Scientia Magna
Vol. 2 (2006), No. 3, 1-25

A note on the Pseudo-Smarandache function

A.A.K. Majumdar[1]

Department of Mathematics, Jahangirnagar University,
Savar, Dhaka 1342, Bangladesh

Abstract This paper gives some results and observations related to the Pseudo-Smarandache function $Z(n)$. Some explicit expressions of $Z(n)$ for some particular cases of n are also given.

Keywords The Pseudo-Smarandache function, Smarandache perfect square, equivalent.

§1. Introduction

The Pseudo-Smarandache function $Z(n)$, introduced by Kashihara [1], is as follows :

Definition 1.1. For any integer $n \geq 1$, $Z(n)$ is the smallest positive integer m such that $1 + 2 + \cdots + m$ is divisible by n. Thus,

$$Z(n) = \min\left\{m : m \in \mathrm{N} : n \mid \frac{m(m+1)}{2}\right\}. \qquad (1.1)$$

As has been pointed out by Ibstedt [2], an equivalent definition of $Z(n)$ is

Definition 1.2.

$$Z(n) = \min\{k : k \in \mathrm{N} : \sqrt{1+8kn} \text{ is a perfect square}\}.$$

Kashihara [1] and Ibstedt [2] studied some of the properties satisfied by $Z(n)$. Their findings are summarized in the following lemmas:

Lemma 1.1. For any $m \in N$, $Z(n) \geq 1$. Moreover, $Z(n) = 1$ if and only if $n = 1$, and $Z(n) = 2$ if and only if $n = 3$.

Lemma 1.2. For any prime $p \geq 3$, $Z(p) = p - 1$.

Lemma 1.3. For any prime $p \geq 3$ and any $k \in N$, $Z(p^k) = p^k - 1$.

Lemma 1.4. For any $k \in N$, $Z(2^k) = 2^{k+1} - 1$.

Lemma 1.5. For any composite number $n \geq 4$, $Z(n) \geq \max\{Z(N) : N \mid n\}$.

In this paper, we give some results related to the Pseudo-Smarandache function $Z(n)$.

In §2, we present the main results of this paper. Simple explicit expressions for $Z(n)$ are available for particular cases of n. In Theorems $2.1 - 2.11$, we give the expressions for $Z(2p)$, $Z(3p)$, $Z(2p^2)$, $Z(3p^3)$, $Z(2p^k)$, $Z(3p^k)$, $Z(4p)$, $Z(5p)$, $Z(6p)$, $Z(7p)$ and $Z(11p)$, where p is a prime and $k(\geq 3)$ is an integer. Ibstedt [2] gives an expression for $Z(pq)$ where p and q are distinct primes. We give an alternative expressions for $Z(pq)$, which is more efficient from the computational point of view. This is given in Theorem 2.12, whose proof shows that the solution of $Z(pq)$ involves the solution of two Diophantine equations. Some particular cases of Theorem

[1]On Sabbatical leave from: Ritsumeikan Asia-Pacific University, 1-1 Jumonjibaru, Beppu-shi, Oita-ken, Japan.

2.12 are given in Corollaries 2.1 – 2.16. We conclude this paper with some observations about the properties of $Z(n)$, given in four Remarks in the last §3.

§2. Main Results

We first state and prove the following results.

Lemma 2.1. Let $n = \frac{k(k+1)}{2}$ for some $k \in N$. Then, $Z(n) = k$.

Proof. Noting that $k(k+1) = m(m+1)$ if and only if $k = m$, the result follows. The following lemma gives lower and upper bounds of $Z(n)$.

Lemma 2.2. $3 \leq n \leq 2n - 1$ for all $n \geq 4$.

Proof. Letting $f(m) = \frac{m(m+1)}{2}, m \in N$, see that $f(m)$ is strictly increasing in m with $f(2) = 3$. Thus, $Z(n) = 2$ if and only if $n = 3$. This, together with Lemma 1.1, gives the lower bound of $Z(n)$ for $n \geq 4$. Again, since $n \mid f(2n-1)$, it follows that $Z(n)$ cannot be greater than $2n - 1$. Since $Z(n) = 2n - 1$ if $n = 2k$ for some $k \in N$, it follows that the upper bound of $Z(n)$ in Lemma 2.2 cannot be improved further. However, the lower bound of $Z(n)$ can be improved. For example, since $f(4) = 10$, it follows that $Z(n) \geq 5$ for all $n \geq 11$. A better lower bound of $Z(n)$ is given in Lemma 1.5 for the case when n is a composite number. In Theorems 2.1 – 2.4, we give expressions for $Z(2p), Z(3p), Z(2p^2)$ and $Z(3p^2)$ where $p \geq 5$ is a prime. To prove the theorems, we need the following results.

Lemma 2.3. Let p be a prime. Let an integer $n(\geq p)$ be divisible by p^k for some integer $k(\geq 1)$. Then, p^k does not divide $n + 1$ (and $n - 1$).

Lemma 2.4. $6 \mid n(n+1)(n+2)$ for any $n \in N$. In particular, $6 \mid (p^2 - 1)$ for any prime $p \geq 5$.

Proof. The first part is a well-known result. In particular, for any prime $p \geq 5$, $6 \mid (p-1)p(p+1)$. But since $p(\geq 5)$ is not divisible by 6, it follows that $6 \mid (p-1)(p+1)$.

Theorem 2.1. If $p \geq 5$ is a prime, then

$$Z(2p) = \begin{cases} p - 1, & \text{if } 4 \mid (p-1); \\ p, & \text{if } 4 \mid (p+1). \end{cases}$$

Proof.

$$Z(2p) = \min\left\{m : 2p \mid \frac{m(m+1)}{2}\right\} = \min\left\{m : p \mid \frac{m(m+1)}{4}\right\}. \tag{1}$$

If $p \mid m(m+1)$, then p must divide either m or $m + 1$, but not both (by Lemma 2.3). Thus, the minimum m in (1) may be taken as $p - 1$ or p depending on whether $p - 1$ or $p + 1$ respectively is divisible by 4. We now consider the following two cases that may arise :

Case 1 : p is of the form p=4a+1 for some integer $a \geq 1$. In this case, $4 \mid (p-1)$, and hence, $Z(2p) = p - 1$.

