On q-free subsets of operation set

Yeong-Nan Yeh

Institute of Mathematics, Academia Sinica
Taipei, Taiwan 11529, Republic of China

Abstract. A set T with a binary operation + is called an operation set and denoted as $\langle T, +\rangle$. An operation set $\langle S, +\rangle$ is called q-free if $qx \notin S$ for all $x \in S$. Let $\psi_q(T)$ be the maximum possible cardinality of a q-free operation subset $\langle S, +\rangle$ of $\langle T, +\rangle$.

We obtain an algorithm for finding $\psi_q(N_n)$, $\psi_q(\mathbf{Z}_n)$ and $\psi_q(\mathbf{D}_n)$, $q \in \mathbf{N}$, where $N_n = \{1, 2, \ldots, n\}$, $\langle \mathbf{Z}_n, +_n\rangle$ is the group of integers under addition modulo n and $\langle \mathbf{D}_n, +\rangle$ is the dihedral group of order $2n$.

1. Introduction

A set T with a binary operation + is called an operation set and denoted as $\langle T, +\rangle$. The operation + may not be closed (i.e. $x + y \notin T$ for some $x, y \in T$). An operation set $\langle S, +, \cdot\rangle$ is called sum-free if $x + y \notin S$ for all $x, y \in S$ and is called q-free if $qx \notin S$ for all $x \in S$. Sum-free operation sets have been extensively studied in many contexts. For a comprehensive survey, see [3]. E. Wang [4] studied the maximum cardinality of double-free (2-free) operation set $\langle S, +\rangle$ where $S \subset \{1, 2, \ldots, n\}$. In this paper, we provide an elegant method to solve Wang's problem (including q-free subset). A group $\langle G, +\rangle$ is an operation set. The maximum cardinality of q-free operation subset $\langle S, +\rangle$ is also discussed here when $\langle S, +\rangle$ is a cyclic group $\langle \mathbf{Z}_n, +\rangle$ or dihedal group $\langle \mathbf{D}_n, +\rangle$

Given a operation set $\langle T, +\rangle$ and function $f(x) = 2x$, we can construct a digraph $G(T)$, which has vertices set $V(G) = T$ and directed edges set $E(G) = \{\vec{xy} | y = 2x \text{ for } x, y \in T\}$. A set $I \subset V(G)$ is called independent if no two vectices of I are adjacent in G i.e. $\vec{xy} \notin E(G)$ and $\vec{yx} \notin E(G)$ for all $x, y \in I$. Obviously, there is a bijection between the set of all double-free subsets with the maximum cardinality of the operation set $\langle T, +\rangle$ and the set of all independent subsets with the maximum cardinality in the digraph $G(T)$.

Notation

Let $\psi(G)$ be the maximum cardinality of an independent subset in $G(T)$. $\lceil\ \rceil$ and $\lfloor\ \rfloor$ denote the ceiling and floor functions respectively. $\varphi(n)$ is the Euler's φ-function. i.e. $\varphi(n)$ is the number of positve integers less than or equal to n that are relatively prime to n. $\chi(S) = 1$ if statement S is true; $\chi(S) = 0$ otherwise.

2. Maximum cardinality of q-free subset of integers

The following two lemmas are straightforward and useful.

Lemma 1. *Let the digraph G have k components $G_1, G_2, \dots G_k$. Then if S_i is a maximally independent subset of G_i, then the disjoint union of all S_i is a maximally independent subset of G and*

$$\psi(G) = \sum_{1 \le i \le k} \psi(G_i).$$

Lemma 2. *Let L_n be the directed path of length n and C_n be the directed cycle of length n. Then $\psi(L_n) = \lceil \frac{n}{2} \rceil$ and $\psi(C_n) = \lfloor \frac{n}{2} \rfloor$.*

Using the above lemmas, we now prove our first theorem.

