International Journal of Mathematics and
Computer Science, **17**(2022), no. 2, 647–658

Friends in $\mathbb{Z}_n$

Nicholas Gaubatz[1], **Peter Johnson**[2]

[1]Department of Mathematics & Statistics
Murray State University
Murray, Kentucky 42071, USA

[2]Department of Mathematics & Statistics
Auburn University
Auburn, Alabama 36849, USA

email: ngaubatz@murraystate.edu, johnspd@auburn.edu

(Received October 3, 2021, Accepted November 3, 2021)

Abstract

For integers $n > 1$, the n-abundancy index, analogous to the abundancy index on the positive integers, is defined on $\mathbb{Z}_n \setminus \{0\}$. Some basic results, founded on basic results about divisor sets in $\mathbb{Z}_n$, are obtained, including the result that if n is a prime power, then the n-abundancy index is one-to-one on $\mathbb{Z}_n \setminus \{0\}$.

1 Introduction

Throughout, $\mathbb{Z}$ will denote the set of integers and $\mathbb{Z}^+$ the set of positive integers. For $n \in \mathbb{Z}^+$, $n > 1$, the elements of the ring of integers modulo n will be denoted $\mathbb{Z}_n$. We allow each congruence class mod n to be represented by any integer in that congruence class. For instance, 13 and 33 represent the same congruence class in (i.e., element of) $\mathbb{Z}_{20}$; this is the same assertion as $13 \equiv 33 \pmod{20}$.

Each congruence class mod n has a representative among $0, 1, \ldots, n-1$. In the definitions in the next section, we will use these favored representatives

Key words and phrases: Abundancy index, ring of integers modulo n.
AMS (MOS) Subject Classifications: 11A07, 11A25.
This work was supported by NSF DMS grant no. 1950563.
ISSN 1814-0432, 2022, http://ijmcs.future-in-tech.net

of the elements of $\mathbb{Z}_n$. We must warn that we will be switching back and forth between $\mathbb{Z}$ and $\mathbb{Z}_n$ in these definitions—$k \in \{0, 1, \ldots, n-1\}$ may be an element of $\mathbb{Z}_n$ in one part of the definition and a plain old integer in another part. But we will take pains to make these matters clear.

As usual, $d|n$ stands for *d divides n*, which is the same as stating that *n is a multiple of d*. When this notation appears, it is understood that $d, n \in \mathbb{Z}^+$ and that the multiplication involved is the usual multiplication in the ring $\mathbb{Z}$.

On $\mathbb{Z}^+$, the *sum-of-divisors function* is defined by $\sigma(n) = \sum_{d|n} d$. The *abundancy index* of $n \in \mathbb{Z}^+$ is defined by

$$I(n) = \frac{\sigma(n)}{n}.$$

This parameter has been of interest for many decades (see [1] and [5]), not least because of its connection with the question, descending from antiquity, of *perfect numbers*, which are positive integers n such that $I(n) = 2$.

Positive integers m and n are said to be *friends* if and only if $m \neq n$ and $I(m) = I(n)$. Thus, all the perfect numbers are friends with each other. It is not known whether or not there is an infinite cohort of mutual friends; the perfect numbers are the only likely candidate, at present.

At the other end of the friendship spectrum, a positive integer $n \in \mathbb{Z}^+$ is said to be *solitary* if it has no friends. It is known (see [4]) that 1 and all prime powers are solitary. The only integers among $1, \ldots, 13$ other than 1 or prime powers are 6, 10, and 12; 6 is perfect (therefore, with quite a few friends), and 12 has at least one friend, namely, 234 [2]. At present, the leading candidate for the smallest solitary $n > 1$ which is not a prime power is 10.

In the next section we define, for $n \in \mathbb{Z}^+$, $n > 1$, the *n-abundancy index* $\overline{I_n} : (\mathbb{Z}_n \setminus \{0\}) \to \mathbb{Q} = \{\text{rational numbers}\}$. In the last section we prove some basic results about this index, culminating in a proof that if n is a prime power, then every $a \in \mathbb{Z}_n \setminus \{0\}$ is n-solitary.