Case 2 : p is of the form $p = 4a + 3$ for some integer $a \geq 1$. Here, $4 \mid (p+1)$ and hence, $Z(2p) = p$.

Theorem 2.2. If $p \geq 5$ is a prime, then

$$Z(3p) = \begin{cases} p-1, & \text{if } 3 \mid (p-1); \\ p, & \text{if } 3 \mid (p+1). \end{cases}$$

Proof.

$$Z(3p) = \min\left\{m : 3p \mid \frac{m(m+1)}{2}\right\} = \min\left\{m : p \mid \frac{m(m+1)}{6}\right\}. \tag{2}$$

If $p \mid m(m+1)$, then p must divide either m or m+1, but not both (by Lemma 2.3). Thus, the minimum m in (2) may be taken as $p-1$ or p according as $p-1$ or $p+1$ respectively is divisible by 6. But, since both $p-1$ and $p+1$ are divisible by 2, it follows that the minimum m in (2) may be taken as $p-1$ or p according as $p-1$ or $p+1$ respectively is divisible by 3.

We now consider the following two possible cases that may arise :

Case 1 : p is of the form $p = 3a+1$ for some integer $a \geq 1$. In this case, $3 \mid (p-1)$, and hence, $Z(3p) = p-1$.

Case 2 : p is of the form $p = 3a+2$ for some integer $a \geq 1$. Here, $3 \mid (p+1)$, and hence, $Z(3p) = p$.

Theorem 2.3. If $p \geq 3$ is a prime, then $Z(2p^2) = p^2 - 1$.

Proof.

$$Z(2p^2) = \min\left\{m : 2p^2 \mid \frac{m(m+1)}{2}\right\} = \min\left\{m : p^2 \mid \frac{m(m+1)}{4}\right\}. \tag{3}$$

If $p^2 | m(m+1)$, then p^2 must divide either m or $m+1$, but not both (by Lemma 2.3). Thus, the minimum m in (3) may be taken as p^2-1 if p^2-1 is divisible by 4. But, since both $p-1$ and $p+1$ are divisible by 2, it follows that $4 \mid (p-1)(p+1)$. Hence, $Z(2p^2) = p^2 - 1$.

Theorem 2.4. If $p \geq 5$ is a prime, then $Z(3p^2) = p^2 - 1$.

Proof.

$$Z(3p^2) = \min\left\{m : 3p^2 \mid \frac{m(m+1)}{2}\right\} = \min\left\{m : p^2 \mid \frac{m(m+1)}{6}\right\}. \tag{4}$$

If $p^2 | m(m+1)$, then p^2 must divide either m or $m+1$, but not both (by Lemma 2.3). Thus, the minimum m in (4) may be taken as $p^2 1$ if p^2-1 is divisible by 6. By Lemma 2.4, $6 \mid (p^2-1)$. Consequently, $Z(2p^2) = p^2 - 1$.

Definition 2.1. A function $g : \mathrm{N} \to \mathrm{N}$ is called multiplicative if and only if $g(n_1 n_2) = g(n_1) g(n_2)$ for all $n_1, n_2 \in N$ with $(n_1, n_2) = 1$.

Remark 2.1. From Lemma 1.2 and Theorem 2.1, we see that $Z(2p) \neq 3(p-1) = Z(2)Z(p)$ for any odd prime p. Moreover, $Z(3p^2) = p^2 - 1 \neq Z(2p^2) + Z(p^2)$. These show that $Z(n)$ is neither additive nor multiplicative, as has already been noted by Kashihara [1]. The expressions for $Z(2p^k)$ and $Z(3p^k)$ for $k \geq 3$ are given in Theorem 2.5 and Theorem 2.6 respectively. For the proofs, we need the following results:

Lemma 2.5.

(1) 4 divides $3^2 k - 1$ for any integer $k \geq 1$.

(2) 4 divides $3^{2k+1} + 1$ for any integer $k \geq 0$.

Proof.

(1) Writing $3^{2k} - 1 = (3k-1)(3k+1)$, the result follows immediately.

(2) The proof is by induction on k. The result is clearly true for $k = 0$. So, we assume that the result is true for some integer k, so that 4 divides $3^{2k+1} + 1$ for some k. Now, since $3^{2k+3} + 1 = 9(3^{2k+1} + 1) - 8$, it follows that 4 divides $3^{2k+3} + 1$, completing the induction.

Lemma 2.6.

(1) 3 divides $2^2k - 1$ for any integer $k \geq 1$.

(2) 3 divides $2^{2k+1} + 1$ for any integer $k \geq 0$.

Proof.

(1) By Lemma 2.4, 3 divides $(2k-1)2k(2k+1)$. Since 3 does not divide $2k$, 3 must divide $(2k-1)(2k+1) = 2^2k - 1$.

(2) The result is clearly true for $k = 0$. To prove by induction, the induction hypothesis is that 3 divides $2^{2k+1} + 1$ for some k. Now, since $2^{2k+3} + 1 = 4(3^{2k+1} + 1) - 3$, it follows that 3 divides $2^{2k+3} + 1$, so that the result is true for $k + 1$ as well, completing the induction.

Theorem 2.5. If $p \geq 3$ is a prime and $k \geq 3$ is an integer, then

$$Z(2p^k) = \begin{cases} p^k, & \text{if } 4 \mid (p-1) \text{ and } k \text{ is odd;} \\ p^k - 1, & \text{otherwise.} \end{cases}$$

Proof.

$$Z(2p^k) = \min\left\{m : 2p^k \mid \frac{m(m+1)}{2}\right\} = \min\left\{m : p^k \mid \frac{m(m+1)}{4}\right\}. \tag{5}$$

If $p^k | m(m+1)$, then p^k must divide either m or $m+1$, but not both (by Lemma 2.3). Thus, the minimum m in (5) may be taken as $p^k - 1$ or p^k according as $p^k - 1$ or p^k is respectively divisible by 4. We now consider the following two possibilities:

Case 1 : p is of the form $4a + 1$ for some integer $a \geq 1$. In this case, $p^k = (4a+1)^k = (4a)^k + C_k^1(4a)^{k-1} + \cdots + C_k^{k-1}(4a) + 1$, showing that $4 \mid (p^k - 1)$. Hence, in this case, $Z(2p^k) = p^k - 1$.