Theorem 1. *Let $N_n = \{1, 2, \dots, n\}$ and $2^t \le n < 2^{t+1}$. Then*

$$\psi(N_n) = \sum_{0 \le i \le \lfloor \frac{t}{2} \rfloor} (a_{2i} - a_{2i+1})$$

where $a_i = \lfloor \frac{n}{2^i} \rfloor$ if $i \le t$; $a_i = 0$ otherwise.

Proof: The digraph $G(N_n)$ has $\lceil \frac{n}{2} \rceil$ components $G_1, G_2, \dots, G_{\lceil \frac{n}{2} \rceil}$ where component G_j, $1 \le j \le \lceil \frac{n}{2} \rceil$, is the directed path

$$(2j-1) \rightarrow 2(2j-1) \rightarrow \cdots \rightarrow 2^s(2j-1)$$

where $2^s \le \frac{n}{2j-1} < 2^{s+1}$.

1	3	5	7	9	11	13	15	17	19	21	23	25
↓	↓	↓	↓	↓	↓	↓						
2	6	10	14	18	22	26						
↓	↓	↓										
4	12	20										
↓	↓											
8	24											
↓												
16												

Figure 1. Digraph $G([26])$

Arrange the components G_j vertically in a tableau (see Figure 1) and for each G_j, take as maximally independent subset S_j, the set formed by the elements on the first row, the third row, etc. (i.e. $(2j-1), 2^2(2j-1), \dots$). Using lemma 1, the set S which is the disjoint union of all of the sets S_j, $1 \le j \le \lceil \frac{n}{2} \rceil$, is an independent subset with the maximum possible cardinality of N_n. But S is made of all the elements in the odd numbered rows and b_i is the number of elements lying on or below row i. Therefore, counting by rows, the theorem is proved. ∎

An operation set $\langle T,+\rangle$ is called q-free if $qx \notin S$ for all $x \in S$. Given an operation set $\langle T,+\rangle$ and a function $f(x) = qx$, we can construct a corresponding digraph $G_q(T)$, which has vertices set $V_q(G) = T$ and directed edges $E_q(G) = \{\vec{xy} | y = qx \text{ for } x, y \in T\}$. Let $\psi_q(G)$ be the maximum possible cardinality of an independent subset in G_q. The proof of the following theorem is similar to that of theorem 1.

Theorem 2. *Let* $N_n = \{1,2,\ldots,n\}$ *and* $q^t \leq n < q^{t+1}$. *Then* $\psi_q(N_n) = \Sigma_{0\leq i\leq\lfloor\frac{t}{2}\rfloor}(b_{2i} - b_{2i+1})$ *where* $b_i = \lfloor\frac{n}{q^i}\rfloor$ *if* $i \leq t$; $b_i = 0$ *otherwise.*

3. Maximum cardinality of q-free subset of $\langle \mathbf{Z}_n, +n\rangle$

Let $\langle \mathbf{Z}_n, +_n\rangle$ be the group of integers under addition modulo n and $\langle \mathbf{Z}_n^*, \cdot_n\rangle$ denote the group of integers relatively prime to n under multiplication mod n. Let H be the cyclic subgroup of $\langle \mathbf{Z}_n^*, \cdot_n\rangle$ generated by 2 when n is an odd integer. The order of 2, $\text{ord}_n(2)$, is the size of subgroup H and the index of 2, $\text{ind}_n(2)$, is the number of distinct right cosets of H in G. Any element $a \in \mathbf{Z}_n^*$ belongs to a unique right coset H_a, that is, there exist $x_1, x_2, \ldots, x_t$, $t = \text{ind}_n(2)$, such that $\mathbf{Z}_n^* = \cup_{1\leq i\leq t} Hx_i$.

When we write $\mathbf{Z}_k \subseteq \mathbf{Z}_l$ we mean inclusion of the underlying *sets* chosen (for convenience) to be $\{0,1,\ldots,k-1\}$ and $\{0,1,\ldots,l-1\}$.