2 Divisors and the Abundancy Index in $\mathbb{Z}_n$

Definition. For $a, b \in \mathbb{Z}$ such that $0 < a, b < n$ and $n \in \mathbb{Z}$ with $n \geq 2$, we say that a is an *n-divisor* of b, denoted $a|_n b$, if there exists a $d \in \mathbb{Z}_n \setminus \{0\}$ such that $da \equiv b \pmod{n}$.

We denote the set of n-divisors of b as $D_{b,n} = \{a \in \mathbb{Z} : 0 < a < n \text{ and } a|_n b\}$.

The next few lemmas state some well-known number theory facts and relate them to our notation.

Lemma 2.1. *For $a, b \in \mathbb{Z}_n \setminus \{0\}$, $a|_n b$ if and only if $(n-a)|_n b$.*

This immediately implies the following corollary:

Corollary 2.2. *Let $a, b \in \mathbb{Z}_n$. We have that $a \in D_{b,n}$ if and only if $n - a \in D_{b,n}$.*

Lemma 2.3. *Let $a, b \in \mathbb{Z}_n \setminus \{0\}$. Then $gcd(a, n)|b$ if and only if $a|_n b$.*

Proof. Let $d = gcd(a, n)$. To prove this lemma, we utilize Bézout's Identity: There exist $u, v \in \mathbb{Z}$ such that $d = ua + vn$.

($\Rightarrow$) Suppose $d|b$, with $b = cd$ for some $c \in \mathbb{Z}$. Then there exist $u, v \in \mathbb{Z}$ such that $d = au + nv \iff au \equiv d \pmod{n}$, so $b \equiv c(au) \pmod{n} \equiv a(cu) \pmod{n}$, so $a|_n b$.

($\Leftarrow$) Suppose $a|_n b$. Then there exists $c \in \mathbb{Z}_n$ such that $b \equiv ac \pmod{n}$, so there exists $y \in \mathbb{Z}$ such that $b = ac + ny$. But, $d|a$ and $d|n$, so $d|(ac + ny) = b$. □

Note that this means $a \in D_{b,n}$ if and only if $gcd(a, n)|b$. Furthermore, $D_{1,n} = \{a \in \mathbb{Z} : 0 < a < n \text{ and } gcd(a, n) = 1\}$.

It is also useful to note that for a, b, $c \in \mathbb{Z}_n \setminus \{0\}$, if $a|_n b$ and $b|_n c$, then $a|_n c$. This immediately implies that if $a \in D_{b,n}$ and $b \in D_{c,n}$, then $a \in D_{c,n}$; i.e., n-divisibility is transitive.

Definition. We define the *sum of n-divisors function* $\overline{\sigma_n} : \mathbb{Z}_n \setminus \{0\} \to \mathbb{Z}$ by

$$\overline{\sigma_n}(m) = \sum_{d|_n m} d.$$

It is important to note that this sum is taken in the ring of integers, for if the sum is taken $mod(n)$, very often it results in 0.

Example. In $\mathbb{Z}_6$, $\overline{\sigma_6}(1) = 1 + 5 = 6$ and $\overline{\sigma_6}(2) = 1 + 2 + 4 + 5 = 12$.

Definition. For $m \in \mathbb{Z}_n$, we define the *n-abundancy index of m* as

$$\overline{I_n}(m) = \frac{\overline{\sigma_n}(m)}{m}.$$

Example. In $\mathbb{Z}_6$, $\overline{I_6}(1) = \frac{6}{1} = 6$ and $\overline{I_6}(2) = \frac{12}{2} = 6$.

Definition. If $\overline{I_n}(a) = \overline{I_n}(b)$ for some $a, b \in \mathbb{Z}_n \setminus \{0\}, a \neq b$, we say that a and b are *n-friends*. A number with at least one n-friend is called *n-friendly*, while a number with no n-friends is called *n-solitary*.

Example. The following table shows 6-abundancy indices for all $m \in \mathbb{Z}_6 \setminus \{0\}$:

m	1	2	3	4	5
$\overline{I_6}(m)$	6	6	3	3	$\frac{6}{5}$

Because 1 and 2 both have 6 as their 6-abundancy indices, 1 and 2 are 6-friends. Likewise, 3 and 4 are also 6-friends. However, 5 is 6-solitary.

