine 1, 2-cycles of $(m \times n)\hat{HV}$-partition of mn for $m = 2, 3$. Let $n = 2$. We note that

$(2-1,\ 2m-1) = (1,\ 2m-1) = 1$ for an integer m. Hence, there are 2 1-cycles in the $(m \times 2)\hat{HV}$-partition of $2m$. For 2-cycles, we note that $(2^2-1,\ 2m-1) = (3,\ 2m-1) = 1,\ 3$. If $m \equiv 0, 1 \bmod 3$, then $e_1 = 1$ and so there are no 2-cycles in the $(m \times 2)\hat{HV}$-partition of $2m$. If $2m-1 \equiv 0 \bmod 3$ or $m \equiv 2 \bmod 3$, $(3,\ 2m-1) = 3$. When we put $2m-1 = 3k$, there are 4 elements,

$$x = 1,\ 1 \cdot \frac{(2m-1)}{3} + 1,\ 2 \cdot \frac{(2m-1)}{3} + 1,\ 3 \cdot \frac{(2m-1)}{3} + 1,$$

that is, $x = 1,\ k+1,\ 2k+1$ and $2m$. Thus, $e_2 = 4 - e_1 = 2$ and so there is one 2-cycle, $(k+1\ \ 2k+1)$, in the $(m \times 2)\hat{HV}$-partition of $2m$.

Corollary 3.2. *The* $(m \times 2)\hat{HV}$*-partition of* $2m$ *is the following*:

(i) $m \equiv 0, 1 \bmod 3$.

$$1 + 1 + (t_1 + t_1) + (t_2 + t_2) + \cdots + (t_k + t_k) + s_1 + s_2 + \cdots + s_\ell,$$

(ii) $m \equiv 2 \bmod 3$.

$$1 + 1 + 2 + (t_1 + t_1) + (t_2 + t_2) + \cdots + (t_k + t_k) + s_1 + s_2 + \cdots + s_\ell,$$

where $t_i (> 2)$ *and even* $s_j (> 2)$ *are divisors of* $o(2)$.

For $n = 3$, we note

$$(3-1,\ 3m-1) = (2,\ 3m-1) = \begin{cases} 1 & m \text{ is even} \\ 2 & m \text{ is odd.} \end{cases}$$

Thus, there are 2 or 3 1-cycles in the $(m \times 3)\hat{HV}$-partition of $3m$. For 2-cycles, we note that $(3^2-1,\ 3m-1) = (8,\ 3m-1) = 1,\ 2,\ 4$ or 8. If m is even, then $(8,\ 3m-1) = 1$. Let us suppose $(8,\ 3m-1) = 2$. Then m is odd. Let $m = 2k+1$. Then $(8,\ 3m-1) = (8,\ 2(3k+1)) = 2$ and so k is even.

Further, $m = 4\ell + 1$ and so $m \equiv 1, 5 \bmod 8$. Clearly, the converse holds. We can apply the same argument for the other cases to get the following:

$$(8,\ 3m-1) = \begin{cases} 1 & m \text{ is even} \\ 2 & m \equiv 1,\ 5 \bmod 8 \\ 4 & m \equiv 7 \bmod 8 \\ 8 & m \equiv 3 \bmod 8. \end{cases}$$

Hence, for even m or $m \equiv 1,\ 5 \bmod 8$, there are no 2-cycles, and there are 1 and 3 2-cycles depending on $m \equiv 7 \bmod 8$ and $m \equiv 3 \bmod 8$, respectively.

Corollary 3.3. *The* $(m \times 3)\hat{HV}$ *-partition of* $3m$ *is the following*:

(i) *m is even*.

$$1 + 1 + (t_1 + t_1) + (t_2 + t_2) + \cdots + (t_k + t_k) + s_1 + s_2 + \cdots + s_\ell,$$

(ii) *m is odd and* $m \equiv 1,\ 5 \bmod 8$.

$$1 + 1 + 1 + (t_1 + t_1) + (t_2 + t_2) + \cdots + (t_k + t_k) + s_1 + s_2 + \cdots + s_\ell,$$

(iii) *m is odd and* $m \equiv 7 \bmod 8$.

$$1 + 1 + 1 + 2 + (t_1 + t_1) + (t_2 + t_2) + \cdots + (t_k + t_k) + s_1 + s_2 + \cdots + s_\ell,$$

(iv) *m is odd and* $m \equiv 3 \bmod 8$.

$$1 + 1 + 1 + 2 + 2 + 2 + (t_1 + t_1) + (t_2 + t_2) + \cdots + (t_k + t_k) + s_1 + s_2 + \cdots + s_\ell,$$

where $t_i (> 2)$ *and even* $s_j (> 2)$ *are divisors of* $o(3)$.