Now, we will discuss $\psi(\mathbf{Z}_n)$ step by step. In these 5 steps, n is seen a (i) prime, (ii) prime power,(iii) prower of 2, (iv) odd number (v) any integer. First, we have

Proposition 1. *Let p be an odd prime and* $ord_p(2) = d$. *Then* $\psi(\mathbf{Z}_p) = \frac{p-1}{d}\lfloor\frac{d}{2}\rfloor$.

Proof: Let $H = \{1,2,2^2,\ldots,2^{d-1}\}$ and $\mathbf{Z}_p^* = \Sigma_{1\leq i\leq t} Hx_i$ where $t = \frac{p-1}{d}$. Then the digraph $G(\mathbf{Z}_p)$ has $t+1$ components $G_0, G_1, \ldots, G_t$, where G_0 is an isolated loop on the vertex 0 and G_i, $i > 0$, is a directed cycle. i.e.,

$$G_i : x_i \rightarrow 2x_i \rightarrow 2^2x_i \rightarrow \cdots \rightarrow 2^{d-1}x_i \rightarrow x_i$$

for $1 \leq i \leq t$. By lemmas 1 and 2, we have

$$\psi(\mathbf{Z}_p) = \sum_{1\leq i\leq t} \lfloor\frac{d}{2}\rfloor = \frac{p-1}{d}\lfloor\frac{d}{2}\rfloor$$

∎

In 1828, Abel asked a question: Is there a prime p and positive integer a such that $a^{p-1} \equiv 1 \pmod{p^2}$. Jacobi gives the following partial answer: If $p \leq 37$ then the solutions of Abel's problem are $p = 11, a = 3$ or 9; $p = 29, a = 14$ and $p = 37, a = 18$.

Definition 1. *Let p be a prime. If $a^{p-1} \equiv$ mod p^k then a is called a kth-Fermat's solution (k-FS) for prime p; otherwise, a is called a kth-non-Fermat's solution (k-NFS).*

Let m, n be two integers and $(m, n) = 1$. It is well-known that $n^{\varphi(m)} \equiv 1 \pmod m$. Hence if $(a, p) = 1$ then a is a first-Fermat's solution (1-FS) for the prime p. In [2], 2 is proved to be a 2-FS for prime 1093. By Binomial Expansion Theorem, the following lemma is obtained.

Lemma 3. *Let p be a prime and 2 be a k-FS and (k + 1)-NFS for the prime p. (i.e. $p^k \mid 2^{p-1} - 1$ but $p^{k+1} \not\mid 2^{p-1} - 1$). Then*

$$ord_{p^s}(2) = \begin{cases} ord_p(2) & if\, 1 \leq s \leq k \\ p^{s-k} ord_p(2) & if\, s > k \end{cases}.$$

Proof: Let $d_s = \text{ord}_{p^s}(2)$, for $s = 1, 2, \ldots$. According to the hypothesis, we have

$$2^{p-1} = xp^k + 1 \text{ where } p \text{ does not divide } x$$

from which it follows that $1 \leq d_1 \leq d_2 \leq \cdots \leq d_k \leq p-1$.

Let

$$2^{d_1} = yp^u + 1 \text{ where } k \geq u \geq 1 \text{ and } p \text{ does not divide } y.$$

By the binomial expansion theorem that p^{u+1} does not divide $2^{d_1 i} - 1$ for $1 \leq i < p$. It implies that $u = k$ and $d_1 = d_k$. Therefore $d_1 = d_2 = \cdots = d_k$. Let $2^{d_k} = zp^k + 1$ where z is not a multiple of p. Then $p^{k+1} \mid 2^{d_k j} - 1 \Leftrightarrow p \mid j$. Hence $d_{k+1} = pd_k$ and so on inductively. ∎

Given a positive integer m, it is easy to use lemma 3 to decide $\text{ord}_{p^s}(2)$ for $1 \leq s \leq m$. Thus, we have