Case 2 : p is of the form $4a + 3$ for some integer $a \geq 1$. Here, $p^k = (4a+3)k = (4a)^k + C_k^1(4a)^{k-1}3 + \cdots + C_k^{k-1}(4a)3^{k-1} + 3^k$.

(1) If $k \geq 2$ is even, then by Lemma 2.5, $4 \mid (3^k - 1)$, so that $4 \mid (p^k - 1)$. Thus, $Z(2p^k) = p^k - 1$.

(2) If $k \geq 3$ is odd, then by Lemma 2.5, $4 \mid (3^k + 1)$, and so $4 \mid (p^k + 1)$. Hence, $Z(2p^k) = p^k$. All these complete the proof of the theorem.

Theorem 2.6. If $p \geq 3$ is a prime and $k \geq 3$ is an integer, then

$$Z(3p^k) = \begin{cases} p^k, & \text{if } 3 \mid (p+1) \text{ and } k \text{ is odd;} \\ p^k - 1, & \text{otherwise.} \end{cases}$$

Proof.

$$Z(3p^k) = \min\left\{m : 3p^k \mid \frac{m(m+1)}{2}\right\} = \min\left\{m : p^k \mid \frac{m(m+1)}{6}\right\}. \tag{6}$$

If $p^k|m(m+1)$, then p^k must divide either m or $m+1$, but not both (by Lemma 2.3). Thus, the minimum m in (6) may be taken as p^k-1 or p^k according as p^k-1 or p^k is respectively divisible by 6. We now consider the following two possible cases:

Case 1 : p is of the form $3a+1$ for some integer $a \geq 1$. In this case, $p^k = (3a+1)^k = (3a)^k + C_k^1(3a)^{k-1} + \cdots + C_k^{k-1}(3a) + 1$, it follows that $3 \mid (p^k-1)$. Thus, in this case, $Z(3p^k) = p^k - 1$.

Case 2 : p is of the form $3a+2$ for some integer $a \geq 1$. Here, $p^k = (3a+2)k = (3a)^k + C_k^1(3a)^{k-1}(2) + \cdots + C_k^{k-1}(3a)2^{k-1} + 2^k$.

(1) If $k \geq 2$ is even, then by Lemma 2.6, $3 \mid (2^k-1)$, so that $3 \mid (p^k-1)$. Thus, $Z(3p^k) = p^k - 1$.

(2) If $k \geq 3$ is odd, then by Lemma 2.6, $3 \mid (2^k+1)$, and so $3 \mid (p^k+1)$. Thus, $Z(3p^k) = p^k$.

In Theorem 2.7 - Theorem 2.9, we give the expressions for $Z(4p)$, $Z(5p)$ and $Z(6p)$ respectively, where p is a prime. Note that, each case involves 4 possibilities.

Theorem 2.7. If $p \geq 5$ is a prime, then

$$Z(4p) = \begin{cases} p-1, & \text{if } 8 \mid (p-1); \\ p, & \text{if } 8 \mid (p+1); \\ 3p-1, & \text{if } 8 \mid (3p-1); \\ 3p, & \text{if } 8 \mid (3p+1). \end{cases}$$

Proof.

$$Z(4p) = \min\left\{m : 4p \mid \frac{m(m+1)}{2}\right\} = \min\left\{m : p \mid \frac{m(m+1)}{8}\right\}. \tag{7}$$

If $p|m(m+1)$, then p must divide either m or $m+1$, but not both (by Lemma 2.3), and then 8 must divide either $p-1$ or $p+1$, In the particular case when 8 divides $p-1$ or $p+1$, the minimum m in (7) may be taken as $p-1$ or $p+1$ respectively. We now consider the following four cases may arise:

Case 1 : p is of the form $p = 8a+1$ for some integer $a \geq 1$. In this case, $8 \mid (p-1)$, and hence $Z(4p) = p-1$.

Case 2 : p is of the form $p = 8a+7$ for some integer $a \geq 1$. Here, $8 \mid (p+1)$, and hence $Z(4p) = p$.

Case 3 : p is of the form $p = 8a+3$ for some integer $a \geq 1$. In this case, $8 \mid (3p-1)$, and hence $Z(4p) = 3p-1$.

Case 4 : p is of the form $p = 8a+5$ for some integer $a \geq 1$. Here, $8 \mid (3p+1)$, and hence $Z(4p) = 3p$.

Theorem 2.8. If $p \geq 7$ is a prime, then

$$Z(5p) = \begin{cases} p-1, & \text{if } 10 \mid (p-1); \\ p, & \text{if } 10 \mid (p+1); \\ 2p-1, & \text{if } 5 \mid (2p-1); \\ 2p, & \text{if } 5 \mid (2p+1). \end{cases}$$

Proof.

$$Z(5p) = \min\left\{m : 5p \mid \frac{m(m+1)}{2}\right\} = \min\left\{m : p \mid \frac{m(m+1)}{10}\right\}. \tag{8}$$

If $p|m(m+1)$, then p must divide either m or $m+1$, but not both (by Lemma 2.3), and then 5 must divide either $m-1$ or $m+1$, In the particular case when 5 divides $p-1$ or $p+1$, the minimum m in (8) may be taken as $p-1$ or $p+1$ respectively. We now consider the four below that may arise:

Case 1 : p is a prime whose last digit is 1. In this case, $10 \mid (p-1)$, and hence $Z(5p) = p-1$.