We find an integer n which has only one nontrivial $\hat{HV}$ -partition, that is, $n = 1 + 1 + (n-2)$.

Theorem 3.4. *If the* $(m \times n)\hat{HV}$ *-partition of* mn *is of form* $1+1+(mn-2)$, *then* $mn-1$ *is prime. Moreover,* $mn = 3, 5, p^k + 1, 2p^k + 1$, *where p is an odd prime and* $k \geq 1$.

Proof. We notice that if the $\hat{H}V$-partition is of form $1+1+(mn-2)$, then the set of all $\hat{H}^k(n) = n^k + 1 \bmod(mn-1)$ is $\{2, 3, ..., mn-1\}$. Hence, $\{n^k \bmod(mn-1) : k \in \mathbb{Z}\} = \{1, 2, 3, ..., mn-2\}$ which means $\mathbb{Z}^*_{mn-1}$ is a cyclic group generated by n. We recall that for a ring $\mathbb{Z}_t = \{0, 1, 2, ..., t-1\}$, $\mathbb{Z}^*_t = \mathbb{Z}_t \backslash \{0\}$ forms a multiplicative group if and only if t is a prime. Thus, $mn-1$ is prime. We also note that for a positive integer t, $\mathbb{Z}_t$ has a primitive root if and only if $t = 2, 4, p^k, 2p^k$, where p is an odd prime and $k \geq 1$, which implies the latter part.

The converse of the above theorem is not true. For example, for $mn = 24$, there are 4 different $(24\times1), (12\times2), (8\times3), (6\times4)\hat{H}V$-moves. By direct calculation, we have the $(24\times1)\hat{H}V$-partition of 24 is a trivial partition and the others produce the same partition $1+1+11+11$.

We recall that a prime number p is called a *Sophie Germain prime* if $2p+1$ is also prime (see [2]).

Theorem 3.5. *For a Sophie Germain prime p, the* $((p+1)\times2)\hat{H}V$*-partition of* $2(p+1)$ *is*

$$\begin{cases} 1+1+2p & p \equiv 1 \bmod 4 \\ 1+1+p+p & p \equiv 3 \bmod 4. \end{cases}$$

Proof. $\mathbb{Z}^*_{2p+1}$ is a multiplicative group of order $2p$. We notice that the subgroup $\langle 2 \rangle$ generated by 2 is of order p or $2p$. Moreover, there is one-to-one correspondence between two sets, $\{2^k : k \in \mathbb{Z}\}$ and $\{2^k + 1 : k \in \mathbb{Z}\}$ under module $2p+1$. Suppose that $p \equiv 1 \bmod 4$. If 2 is of order 2^p, that is, $2^p \equiv 1 \bmod(2p+1)$, then 2 is a quadratic residue $\bmod(2p+1)$. However, $p \equiv 1 \bmod 4$ and so $2p+1 \equiv 3 \bmod 8$. Thus, 2 is a quadratic nonresidue

$\bmod(2p+1)$, a contradiction. Let $p \equiv 3 \bmod 4$. If 2 is of order 2^p, that is, $2^p \equiv -1 \bmod(2p+1)$, then $2^{p+1} \equiv (2^{\frac{p+1}{2}})^2 \equiv 1 \bmod(2p+1)$. Thus, –2 is a quadratic residue $\bmod(2p+1)$. However, $p \equiv 3 \bmod 4$ and so $2p+1 \equiv 7 \bmod 8$. Thus, –2 is a quadratic nonresidue $\bmod(2p+1)$, a contradiction.

References

[1] P. F. Windley, Transposing matrices in a digital computer, Comput. J. 2 (1959), 47-48.

[2] https://en.wikipedia.org/wiki/Sophie_Germain_prime, Sophie Germain prime