Proposition 2. *Let p be an odd prime and m be a positive integer. Let $ord_{p^s}(2) = d_s$ for $1 \leq s \leq m$. Then $\psi(\mathbf{Z}_{p^m}) = \Sigma_{1 \leq s \leq m} \frac{\varphi(p^s)}{d_s} \lfloor \frac{d_s}{2} \rfloor$.*

Proof: Let $H_s = \{1, 2, 2^2, \ldots, 2^{d_s - 1}\}$ and $\mathbf{Z}_{p^s}^* = \cup_{1 \leq i \leq t_s} H x_{si}$ where $t_s = \frac{\varphi(p^s)}{d_s}$ for $1 \leq s \leq m$. Then

$$\mathbf{Z}_{p^m} = \left(\bigcup_{1 \leq s \leq m} p^{m-s} \mathbf{Z}_{p^s}^* \right) \cup \{0\}$$
$$= \left(\bigcup_{1 \leq s \leq m} \bigcup_{1 \leq i \leq t_s} p^{m-s} H x_{si} \right) \cup \{0\}$$

Hence the digraph $G(\mathbf{Z}_{p^m})$ has $1 + \Sigma_{1 \leq s \leq m} t_s$ components $G_0, G_{11}, \ldots, G_{mt_m}$ where G_0 is an isolated loop on the vertex 0 and G_i, $i > 0$ is a directed cycle. i.e.,

$$G_{si}: x_{si}p^{m-s} \to 2x_{si}p^{m-s} \to \cdots \to 2^{d_s - 1} x_{si} p^{m-s} \to x_{si}p^{m-s}$$

for $1 \leq s \leq m$, $1 \leq i \leq t_s$. By lemmas 1 and 2, we have

$$\psi(Z_{p^m}) = \sum_{1\leq s\leq m}\sum_{1\leq i\leq t_s} \lfloor \frac{d_s}{2} \rfloor = \sum_{1\leq s\leq m} \frac{\varphi(p^s)}{d_s} \lfloor \frac{d_s}{2} \rfloor$$

∎

Now, we will discuss the case when n is a power of 2.

Proposition 3.

$$\psi(Z_{2^m}) = \sum_{0\leq i\leq \lfloor \frac{m-1}{2} \rfloor} 2^{m-1-2i} = \begin{cases} \frac{2}{3}(2^m - 1) & \text{if } m \text{ is even.} \\ \frac{1}{3}(2^{m+1} - 1) & \text{if } m \text{ is odd.} \end{cases}$$

Proof: First, we have a partition of Z_{2^m} in the following

$$Z_{2^m} = \left(\bigcup_{0\leq j\leq \lfloor \frac{m-1}{2} \rfloor} \bigcup_{1\leq i\leq r} (A_{ij} \cup B_{ij}) \right) \cup \{0\}$$

where $r = 2^{m-2-2j}$, $A_{ij} = \{2^{2j}(2i-1), 2^{2j+1}(2i-1)\}$ and $B_{ij} = \{2^{2j}(2i-1) + 2^{m-1})\}$.

We know that 0 does not belong to any double-free subset of Z_{2^m} and any double-free subset of Z_{2^m} can contain one element in each of the doubletons sets A_{ij} at most. Hence,

$$\psi(Z_{2^m}) \leq \sum_{0\leq j\leq \lfloor \frac{m-1}{2} \rfloor} \sum_{1\leq i\leq r} (1+1) \leq \sum_{0\leq j\leq \lfloor \frac{m-1}{2} \rfloor} 2^{m-1-2j}.$$