3 New Results

Based on everything stated so far, we can show a simple result involving p-friends, where p is any prime.

Proposition 3.1. *If p is prime, then every $m \in \mathbb{Z}_p \setminus \{0\}$ is p-solitary.*

Proof. Since $\mathbb{Z}_p$ is a field, every $a \in \mathbb{Z}_p \setminus \{0\}$ is p-divisible by every $b \in \mathbb{Z}_p \setminus \{0\}$. Therefore, $\overline{\sigma_a} = \sum_{k=1}^{p-1} k = \frac{p(p-1)}{2}$ for every $a \in \mathbb{Z}_p \setminus \{0\}$. Thus, for every a, $b \in \mathbb{Z}_p \setminus \{0\}$ such that $a \neq b$, $\overline{I_p}(a) = \frac{p(p-1)}{2a} \neq \frac{p(p-1)}{2b} = \overline{I_p}(b)$. □

Before we state our next result, let us present some notation. Let $A \subseteq \mathbb{Z}_n$ and let $k \in \mathbb{Z}$, $0 < k < n$. Denote

$$kA := \{ka \pmod{n} | a \in A\}.$$

Thus, $kA \subset \{0, 1, \ldots, n-1\}$.

We will denote $\sum A$ as the integer sum of elements of a set $A \subset \mathbb{Z}$.

Now, in view of our goal to characterize n-friend relations in generality, we first build toward a result relating 1 and 2 in $\mathbb{Z}_{2m}$, where m is odd.

Proposition 3.2. *Consider $\mathbb{Z}_{2m}$, where m is odd. Then the following statements hold:*

1) $D_{2,2m} = D_{1,2m} \cup 2D_{1,2m}$,
2) $D_{1,2m} \cap 2D_{1,2m} = \emptyset$, and
3) $|D_{1,2m}| = |2D_{1,2m}|$.

Proof. 1)

($\supseteq$) Suppose $a \in D_{1,2m}$. Then $a|_{2m}1$, so $1 \equiv ad \pmod{2m}$ for some $d \in \mathbb{Z}_{2m}$. Thus, $2 \equiv 2ad \pmod{2m} \equiv a(2d) \pmod{2m}$, so $a|_{2m}2$ and thus $a \in D_{2,2m}$.

Instead suppose $a \in 2D_{1,2m}$. Then $a \equiv 2b \pmod{2m}$ for some $b \in D_{1,2m}$; i.e., $bd \equiv 1 \pmod{2m}$ for some $d \in \mathbb{Z}_{2m}$. Thus, $ad \equiv 2bd \pmod{2m} \equiv 2 \pmod{2m}$, so $a|_{2m}2$ and thus $a \in D_{2,2m}$.

($\subseteq$) Now suppose $a \in D_{2,2m}$; that is, $a|_{2m}2$. By Lemma 2.3, $gcd(a, 2m)|2$. This means that $gcd(a, 2m) = 1$ or $gcd(a, 2m) = 2$.

If $gcd(a, 2m) = 1$, then $a|_{2m}1$, so $a \in D_{1,2m}$.

If $gcd(a, 2m) = 2$, then $2|a$, so a is even with $a = 2c$ for some $c \in \mathbb{Z}^+$. Since $1 < a < 2m$, we have that $1 \leq c < m$; also, $gcd(c, m) = 1$.

If c is odd, then $gcd(c, 2m) = 1$, so $a = 2c \in 2D_{1,2m}$. So, suppose c is even. Since m is odd, $m + c$ is also odd. Therefore, $gcd(m + c, 2m) = 1$; also, $1 \leq m + c < 2m$. Consequently, $m + c \in D_{1,2m}$. Therefore, $a = 2c \equiv 2(m + c) \pmod{2m} \in 2D_{1,2m}$.

2) Suppose $a \in D_{1,2m}$. Then $a|_{2m}1$, so $gcd(a, 2m)|1 \Rightarrow gcd(a, 2m) = 1$, so a must be odd. Now, note that all elements of $2D_{1,2m}$ are even, since if $b \in 2D_{1,2m}$ then there exists a $c \in D_{1,2m}$ such that $b \equiv 2c \pmod{2m} \Rightarrow b = 2c + 2mv = 2(c + mv)$ for some $v \in \mathbb{Z}$. Therefore, $a \notin 2D_{1,2m}$, so $D_{1,2m} \cap 2D_{1,2m} = \emptyset$.