Case 2 : p is a prime whose last digit is 9. In such a case, $10 \mid (p+1)$, and so $Z(5p) = p$.

Case 3 : p is a prime whose last digit is 3. In this case, $5 \mid (2p-1)$. Thus, the minimum m in (9) may be taken as $2p-1$. Hence $Z(5p) = 2p-1$.

Case 4 : p is a prime whose last digit is 7. Here, $5 \mid (2p+1)$, and hence $Z(5p) = 2p$.

Theorem 2.9. If $p \geq 5$ is a prime, then

$$Z(6p) = \begin{cases} p-1, & \text{if } 12 \mid (p-1); \\ p, & \text{if } 12 \mid (p+1); \\ 2p-1, & \text{if } 4 \mid (3p+1); \\ 2p, & \text{if } 4 \mid (3p-1). \end{cases}$$

Proof.

$$Z(6p) = \min\left\{m : 6p \mid \frac{m(m+1)}{2}\right\} = \min\left\{m : p \mid \frac{m(m+1)}{12}\right\}. \tag{9}$$

If $p|m(m+1)$, then p must divide either m or $m+1$, but not both (by Lemma 2.3), and then 12 must divide either $m-1$ or $m+1$, In the particular case when 12 divides $p-1$ or $p+1$, the minimum m in (9) may be taken as $p-1$ or p respectively. We now consider the four cases that may arise:

Case 1 : p is of the form $p = 12a+1$ for some integer $a \geq 1$. In this case, $12 \mid (p-1)$, and hence $Z(6p) = p-1$.

Case 2 : p is of the form $p = 12a+11$ for some integer $a \geq 1$. Here, $12 \mid (p+1)$, and hence $Z(6p) = p$.

Case 3 : p is of the form $p = 12a+5$ for some integer $a \geq 1$. In this case, $4 \mid (3p+1)$. The minimum m in (10) may be taken as $3p$, and hence $Z(6p) = 3p$.

Case 4 : p is of the form $p = 12a+7$ for some integer $a \geq 1$. Here, $4 \mid (3p-1)$, and hence $Z(6p) = 3p-1$.

It is possible to find explicit expressions for $Z(7p)$ or $Z(11p)$, where p is a prime, as are given in Theorem 2.10 and Theorem 2.11 respectively, but it becomes more complicated. For example, in finding the expression for $Z(7p)$, we have to consider all the six possibilities, while the expression for $Z(11p)$ involves 10 alternatives.

Theorem 2.10. If $p \geq 11$ is a prime, then

$$Z(7p) = \begin{cases} p-1, & \text{if } 7 \mid (p-1); \\ p, & \text{if } 7 \mid (p+1); \\ 2p-1, & \text{if } 7 \mid (2p-1); \\ 2p, & \text{if } 7 \mid (2p+1); \\ 3p-1, & \text{if } 7 \mid (3p-1); \\ 3p, & \text{if } 7 \mid (3p+1). \end{cases}$$

Proof:

$$Z(7p) = \min\{m : 7p|\frac{m(m+1)}{2}\} = \min\{m : p|\frac{m(m+1)}{14}\}. \tag{10}$$

If $p|m(m+1)$, then p must divide either m or $m+1$, but not both (by Lemma 2.3), and then 7 must divide either $m+1$ or m respectively. In the particular case when 12 divides $p-1$ or $p+1$, the minimum m in (10) may be taken as $p-1$ or p respectively. We now consider the following six cases that may arise:

Case 1 : p is of the form $p = 7a+1$ for some integer $a \geq 1$. In this case, $7|(p-1)$. Therefore, $Z(7p) = p-1$.

Case 2 : p is of the form $p = 7a+6$ for some integer $a \geq 1$. Here, $7|(p+1)$, and so, $Z(7p) = p$.

Case 3 : p is of the form $p = 7a+2$ for some integer $a \geq 1$, so that $7|(3p+1)$. In this case, the minimum m in (11) may be taken as $3p$. That is, $Z(7p) = 3p$.

Case 4 : p is of the form $p = 7a+5$ for some integer $a \geq 1$. Here, $7|(3p-1)$, and hence, $Z(7p) = 3p-1$.

Case 5 : p is of the form $p = 7a+3$ for some integer $a \geq 1$. In this case, $7|(2p+1)$, and hence, $Z(7p) = 2p$.

Case 6 : p is of the form $p = 7a+4$ for some integer $a \geq 1$. Here, $7|(2p-1)$, and hence, $Z(7p) = 2p-1$.

Theorem 2.11. For any prime $p \geq 13$,

$$Z(7p) = \begin{cases} p-1, & \text{if } 11 \mid (p-1); \\ p, & \text{if } 11 \mid (p+1); \\ 2p-1, & \text{if } 11 \mid (2p-1); \\ 2p, & \text{if } 11 \mid (2p+1); \\ 3p-1, & \text{if } 11 \mid (3p-1); \\ 3p, & \text{if } 11 \mid (3p+1); \\ 4p-1, & \text{if } 11 \mid (4p-1); \\ 4p, & \text{if } 11 \mid (4p+1); \\ 5p-1, & \text{if } 11 \mid (5p-1); \\ 5p, & \text{if } 11 \mid (5p+1). \end{cases}$$

,

Proof:

$$Z(11p) = \min\{m : 11p|\frac{m(m+1)}{2}\} = \min\{m : p|\frac{m(m+1)}{22}\}. \tag{11}$$

If $p|m(m+1)$, then p must divide either m or $m+1$, but not both (by Lemma 2.3), and then 11 must divide either $m+1$ or m respectively. In the particular case when 11 divides $p-1$ or $p+1$, the minimum m in (11) may be taken as $p-1$ or p respectively. We have to consider the ten possible cases that may arise :

Case 1 : p is of the form $p = 11a + 1$ for some integer $a \geq 1$. In this case, $11|(p-1)$, and so, $Z(11p) = p - 1$.

Case 2 : p is of the form $p = 11a + 10$ for some integer $a \geq 1$. Here, $11|(p+1)$, and hence, $Z(11p) = p$.