Where $r = 2^{m-2-2j}$. Let $M = \{2+2^{m-1})|0 \leq j \leq \lfloor \frac{m-1}{2} \rfloor, 1 \leq i \leq 2^{m-2-2j}\}$. Then M is a double-free subset of Z_{2^m} and $|M| = \sum_{0\leq j\leq \lfloor \frac{m-1}{2} \rfloor} 2^{m-1-2j}$. Therefore, we have

$$\psi(Z_{2^m}) = \sum_{0\leq j\leq \lfloor \frac{m-1}{2} \rfloor} 2^{m-1-2j}.$$

∎

Let $\mathbf{p} = (p_1, p_2, \ldots, p_r)$ be a sequence of distinct odd primes and $\mathbf{e} = (e_1, e_2, \ldots, e_r)$ be a sequence of non-negative integers. We shall denote $\mathbf{p}^{\mathbf{e}}$ the integer $p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ and $\mathbf{0}$ as the sequence $(0, 0, \ldots, 0)$. Let $\mathbf{a} = (a_1, a_2, \ldots, a_r)$ be a sequence of non-negative integers. We write $\mathbf{a} \leq \mathbf{e}$ if $0 \leq a_i \leq e_i$ for $1 \leq i \leq r$.

Let $n = \mathbf{p}^{\mathbf{e}}$ and $\text{ord}_{p_i^j}(2) = d_{ij}$ for $1 \leq j \leq e_i$, $1 \leq i \leq r$. Let

$$d_{\mathbf{a}} = \text{LCM}\{d_{ia_i} | 1 \leq i \leq r, a_i > 0\}.$$

Then $\text{ord}_{\mathbf{p}^{\mathbf{a}}}(2) = d_{\mathbf{a}}$. Let $t_{\mathbf{a}}$ be the number $\varphi(\mathbf{p}^{\mathbf{a}})/d_{\mathbf{a}}$ and φ is the Euler φ function.

Proposition 4. *Let* $\mathbf{P}, \mathbf{e}, \mathbf{a}, d_a$ *be defined as above. Then* $\psi(\mathbf{Z}_{p^e}) = \Sigma_{0<a\le e} \frac{\varphi(p^a)}{d_a} \lfloor \frac{d_a}{2} \rfloor$

Proof: Let $H_a = \{1, 2, 2^2, \ldots, 2^{d_a - 1}\}$. Then $\langle H_a, \cdot_{p^a} \rangle$ is a subgroup of $\langle \mathbf{Z}^*_{p^a}, \cdot_{p^a} \rangle$. We have $\mathrm{ord}_{p^a}(2) = d_a$. Let $\varphi(p^a) = d_a \cdot t_a$. There exists $x_{a1}, x_{a2}, \ldots, x_{at_a}$ such that

$$\mathbf{Z}^*_{p^a} = \bigcup_{1\le i\le t_a} H_a x_{ai} \quad \text{for } 0 < a \le e.$$

Hence

$$\mathbf{Z}_{p^e} = \left(\bigcup_{0<a\le e} p^{e-a} \mathbf{Z}^*_{p^a} \right) \cup \{0\}$$
$$= \left(\bigcup_{0<a\le e} \bigcup_{1\le i\le t_a} p^{e-a} H_a x_{ai} \right) \cup \{0\}.$$

Then the digraph $G(\mathbf{Z}_{p^e})$ has distinct components G_0 and G_{ai} for $1 \le i \le t_a$ where G_0 is an isolated loop on the vertex 0 and G_{ai}, $i > 0$, is a directed cycle. i.e.,

$$G_{ai}: p^{e-a} x_{ai} \to 2p^{e-a} x_{ai} \to 2^2 p^{e-a} x_{ai} \to \cdots \to 2^{d_a - 1} p^{e-a} x_{ai} \to p^{e-a} x_{ai}$$

By lemmas 1 and 2, we have

$$\psi(\mathbf{Z}_{p^e}) = \sum_{0<a\le e} \sum_{1\le i\le t_a} \lfloor \frac{d_a}{2} \rfloor = \sum_{0<a\le e} \frac{\varphi(p^a)}{d_a} \lfloor \frac{d_a}{2} \rfloor.$$

∎

After discussing the propositions 1, 2, 3 and 4, we are ready to prove the following theorem.