3) Consider the map $\phi : D_{1,2m} \to 2D_{1,2m}$, $\phi(a) \equiv 2a \pmod{2m}$. We will show that ϕ is a bijection.

(*Injection:*) Suppose $\phi(a) \equiv \phi(b) \pmod{2m}$ for some $a, b \in D_{1,2m}$. By the above, both a and b are odd. Then $2a \equiv 2b \pmod{2m}$ implies that $2(a - b) \equiv 0 \pmod{2m}$. Thus, $a - b \equiv 0 \pmod{2m}$, in which case $a \equiv b \pmod{2m}$ and we are done, or $a - b \equiv m \pmod{2m}$, in which case a and b being odd means that m is even, a contradiction. Thus, ϕ is injective.

(*Surjection:*) By definition, if $a \in 2D_{1,2m}$, then $a \equiv 2b \pmod{2m}$ for some $b \in D_{1,2m}$. Thus, ϕ is surjective.

Therefore, $|D_{1,2m}| = |2D_{1,2m}|$. □

We are now ready to state our first "new" result.

Theorem 3.3. *If m is odd, then 1 and 2 are $2m$-friends.*

Proof. Note that $\overline{I_{2m}}(1) = \overline{\sigma_{2m}}(1) = \sum D_{1,2m}$. We will show that $\sum 2D_{1,2m} = \sum D_{1,2m}$; this, in view of Proposition 3.2, will prove the theorem's claim.

To this end, recall that by Corollary 2.2, $a \in D_{1,2m}$ if and only if $2m - a \in D_{1,2m}$, so $D_{1,2m} = \{a_1, \ldots, a_k, 2m - a_1, \ldots, 2m - a_k\}$ for some $k \in \mathbb{Z}$, where

we arrange the elements so that $1 \leq a_1, \ldots, a_k < m$. Thus, $\sum D_{1,2m} = a_1 + \cdots + a_k + (2m - a_1) + \cdots + (2m - a_k) = k(2m)$.

Furthermore, since arrangements have been made so that $1 \leq a_1, \ldots, a_k < m$, we have that $2 \leq 2a_j < 2m$, for all $j = 1, \ldots, k$. Meanwhile, $2(2m - a_j) = 4m - 2a_j \equiv 2m - 2a_j \pmod{2m}$, and $0 < 2m - 2a_j < 2m$. Therefore, $2D_{1,2m} = \{2a_1, \ldots, 2a_k, 2m - 2a_1, \ldots, 2m - 2a_k\}$, where each of the $2k$ integers listed are distinct because $|D_{1,2m}| = |2D_{1,2m}|$. Therefore,

$$\sum 2D_{1,2m} = \sum_{j=1}^{k} 2a_j + \sum_{j=1}^{k} (2m - 2a_j) = k(2m) = \sum D_{1,2m}.$$

Thus, $\sum D_{2,2m} = \sum (D_{1,2m} \cup 2D_{1,2m}) = \sum D_{1,2m} + \sum 2D_{1,2m} = 2\sum D_{1,2m}$ since $D_{1,2m}$ and $2D_{1,2m}$ are disjoint. Therefore, 1 and 2 are $2m$-friends. □

Now that we have established the result that 1 and 2 are $2m$-friends for any odd m, we must build up some more theory before trying to tackle any other cases. The following lemma is essential for constructing $mD_{1,n}$ for any m and n.

Lemma 3.4. *Suppose a, b, and $m > 1$ are positive integers and $gcd(m, b) = 1$. Then at least one of the integers $a + kb$, $0 \leq k \leq m - 1$, is relatively prime to m.*

Proof. We will show that the congruence classes modulo m of the integers $a, a + b, \ldots, a + (m - 1)b$ are distinct.

Suppose $0 \leq k < q \leq m - 1$ with $a + kb \equiv a + qb \pmod{m}$. Then $m|(q - k)b \implies m|(q - k)$ since $gcd(m, b) = 1$. But $1 \leq q - k \leq m - 1$, so it is impossible that $m|(q - k)$.