Case 3 : p is of the form $p = 11a + 2$ for some integer $a \geq 1$. In this case, $11|(5p+1)$, and hence, $Z(11p) = 5p$.

Case 4 : p is of the form $p = 11a + 9$ for some integer $a \geq 1$. Here, $11|(5p-1)$, and hence, $Z(11p) = 5p - 1$.

Case 5 : p is of the form $p = 11a + 3$ for some integer $a \geq 1$. In this case, $11|(4p-1)$, and hence, $Z(11p) = 4p - 1$.

Case 6 : p is of the form $p = 11a + 8$ for some integer $a \geq 1$. Here, $11|(4p+1)$, and hence, $Z(11p) = 4p$.

Case 7 : p is of the form $p = 11a + 4$ for some integer $a \geq 1$. In this case, $11|(3p-1)$, and hence, $Z(11p) = 3p - 1$.

Case 8 : p is of the form $p = 11a + 7$ for some integer $a \geq 1$. Here, $11|(3p+1)$, and hence, $Z(11p) = 3p$.

Case 9 : p is of the form $p = 11a + 5$ for some integer $a \geq 1$. In this case, $11|(2p+1)$, and hence, $Z(11p) = 2p$.

Case 10 : p is of the form $p = 11a + 6$ for some integer $a \geq 1$. Here, $11|(2p-1)$, and hence, $Z(11p) = 2p - 1$.

In Theorem 2.12, we give an expression for $Z(pq)$, where p and q are two distinct primes. In this connection, we state the following lemma. The proof of the lemma is similar to, for example, Theorem 12.2 of Gioia [3], and is omitted here.

Lemma 2.7. Let p and q be two distinct primes. Then, the Diophantine equation

$$qy - px = 1$$

has an infinite number of solutions. Moreover, if (x_0, y_0) is a solution of the Diophantine equation, then any solution is of the form

$$x = x_0 + qt, y = y_0 + pt,$$

where $t \geq 0$ is an integer.

Theorem 2.12. Let p and q be two primes with $q > p \geq 5$. Then,

$$Z(pq) = \min\{qy_0 - 1, px_0 - 1\},$$

where

$$y_0 = \min\{y : x, y \in N, qy - px = 1\},$$

$$x_0 = \min\{x : x, y \in N, px - qy = 1\}.$$

Proof: Since

$$Z(pq) = \min\{m : pq|\frac{m(m+1)}{2}\}, \quad (12)$$

it follows that we have to consider the three cases below that may arise :

Case 1 : When $p|m$ and $q|(m+1)$. In this case, $m = px$ for some integer $x \geq 1$, $m+1 = qy$ for some integer $y \geq 1$. From these two equations, we get the Diophantine equation

$$qy - px = 1.$$

By Lemma 2.7, the above Diophantine equation has infinite number of solutions. Let

$$y_0 = \min\{y : x, y \in N, qy - px = 1\}.$$

For this y_0, the corresponding x_0 is given by the equation $q_0y - p_0x = 1$. Note that y_0 and x_0 cannot be both odd or both even. Then, the minimum m in (12) is given by

$$m + 1 = qy_0 \Rightarrow m = qy_0 - 1.$$

Case 2 : When $p|(m + 1)$ and $q|m$. Here, $m + 1 = px$ for some integer $x \geq 1$, $m = qy$ for some integer $y \geq 1$. These two equations lead to the Diophantine equation. $px - qy = 1$. Let

$$x_0 = \min\{x : x, y \in N, px - qy = 1\}.$$

For this x_0, the corresponding y_0 is given by $y_0 = (px_0 - 1)/q$. Here also, x_0 and y_0 both cannot be odd or even simultaneously. The minimum m in (12) is given by

$$m + 1 = px_0 \Rightarrow m = px_0 - 1.$$

Case 3 : When $pq|(m+1)$. In this case, $m = pq-1$. But then, by Case 1 and Case 2 above, this does not give the minimum m. Thus, this case cannot occur. The proof of the theorem now follows by virtue of Case 1 and Case 2.

Remark 2.2. Let p and q be two primes with $q \geq p \geq 5$. Let $q = kp + \ell$ for some integers k and ℓ with $k \geq 1$ and $1 \leq \ell \leq p - 1$. We now consider the two cases given in Theorem 2.12 :

Case 1 : When $p|m$ and $q|(m + 1)$. In this case, $m = px$ for some integer $x \geq 1$, $m + 1 = qy = (kp + \ell)y$ for some integer $y \geq 1$. From these two equations, we get

$$\ell y - (x - ky)p = 1 \quad (2.1).$$

Case 2 : When $p|(m+1)$ and $q|m$. Here, $m+1 = px$ for some integer $x \geq 1$, $m = (kp+\ell)y$ for some integer $y \geq 1$. These two equations lead to

$$(x - ky)p - \ell y = 1 \quad (2.2).$$

In some particular cases, explicit expressions of $Z(pq)$ may be found. These are given in the following corollaries.

Corollary 2.1. Let p and q be two primes with $q > p \geq 5$. Let $q = kp + 1$ for some integer $k \geq 2$. Then, $Z(pq) = q - 1$.

Proof. From (2.1) with $\ell = 1$, we get $y - (x - ky)p = 1$, the minimum solution of which is $y = 1$, $x = ky = k$. Then, the minimum m in (12) is given by

$$m + 1 = qy = q \Rightarrow m = q - 1.$$

Note that, from (2.2) with $\ell = 1$, we have $(x - ky)p - y = 1$, with the least possible solution $y = p - 1$ (and $x - ky = 1$).

Corollary 2.2. Let p and q be two primes with $q > p \geq 5$. Let $q = (k+1)p - 1$ for some integer $k \geq 1$.

Then, $Z(pq) = q$.