Theorem 3. *Let* $\mathbf{p}, \mathbf{e}, \mathbf{a}, d_a$ *be defined as proposition 4 and* $n = 2^m p^e$. *Then*

$$\psi(\mathbf{Z}_n) = p^e \cdot \psi(\mathbf{Z}_{2^m}) + \chi(m \ \textit{is even}) \psi(\mathbf{Z}_{p^e})$$

where $\chi(S) = 1$ *if statement* S *is true;* $\chi(S) = 0$ *otherwise.*

Proof: Let us prove this theorem in the cases when m is even or odd.

(i) when m is odd, we have a partition of $\mathbf{Z}_n$ as follows

$$\mathbf{Z}_n = \left(\bigcup_{1\le k\le p^e} \bigcup_{0\le j\le \frac{m-1}{2}} \bigcup_{1\le i\le 2^{m-2-2j}} (\mathbf{A}_{ijk} \cup \mathbf{B}_{ijk}) \right) \cup \{0\}$$

where

$$A_{ijk} = \{2^{2j}(2i-1)k, 2^{2j+1}(2i-1)k\} \text{ and}$$
$$B_{ijk} = \{2^{2j}(2i-1)k + 2^{m-1}\mathbf{p}^{e}\}.$$

Every double free subset can contain one element in each of the doubleton set A_{ijk} at most. Hence

$$\psi(\mathbf{Z}_n) \le \sum_{1\le k\le \mathbf{p}^e} \sum_{0\le j\le \frac{m-1}{2}} \sum_{1\le i\le 2^{m-2-2j}} (1+1)$$
$$= \mathbf{p}^{e} \cdot \psi(\mathbf{Z}_{2^m}).$$

Let $M = \{2^{2j}(2i-1)k, 2^{j}(2i-1)k+2^{m-1}\mathbf{p}^{e} \mid 1 \le k \le \mathbf{p}^{e}, 0 \le j \le \frac{m-1}{2}$ and $1 \le i \le 2^{m-2-2j}\}$. Then M is a double-free subset of $\mathbf{Z}_n$ and $|M| = \mathbf{p}^{e} \cdot \psi(\mathbf{Z}_{2^m})$. Thus, we have $\psi(\mathbf{Z}_n) = p^{e} \cdot \psi(\mathbf{Z}_{2^m})$.

(ii) When m is even, Let $D = \{2^{m}i \mid 1 \le i < \mathbf{p}^{e}\}$ and $E = \mathbf{Z}_n - D$. Then the digraph $G(D)$ is isomophic to $G(\mathbf{Z}_{\mathbf{p}^e})$. Therefore $\psi(D) = \psi(\mathbf{Z}_{\mathbf{p}^e})$. We have a partition of E:

$$E = \left(\bigcup_{1\le k\le p^e} \bigcup_{0\le j\le \frac{m}{2}-1} \bigcup_{1\le i\le 2^{m-2-2j}} (\mathrm{A}_{ijk} \cup \mathrm{B}_{ijk}) \right) \cup \{0\}$$

where

$$A_{ijk} = \{2^{2j}(2i-1)k, 2^{2j+1}(2i-1)k\} \text{ and}$$
$$B_{ijk} = \{2^{2j}(2i-1)k + 2^{m-1}\mathbf{p}^{e}\}.$$

Every double free subset can contain one element in each of the double sets A_{ijk} at most. Hence

$$\psi(E) \le \sum_{1\le k\le \mathbf{p}^e} \sum_{0\le j\le \frac{m}{2}-1} \sum_{1\le i\le 2^{m-2-2j}} (1+1) = p^{e} \cdot \psi(\mathbf{Z}_{2^m})$$

Let $M = \{2^{2j}(2i-1)k, 2^{j}(2i-1)k + 2^{m-1}\mathbf{p}^{e} \mid 1 \le k \le \mathbf{p}^{e}, 0 \le j \le \frac{m}{2} - 1$ and $1 \le i \le 2^{m-2-j}\}$. Then M is a double-free subset of E. Thus we have $\psi(E) = \mathbf{p}^{e} \cdot \psi(\mathbf{Z}_{2^m})$.