Therefore, the congruence classes of the integers $a + kb$, $0 \leq k \leq m - 1$, are distinct. Since there are m of these congruence classes, it must be that $a + kb \equiv 1 \pmod{m}$ for some $k \in \{0, \ldots, m - 1\}$. Thus, $gcd(a + kb, m) = 1$. □

In fact, the conclusion of the previous lemma can be sharpened to the following: $\varphi(m)$ of the integers $a + kb$, $0 \leq k \leq m - 1$, are relatively prime to m, where φ is Euler's totient function.

Proposition 3.5. *Let $m \in \mathbb{Z}$, with $0 < m < n$. If $m|n$, then*

$$mD_{1,n} = \{d \in \mathbb{Z} | 0 < d < n \text{ and } gcd(d, n) = m\}.$$

Proof. ($\subseteq$) Suppose $d \in mD_{1,n}$. Then $d \equiv mj \pmod{n}$ for some $j|_n 1$. Thus, $d = mj+nv$ for some $v \in \mathbb{Z}$; but, $m|m$ and $m|n$, so $m|d$. Thus, $gcd(d,n) \geq m$. However, since $j|_n 1$, $1 \equiv jl \pmod{n}$ for some $l \in \mathbb{Z}$, so $m \equiv mjl \pmod{n} \equiv dl \pmod{n}$, so $d|_n m$, which implies that $gcd(d,n)|m$ and thus $gcd(d,n) \leq m$. Therefore, $gcd(d,n) = m$.

($\supseteq$) Suppose that n, d, and m are positive integers satisfying $0 < d < n$ and $m = gcd(d,n)$. Let integers c and t be defined by $d = mc$ and $n = mt$. Then $gcd(c,t) = 1$.

We will show that $d \equiv mx \pmod{n}$ for some $x \in \{1, \ldots, n-1\}$ satisfying $gcd(x,n) = 1$.

Using the Unique Factorization Theorem, we can refactor n as $n = MT$, in which $M|m$, $t|T$, and $gcd(M,T) = 1$; also, every prime divisor of T is a prime divisor of t. Because $gcd(c,t) = 1$, it follows that $gcd(c,T) = 1$.

We will look for x in the arithmetic progression $c + kT$, $0 \leq k \leq M-1$. Observe that for all such k, $m(c+kT) = mc+kmT = d+kmT \equiv d \pmod{n}$, because $t|T$ implies that $n = mt|kmT$. Therefore, it will suffice to show the existence of $k \in \{0, \ldots, M-1\}$ such that $gcd(c+kT, n) = 1$.

Since $gcd(M,T) = 1$, Lemma 3.4 allows us to conclude that $gcd(c + kT, M) = 1$ for some $k' \in \{0, \ldots, M-1\}$. But since $n = MT$, it follows that $gcd(c+k'T, n) = gcd(c+k'T, T)$. But, any common divisor of T and $c+k'T$ must divide c, so $gcd(c+k'T, T) = gcd(c,T) = 1$. □

The following corollary is a generalization of parts (1) and (2) of Proposition 3.2:

Corollary 3.6. *Suppose $k \in \mathbb{Z}$ with $0 < k < n$, and let M be the set of all positive integers m such that $m|k$ and $m|n$. Then*

1)

$$D_{k,n} = \bigcup_{m \in M} mD_{1,n}.$$

2)

$$mD_{1,n} \cap m'D_{1,n} = \emptyset \text{ for all } m, m' \in M, m \neq m'.$$

Proof. 1) ($\subseteq$) Suppose $a \in D_{k,n}$. Then by Lemma 2.3, $gcd(a,n)|k$. Let $m_a = gcd(a,n)$. Then $a \in m_a D_{1,n}$ by Proposition 3.5, where $m_a|k$ and $m_a|n$ implies that $m_a \in M$.

($\supseteq$) If $a \in mD_{1,n}$ for some $m \in \mathbb{Z}$ with $m|k$ and $m|n$, then $a \equiv mj \pmod{n}$ for some $j|_n 1$ and $k = mp$ for some $p \in \mathbb{Z}$. Thus, $jl \equiv 1 \pmod{n}$ for some

$l \in \mathbb{Z}$, so

$$\begin{aligned} k &= mp \\ &\equiv m(jl)p \pmod{n} \\ &\equiv a(lp) \pmod{n}, \end{aligned}$$

so $a|_n k$ and thus $a \in D_{k,n}$.