Proof. From (2.2) with $\ell = p - 1$, we have, $y - [(k+1)y - x]p = 1$, the minimum solution of which is $y = 1$, $x = (k+1)y = k+1$. Then, the minimum m in (12) is given by $m = qy = q$. Note that, from (2.1) with $\ell = p - 1$, we have $[(k+1)y - x]p - x = 1$ with the least possible solution $y = p - 1$ (and $(k+1)y - x = 1$).

Corollary 2.3. Let p and q be two primes with $q > p \geq 5$. Let $q = kp + 2$ for some integer $k \geq 1$. Then,

$$Z(pq) = \frac{q(p-1)}{2}.$$

Proof. From (2.2) with $\ell = 2$, we have $(x - ky)p - 2y = 1$, with the minimum solution $y = \frac{p-1}{2}$ (and $x - ky = 1$). This gives $m = qy = \frac{q(p-1)}{2}$ as one possible solution of (12). Now, (2.1) with $\ell = 2$ gives $2y - (x - ky)p = 1$, with the minimum solution $y = \frac{p+1}{2}$ (and $x = ky + 1$). This gives $m = qy - 1 = \frac{q(p+1)}{2} - 1$ as another possible solution of (12). Now, since $\frac{q(p+1)}{2} - 1 > \frac{q(p-1)}{2}$, it follows that

$$Z(pq) = \frac{q(p-1)}{2},$$

which we intended to prove.

Corollary 2.4. Let p and q be two primes with $q > p \geq 5$. Let $q = (k+1)p - 2$ for some integer $k \geq 1$. Then,

$$Z(pq) = \frac{q(p-1)}{2} - 1.$$

Proof. By (2.1) with $\ell = p - 2$, we get $[(k+1)y - x]p - 2y = 1$, whose minimum solution is $y = \frac{p-1}{2}$(and $x = (k+1)y - 1$). This gives $m = qy - 1 = \frac{q(p-1)}{2} - 1$ as one possible solution of (12). Note that, (2.2) with $\ell = p - 2$ gives $2y - [(k+1)y - x]p = 1$, with the minimum solution $y = \frac{p+1}{2}$ (and $x = (k+1)y - 1$). Corresponding to this case, we get $m = qy = \frac{q(p+1)}{2}$ as another possible solution of (12). But since $\frac{q(p+1)}{2} > \frac{q(p-1)}{2} - 1$, it follows that $Z(pq) = \frac{q(p-1)}{2} - 1$, establishing the theorem.

Corollary 2.5. Let p and q be two primes with $q > p \geq 7$. Let $q = kp + 3$ for some integer $k \geq 1$. Then,

$$Z(pq) = \begin{cases} \frac{q(p-1)}{3}, & \text{if } 3|(p-1); \\ \frac{q(p+1)}{3} - 1, & \text{if } 3|(p+1). \end{cases}$$

Proof. From (2.1) and (2.2) with $\ell = 3$, we have respectively

$$3y - (x - ky)p = 1, \tag{13}$$

$$(x - ky)p - 3y = 1. \tag{14}$$

We now consider the following two possible cases :

Case 1 : When 3 divides $p - 1$.

In this case, the minimum solution is obtained from (14), which is $y = \frac{p-1}{3}$(and $x - ky = 1$). Also, $p - 1$ is divisible by 2 as well. Therefore, the minimum m in (12) is $m = qy = \frac{q(p-1)}{3}$.

Case 2 : When 3 divides $p + 1$.

In this case, (13) gives the minimum solution, which is $y = \frac{p+1}{3}$(and $x - ky = 1$). Note that, 2 divides $p + 1$. Therefore, the minimum m in (12) $m = qy - 1 = \frac{q(p+1)}{3} - 1$.

Thus, the theorem is established.

Corollary 2.6. Let p and q be two primes with $q > p \geq 7$. Let $q = (k + 1)p - 3$ for some integer $k \geq 1$. Then,

$$Z(pq) = \begin{cases} \frac{q(p+1)}{3}, & \text{if } 3|(p+1); \\ \frac{q(p-1)}{3} - 1, & \text{if } 3|(p-1). \end{cases}$$

Proof. From (2.1) and (2.2) with $\ell = p - 3$, we have respectively

$$[(k + 1)y - x]p - 3y = 1, \tag{15}$$

$$3y - [(k + 1)y - x]p = 1. \tag{16}$$

We now consider the following two cases :

Case 1 : When 3 divides $p + 1$.

In this case, the minimum solution, obtained from(14), is $y = \frac{p+1}{3}$(and $x = (k + 1)y - 1$).Moreover, 2 divides $p + 1$. Therefore, the minimum m in (12) is $m = qy = \frac{q(p+1)}{3}$.

Case 2 : When 3 divides $p - 1$.

In this case, the minimum solution, obtained from (13), is $y = \frac{p-1}{3}$(and $x = (k+1)y - 1$). Moreover, 2 divides $p - 1$. Therefore, the minimum m in (12) is $m = qy = \frac{q(p-1)}{3} - 1$.

Corollary 2.7. Let p and q be two primes with $q > p \geq 7$. Let $q = kp+4$ for some integer $k \geq 1$. Then,

$$Z(pq) = \begin{cases} \frac{q(p-1)}{4}, & \text{if } 4|(p-1); \\ \frac{q(p+1)}{4} - 1, & \text{if } 4|(p+1). \end{cases}$$

Proof. From (2.1) and (2.2) with $\ell = 4$, we have respectively

$$4y - (x - ky)p = 1, \tag{17}$$

$$(x - ky)p - 4y = 1. \tag{18}$$

Now, for any prime $p \geq 7$, exactly one of the following two cases can occur : Either $p - 1$ is divisible by 4, or $p+1$ is divisible by 4. We thus consider the two possibilities separately below:

Case 1 : When 4 divides $p - 1$.

In this case, the minimum solution is obtained from (18), is $y = \frac{p-1}{4}$(and $x = ky + 1$). Therefore, the minimum m in (12) is is $m = qy = \frac{q(p-1)}{4}$.

Case 2 : When 4 divides $p + 1$.