It is obvious that

$$\psi(\mathbf{Z}_n) \le \psi(E) + \psi(D).$$

There is no edge between the element in D and the element in M. Therefore $\psi(\mathbf{Z}_n) = \psi(E) + \psi(D)$. Hence, we have

$$\psi(\mathbf{Z}_n) = \mathbf{p}^{\mathbf{e}}\psi(\mathbf{Z}_{2^m}) + \chi(m \text{ is even})\psi(\mathbf{Z}_{\mathbf{p}^{\mathbf{e}}}).$$

∎

Example 1: Figures 2 and 3 give the digraphs $G(\mathbf{Z}_{24})$ and $G(\mathbf{Z}_{28})$. We have $\psi(\mathbf{Z}_{24}) = 15$ and $\psi(\mathbf{Z}_{28}) = 16$.

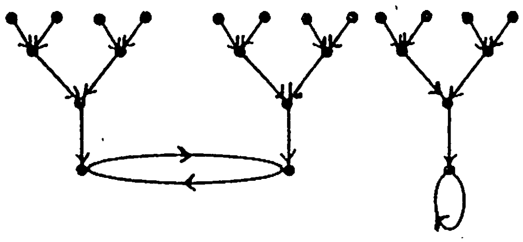

Figure 2. Digraph $G(\mathbf{Z}_{24})$

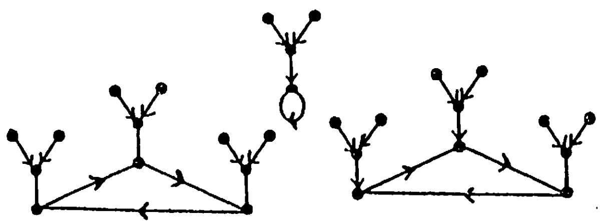

Figure 3. Digraph $G(\mathbf{Z}_{28})$

All the statements in propositions 1, 2, 3, 4 and theorem 3 can be generalized into the q-free subset for any prime q. That is

Theorem 4. *Let* $\mathbf{p} = (p_1, p_2, \ldots, p_r)$ *be a sequence of distinct primes and let* q *be a prime.* $p_i \neq q$ *for* $1 \leq i \leq r$. *Let* $\mathbf{e}$ *be a sequence of non-negative integers and* $ord_{p^e}(q) = d_{\mathbf{e}}$. *Then*

$$\psi_q(\mathbf{Z}_{q^m \cdot \mathbf{p}^m}) = \mathbf{p}^{\mathbf{e}} \cdot \psi_q(\mathbf{Z}_{q^m}) + \chi(m \textit{ is even})\psi_q(\mathbf{Z}_{\mathbf{p}^{\mathbf{e}}})$$

and

$$\psi_q(\mathbf{Z}_{q^m}) = \sum_{0 \leq i \leq \lfloor \frac{m-1}{2} \rfloor} q^{m-1-2i}.$$

We can use that same method to find $\psi_q(\mathbf{Z}_n)$ when q is not a prime but the calculation would be tedious. Therefore, we do not discuss it in detail.

4. Maximum cardinality of q-free subset of $\langle \mathbf{D}_n, + \rangle$.

A digraph is called functional if the outdegree of every vertex is equal to one. Let G be a functional digraph and let x be a vertex that belongs to $V(G)$ and let H be a functional rooted digraph with root z. Then the functional digraph $G_{x;z}H$ is the digraph obtained by identifying the two vertices x and z.