2) By way of contradiction, suppose there exists an a such that $a \in m_1 D_{1,n}$ and $a \in m_2 D_{1,n}$, where $m_1 \neq m_2$. Then by Proposition 3.5, $gcd(a,n) = m_1$ and $gcd(a,n) = m_2$, so $m_1 = m_2$. □

Indeed, if we let $k = 2$ and $n = 2m$ for an odd $m \in \mathbb{Z}$, then by Corollary 3.6 we get parts (1) and (2) of Proposition 3.2.

Example. Consider $\mathbb{Z}_{12}$:

$$\begin{aligned} D_{1,12} &= \{1,5,7,11\} \\ 2D_{1,12} &= \{2,10\} \\ 3D_{1,12} &= \{3,9\} \\ 4D_{1,12} &= \{4,8\} \\ 6D_{1,12} &= \{6\} \end{aligned}$$

Indeed,

$$\begin{aligned} D_{1,12} &= \{1,5,7,11\} \\ D_{2,12} &= \{1,2,5,7,10,11\} = D_{1,12} \cup 2D_{1,12} \\ D_{3,12} &= \{1,3,5,7,9,11\} = D_{1,12} \cup 3D_{1,12} \\ D_{4,12} &= \{1,2,4,5,7,8,10,11\} = D_{1,12} \cup 2D_{1,12} \cup 4D_{1,12} \\ D_{5,12} &= \{1,5,7,11\} = D_{1,12} \\ D_{6,12} &= \{1,2,3,5,6,7,9,10,11\} = D_{1,12} \cup 2D_{1,12} \cup 3D_{1,12} \cup 6D_{1,12} \\ D_{7,12} &= \{1,5,7,11\} = D_{1,12} \\ D_{8,12} &= \{1,2,4,5,7,8,10,11\} = D_{1,12} \cup 2D_{1,12} \cup 4D_{1,12} \\ D_{9,12} &= \{1,3,5,7,9,11\} = D_{1,12} \cup 3D_{1,12} \\ D_{10,12} &= \{1,2,5,7,10,11\} = D_{1,12} \cup 2D_{1,12} \\ D_{11,12} &= \{1,5,7,11\} = D_{1,12} \end{aligned}$$

Proposition 3.7. *For any integer $n \geq 2$ with prime factorization $n = p_1^{k_1} \cdots p_r^{k_r}$,*

$$\overline{I_n}(1) = \sum D_{1,n} = \frac{1}{2}(p_1^{2k_1-1}(p_1-1) \cdots p_r^{2k_r-1}(p_r-1)).$$

Proof. Consider Euler's totient function $\varphi(n)$, the number of positive integers $k < n$ such that k is relatively prime to n. Then, by definition, $|D_{1,n}| = \varphi(n)$.

It is well-known that

$$\varphi(n) = p_1^{k_1-1}(p_1 - 1) \cdots p_r^{k_r-1}(p_r - 1).$$

Next, note that by Corollary 2.2, the values of $D_{1,n}$ come in pairs, each summing to n. Thus, the average of the values of $D_{1,n}$ is equal to $\frac{n}{2}$. Therefore, to get $\sum D_{1,n}$ we take the average and multiply it with the cardinality to get that

$$\begin{aligned}
\overline{I_n}(1) &= \sum D_{1,n} \\
&= \frac{n}{2} \cdot |D_{1,n}| \\
&= \frac{n}{2} \cdot \varphi(n) \\
&= \frac{p_1^{k_1} \cdots p_r^{k_r}}{2} \cdot (p_1^{k_1-1}(p_1 - 1) \cdots p_r^{k_r-1}(p_r - 1)) \\
&= \frac{1}{2} p_1^{2k_1-1}(p_1 - 1) \cdots p_r^{2k_r-1}(p_r - 1).
\end{aligned}$$

□

Examples.