In this case, (17) gives the minimum solution, which is $y = \frac{p+1}{4}$(and $x = ky+1$). Therefore, the minimum m in (12) $m = qy - 1 = \frac{q(p+1)}{4} - 1$.

Corollary 2.8. Let p and q be two primes with $q > p \geq 7$. Let $q = (k + 1)p - 4$ for some integer $k \geq 1$. Then,

$$Z(pq) = \begin{cases} \frac{q(p+1)}{4}, & \text{if } 4|(p+1); \\ \frac{q(p-1)}{4} - 1, & \text{if } 4|(p-1). \end{cases}$$

Proof. From (2.1) and (2.2) with $\ell = p - 4$, we have respectively

$$[(k + 1)y - x]p - 4y = 1, \tag{19}$$

$$4y - [(k + 1)y - x]p = 1. \tag{20}$$

We now consider the following two cases which are the only possibilities (as noted in the proof of Corollary 2.7).

Case 1 : When 4 divides $p + 1$.

In this case, the minimum solution obtained from (20) is $y = \frac{p+1}{4}$ (and $x = (k + 1)y - 1$).Therefore, the minimum m in (12) is $m = qy = \frac{q(p+1)}{4}$.

Case 2 : When 4 divides $p - 1$.

In this case, the minimum solution, obtained from (19),is $y = \frac{p-1}{4}$ (and $x = (k + 1)y - 1$).Therefore, the minimum m in (12) is $m = qy = \frac{q(p-1)}{4} - 1$.

Corollary 2.9 . Let p and q be two primes with $q > p \geq 11$. Let $q = kp + 5$ for some integer $k \geq 1$. Then,

$$Z(pq) = \begin{cases} \frac{q(p-1)}{5}, & \text{if } 5|(p-1); \\ q(2a+1) - 1, & \text{if } p = 5a+2; \\ q(2a+1), & \text{if } p = 5a+3; \\ \frac{q(p+1)}{5} - 1, & \text{if } 5|(p+1). \end{cases}$$

Proof. From (2.1) and (2.2) with $\ell = 5$, we have respectively

$$5y - (x - ky)p = 1, \tag{21}$$

$$(x - ky)p - 5y = 1. \tag{22}$$

Now, for any prime $p \geq 7$, exactly one of the following four cases occur:

Case 1 : When p is of the form $p = 5a + 1$ for some integer $a \geq 2$.

In this case, 5 divides $p - 1$. Then, the minimum solution is obtained from (22) which is $y = \frac{p-1}{5}$ (and $x - ky = 1$). Therefore, the minimum m in (12) is $m = qy = \frac{q(p-1)}{5}$.

Case 2 : When p is of the form $p = 5a + 2$ for some integer $a \geq 2$.

In this case, from (21) and (22), we get respectively

$$1 = 5y - (x - ky)(5a + 2) = 5[y - (x - ky)a] - 2(x - ky), \tag{23}$$

$$1 = (x - ky)(5a + 2) - 5y = 2(x - ky) - 5[y - (x - ky)a] \quad (24)$$

Clearly, the minimum solution is obtained from (23), which is

$y - (x - ky)a = 1, \quad x - ky = 2 \Longrightarrow y = 2a + 1$ (and $x = k(2a + 1) + 2$).

Hence, in this case, the minimum m in (12) is $m = qy - 1 = q(2a + 1) - 1$.

Case 3 : When p is of the form $p = 5a + 3$ for some integer $a \geq 2$. From (21) and (22), we get

$$1 = 5y - (x - ky)(5a + 3) = 5[y - (x - ky)a] - 3(x - ky), \quad (25)$$

$$1 = (x - ky)(5a + 3) - 5y = 3(x - ky) - 5[y - (x - ky)a]. \quad (26)$$

The minimum solution is obtained from (27) as follows :

$y - (x - ky)a = 1, \quad x - ky = 2 \Longrightarrow y = 2a + 1$ (and $x = k(2a + 1) + 2$).

Hence, in this case, the minimum m in (12) is $m = qy = q(2a + 1)$.

Case 4 : When p is of the form $p = 5a + 4$ for some integer $a \geq 2$.

In this case, 5 divides $p + 1$. Then, the minimum solution is obtained from (21), which is $y = \frac{p+1}{5}$ (and $x - ky = 1$). Therefore, the minimum m in (12) is $m = qy - 1 = \frac{q(p+1)}{5} - 1$.

Corollary 2.10. Let p and q be two primes with $q > p \geq 11$. Let $q = (k + 1)p - 5$ for some integer $k \geq 1$. Then,

$$Z(pq) = \begin{cases} \frac{q(p-1)}{5} - 1, & \text{if } 5|(p - 1); \\ q(2a + 1), & \text{if } p = 5a + 2; \\ q(2a + 1) - 1, & \text{if } p = 5a + 3; \\ \frac{q(p+1)}{5}, & \text{if } 5|(p + 1). \end{cases}$$

Proof. From (2.1) and (2.2) with $\ell = p - 5$, we have respectively

$$[(k + 1)y - x]p - 5y = 1, \quad (27)$$

$$5y - [(k + 1)y - x]p = 1. \quad (28)$$

As in the proof of Corollary 2.9, we consider the following four possibilities :

Case 1 : When p is of the form $p = 5a + 1$ for some integer $a \geq 2$.

In this case, 5 divides $p - 1$. Then, the minimum solution is obtained from (27), which is $y = \frac{p-1}{5}$ (and $x = (k+1)y-1$). Therefore, the minimum m in (12) is $m = qy-1 = \frac{q(p-1)}{5}-1$.

Case 2 : When p is of the form $p = 5a + 2$ for some integer $a \geq 2$.

In this case, from (27) and (28), we get respectively

$$1 = [(k + 1)y - x](5a + 2) - 5y = 2[(k + 1)y - x] - 5[y - a(k + 1)y - x], \quad (29)$$

$$1 = 5y - [(k + 1)y - x](5a + 2) = 5[y - a(k + 1)y - x] - 2[(k + 1)y - x]. \quad (30)$$

Clearly, the minimum solution is obtained from (30), which is

$y - a(k + 1)y - x = 1, (k + 1)y - x = 2 \Longrightarrow y = 2a + 1$ (and $x = (k + 1)(2a + 1) - 2$).