The dihedral group $\mathbf{D}_n = \{xa + yb \mid x = 0 \text{ or } 1, 0 \leq y \leq n-1\}$ with $2a = nb = 0$ and $a + b = -b + a$. Let $A = \{yb \mid 0 \leq y \leq n-1\}$ and $B = \{a + yb \mid 0 \leq y \leq n-1\}$. Then $\mathbf{D}_n = A_n \cup B_n$. The digraph $G_q(A_n)$ is isomorphic to $G_q(\mathbf{Z}_n)$. If q is odd, then the digraph $G_q(B_n)$ is made of n separate single vertex loops since $q(a + ib) = a + ib \forall 0 \leq i \leq n-1$. If q is even, then the digraph $G_g(B_n \cup \{0\})$ is a star digraph with root 0 (i.e. the directed edges set of $G_q(B_n \cup \{0\})$ is $\{\vec{z0} \mid z \in B_n\}$).

Figures 4 and 5 give the digraphs $G(\mathbf{D}_{24})$ and $G_3(\mathbf{D}_{24})$.

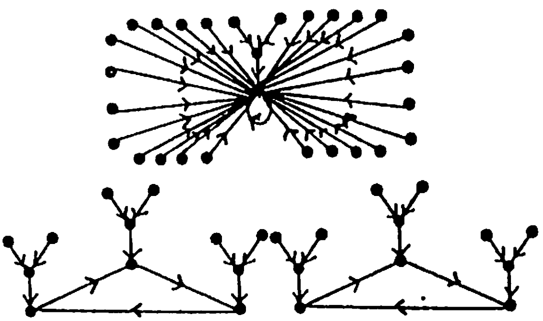

Figure 4. Digraph $G(\mathbf{D}_{24})$

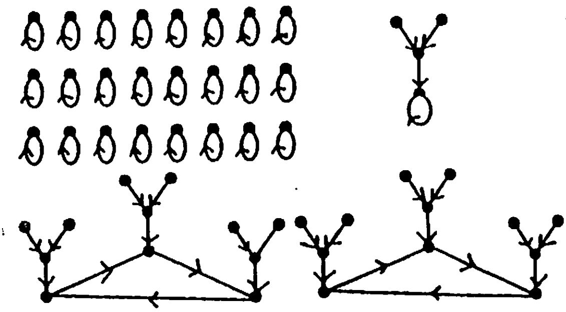

Figure 5. Digraph $G_3(\mathbf{D}_{24})$

Let us discuss the digraph $G_q(\mathbf{D}_n)$ in these cases in which q is odd or even.

Case 1: When q is odd, the digraph $G_q(\mathbf{D}_n)$ is the union of digraph $G_q(A_n)$ with n single vertex loops.

Case 2: When q is even, the digraph $G_q(\mathbf{D}_n) = G_q(A_n)0; 0G_q(B_n \cup \{0\})$.

It is known that B_n is an independent subset of $G_q(\mathbf{D}_n)$ and there are no edges between the elements in B_n and the nonzero elements in A_n. Hence, $\psi_q(\mathbf{D}_n) = \psi_q(A_n) + \psi_q(B_n)$. Thus, we obtain the following theorem.

Theorem 5.

$$\psi_q(\mathbf{D}_n) = \begin{cases} \psi_q(\mathbf{Z}_n) & \text{if } q \text{ is odd.} \\ \psi_q(\mathbf{Z}_n) + n & \text{if } q \text{ is even.} \end{cases}$$

Acknowledgement

The author would like to thank Professors P. Bouchard and E. Wang for many valuable discussions and the referee for enumerous corrections. He would also like to thank the National Science Council, Taiwan, R.O.C. for its financial support.

References

1. Crux Mathematicorum **14** (2) (1988), 35.
2. L.K. Hua, "Introduction to number theory", Springer-Verlag, New York, 1982.
3. W.D. Wallis, Anne Penfold Street, Jennifer Seberry Wallis, *Combinatorics: Room-Squares, Sum-Free Sets, Hadamard Matrices*, Lecture Notes in Mathematics **292** (1972). Springer-Verlag, New York
4. E. Wang, *On double-free sets of integers*, Ars Combinatoria **28** (1989), 97–100.