$$\begin{aligned}
\overline{I_6}(1) &= 1 + 5 = 6 = \frac{1}{2}(2 \cdot 1 \cdot 3 \cdot 2). \\
\overline{I_{10}}(1) &= 1 + 3 + 7 + 9 = 20 = \frac{1}{2}(2 \cdot 1 \cdot 5 \cdot 4). \\
\overline{I_{12}}(1) &= 1 + 5 + 7 + 11 = 24 = \frac{1}{2}(2^3 \cdot 1 \cdot 3 \cdot 2). \\
\overline{I_{32}}(1) &= \frac{1}{2}(2^9 \cdot 1) = 256.
\end{aligned}$$

Note in the case that the power of each prime in the prime factorization of n is 1 (i.e., $k_i = 1$ for all $1 \leq i \leq r$), $\overline{I_n}(1) = \frac{1}{2}(p_1(p_1 - 1) \cdots p_r(p_r - 1)) = \frac{n}{2}((p_1 - 1) \cdots (p_r - 1))$.

Lemma 3.8. *If p is prime and $j, k \in \mathbb{Z}$ with $0 \leq j < k$, then*

$$|p^j D_{1,p^k}| = p^{k-(j+1)}(p - 1).$$

Proof. By Proposition 3.5, $d \in p^j D_{1,p^k}$ for some $0 \leq j < k$ if and only if $0 < d < p^k$ and $gcd(d, p^k) = p^j$. There are exactly $p^{k-j-1}(p-1)$ such $d < p^k$ satisfying this requirement, which completes the proof. □

Example. Consider $\mathbb{Z}_{27}$:

$$\begin{aligned} D_{1,27} &= \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\} \\ 3D_{1,27} &= \{3, 6, 12, 15, 21, 24\} \\ 9D_{1,27} &= \{9, 18\}. \end{aligned}$$

Indeed,

$$\begin{aligned} |D_{1,27}| &= 18 = 3^2(3-1) \\ |3D_{1,27}| &= 6 = 3^1(3-1) \\ |9D_{1,27}| &= 2 = 3^0(3-1). \end{aligned}$$

Corollary 3.9. *If p is prime and $m, k \in \mathbb{Z}^+$ with $0 \leq m < k$, then*

$$\sum D_{p^m,p^k} = \frac{1}{2} p^{2k-(m+1)}(p^{m+1} - 1).$$

Proof. Applying Corollary 3.6 and Lemma 3.8,

$$\begin{aligned} \sum D_{p^m,p^k} &= \sum \Big(\bigcup_{i=0}^{m} p^i D_{1,p^k} \Big) \\ &= \sum_{i=0}^{m} \Big(\sum p^i D_{1,p^k} \Big) \\ &= \sum_{i=0}^{m} \frac{p^k}{2} |p^i D_{1,p^k}| \\ &= \frac{p^k}{2} \sum_{i=0}^{m} p^{k-(i+1)}(p-1) \\ &= \frac{p^k}{2} p^{k-(m+1)} \sum_{i=0}^{m} (p^{m-i})(p-1) \\ &= \frac{1}{2} p^{2k-(m+1)}(p^{m+1} - 1). \end{aligned}$$

□

Lemma 3.10. *Let $a, b, n \in \mathbb{Z}^+$ with $b < a < n$ and $b|n$. If $a \in bD_{1,n}$, then $D_{a,n} = D_{b,n}$.*

Proof. Suppose $a \equiv bc \pmod{n}$ for some $c \in D_{1,n}$, where $cd \equiv 1 \pmod{n}$ for some $d \in \mathbb{Z}$.

($\subseteq$) Suppose $m \in D_{a,n}$. Then $mk \equiv a \pmod{n}$ for some $k \in \mathbb{Z}$. Thus, b $\equiv bcd \pmod{n} \equiv ad \pmod{n} \equiv mkd \pmod{n}$, so $m|_n b$, and thus $m \in D_{b,n}$.

($\supseteq$) Suppose $m \in D_{b,n}$. Then $m|_n b$, which implies that $ml \equiv b \pmod{n}$ for some $l \in \mathbb{Z}$, so $bc \equiv mlc \pmod{n} \implies a = bc \equiv mlc \pmod{n}$, and thus $m|_n a$. □

We are now ready to characterize friendliness in rings $\mathbb{Z}_n$ of cardinality equal to a prime power.

Theorem 3.11. *If p is prime and $k \in \mathbb{Z}^+$, then every $a \in \mathbb{Z}_{p^k} \setminus \{0\}$ is p^k-solitary.*

Proof. Let $a \in p^j D_{1,p^k}$ for some $0 \leq j < k$; then by Lemma 3.10, $D_{a,p^k} = D_{p^j,p^k}$. We will show that a has no p^k-friends.

Consider b with $0 < b < p^k$ and $b \neq a$.

Suppose $b \in p^j D_{1,p^k}$. In this case, by Lemma 3.10 we have that $D_{b,p^k} = D_{p^j,p^k} = D_{a,p^k}$. Thus,

$$\begin{aligned}
\overline{I_{p^k}}(a) &= \frac{\overline{\sigma_{p^k}}(a)}{a} \\
&= \frac{\sum D_{a,p^k}}{a} \\
&= \frac{\sum D_{b,p^k}}{a} \\
&\neq \frac{\sum D_{b,p^k}}{b} \\
&= \overline{I_{p^k}}(b).
\end{aligned}$$

This takes care of $b \in p^j D_{1,p^k}$.

Now, suppose $b \in p^i D_{1,p^k}$, where $i \neq j$. Then by Lemma 3.10, $D_{b,p^k} = D_{p^i,p^k}$, so by Corollary 3.9,

$$\overline{I_{p^k}}(b) = \frac{p^{2k-(i+1)}(p^{i+1}-1)}{2b}.$$

Thus, if $\overline{I_{p^k}}(a) = \overline{I_{p^k}}(b)$, then

$$\frac{p^{2k-(j+1)}(p^{j+1}-1)}{2a} = \frac{p^{2k-(i+1)}(p^{i+1}-1)}{2b},$$

which implies that $a(1-p^{-(i+1)}) = b(1-p^{-(j+1)})$. But, $a \in p^j D_{1,p^k}$ and $b \in p^i D_{1,p^k}$, so by Proposition 3.5 we have that $gcd(a,p^k) = p^j$ and $gcd(b,p^k) = p^i$. Thus, $a = a'p^j$ for some integer a' with $0 < a' < p^{k-j}$ and $p \nmid a'$, and $b = b'p^i$ for some integer b' with $0 < b' < p^{k-i}$ and $p \nmid b'$.

Therefore,

$$\begin{aligned} a(1-p^{-(i+1)}) &= b(1-p^{-(j+1)}) \\ \implies ap^{j+1}(p^{i+1}-1) &= bp^{i+1}(p^{j+1}-1) \\ \implies a(p^{i+j+2}-p^{j+1}) &= b(p^{i+j+2}-p^{i+1}) \\ \implies a'(p^{i+2j+2}-p^{2j+1}) &= b'(p^{2i+j+2}-p^{2i+1}) \\ \implies a'p^{2j}(p^{i+1}-1) &= b'p^{2i}(p^{j+1}-1). \end{aligned}$$

Without loss of generality, assume $i < j$. Then

$$a'p^{2(j-1)}(p^{i+1}-1) = b'(p^{j+1}-1).$$

Now, p divides the left side but not the right side, a contradiction. Therefore, $\overline{I_{p^k}}(a) \neq \overline{I_{p^k}}(b)$ for all $0 < b < p^k$ with $a \neq b$, so a is p^k-solitary.

□

The natural question to ask next is does the converse of the statement hold? That is, do n-friends necessarily exist when n is not a prime power? In addition, is there any connection between the notion of n-friends and friends in the regular integers?

References

[1] P. Erdős, On the distribution of numbers of the form $\sigma(n)/n$ and on some related questions, Pacific J. Math 52 (1), 1974.

[2] Doyon Kim, Friends of 12, Alabama Journal of Mathematics (ajmonline) 39 (2015), 3 pp.

[3] R. Laatsch, Measuring the abundancy of integers, Math. Magazine 59 (1986), 84-92.

[4] Jeffrey Ward, Does ten have a friend?, International Journal of Mathematics and Computer Science 3 (2008), 153-158.

[5] P.A. Weiner, The abundancy ratio, a measure of perfection, Math. Magazine 73 (2000), 307-310.