Hence, in this case, the minimum m in (12) is $m = qy = q(2a + 1)$.

Case 3 : When p is of the form $p = 5a + 3$ for some integer $a \geq 2$.

In this case, from (27) and (28), we get respectively

$$1 = [(k+1)y - x](5a+3) - 5y = 3[(k+1)y - x] - 5[y - a(k+1)y - x], \tag{31}$$

$$1 = 5y - [(k+1)y - x](5a+3) = 5[y - a(k+1)y - x] - 3[(k+1)y - x]. \tag{32}$$

The minimum solution is obtained from (31) as follows :

$y - a(k+1)y - x = 1, (k+1)y - x = 2 \Longrightarrow y = 2a+1$ (and $x = (k+1)(2a+1) - 2$).

Hence, in this case, the minimum m in (12) is $m = qy - 1 = q(2a+1) - 1$.

Case 4 : When p is of the form $p = 5a + 4$ for some integer $a \geq 2$.

In this case, 5 divides $p + 1$. Then, the minimum solution is obtained from (28), which is $y = \frac{p+1}{5}$ (and $x = (k+1)y - 1$). Therefore, the minimum m in (12) is $m = qy = \frac{q(p+1)}{5}$.

Corollary 2.11. Let p and q be two primes with $q > p \geq 13$. Let $q = kp + 6$ for some integer $k \geq 1$. Then,

$$Z(pq) = \begin{cases} \frac{q(p-1)}{6}, & \text{if } 6|(p-1); \\ \frac{q(p+1)}{6} - 1, & \text{if } 6|(p+1). \end{cases}$$

Proof. From (2.1) and (2.2) with $\ell = 6$, we have respectively

$$6y - (x - ky)p = 1, \tag{33}$$

$$(x - ky)p - 6y = 1. \tag{34}$$

Now, for any prime $p \geq 13$, exactly one of the following two cases can occur : Either $p - 1$ is divisible by 6, or $p + 1$ is divisible by 6. We thus consider the two possibilities separately below :

Case 1 : When 6 divides $p - 1$.

In this case, the minimum solution, obtained from (34), is $y = \frac{p-1}{6}$ (and $x = ky + 1$). Therefore, the minimum m in (12) is $m = qy = \frac{q(p-1)}{6}$.

Case 2 : When 6 divides $p + 1$.

In this case, (33) gives the minimum solution, which is $y = \frac{p+1}{6}$ (and $x = ky+1$). Therefore, the minimum m in (12) is $m = qy - 1 = \frac{q(p+1)}{6} - 1$.

Corollary 2.12. Let p and q be two primes with $q > p \geq 13$. Let $q = (k+1)p - 6$ for some integer $k \geq 1$. Then,

$$Z(pq) = \begin{cases} \frac{q(p+1)}{6}, & \text{if } 6|(p+1); \\ \frac{q(p-1)}{6} - 1, & \text{if } 6|(p-1). \end{cases}$$

Proof. From (2.1) and (2.2) with $\ell = p - 6$, we have respectively

$$[(k+1)y - x]p - 6y = 1, \tag{35}$$

$$6y - [(k+1)y - x]p = 1. \tag{36}$$

We now consider the following two cases which are the only possibilities (as noted in the proof of Corollary 2.11) :

Case 1 : When 6 divides $p + 1$.

In this case, the minimum solution, obtained from (36), is $y = \frac{p+1}{6}$ (and $x = (k+1)y - 1$). Therefore, the minimum m in (12) is $m = qy = \frac{q(p+1)}{6}$.

Case 2 : When 6 divides $p - 1$.

Here, the minimum solution is obtained from (35), which is $y = \frac{p-1}{6}$ (and $x = (k+1)y-1$). Therefore, the minimum m in (12) is $m = qy = \frac{q(p-1)}{6} - 1$.

Corollary 2.13. Let p and q be two primes with $q > p \geq 13$. Let $q = kp + 7$ for some integer $k \geq 1$. Then,

$$Z(pq) = \begin{cases} \frac{q(p-1)}{7}, & \text{if } 7|(p-1); \\ q(3a+1) - 1, & \text{if } p = 7a+2; \\ q(2a+1) - 1, & \text{if } p = 7a+3; \\ q(2a+1), & \text{if } p = 7a+4; \\ q(3a+2), & \text{if } p = 7a+5; \\ \frac{q(p+1)}{7} - 1, & \text{if } 7|(p+1). \end{cases}$$

Proof. From (2.1) and (2.2) with $\ell = 7$, we have respectively

$$7y - (x - ky)p = 1, \tag{37}$$

$$(x - ky)p - 7y = 1. \tag{38}$$

Now, for any prime $p \geq 11$, exactly one of the following six cases occur :

Case 1 : When p is of the form $p = 7a + 1$ for some integer $a \geq 2$.
In this case, 7 divides $p - 1$. Then, the minimum solution is obtained from (38), which is $y = \frac{p-1}{7}$ (and $x - ky = 1$).
Therefore, the minimum m in (12) is $m = qy = \frac{q(p-1)}{7}$.

Case 2 : When p is of the form $p = 7a + 2$ for some integer $a \geq 2$.
In this case, from (37) and (38), we get respectively

$$1 = 7y - (x - ky)(7a + 2) = 7[y - (x - ky)a] - 2(x - ky), \tag{39}$$

$$1 = (x - ky)(7a + 2) - 7y = 2(x - ky) - 7[y - (x - ky)a]. \tag{40}$$

Clearly, the minimum solution is obtained from (39), which is

$y - (x - ky)a = 1, x - ky = 3 \Longrightarrow y = 3a + 1$ (and $x = k(3a + 1) + 3$).
Hence, in this case, the minimum m in (12) is $m = qy - 1 = q(3a + 1) - 1$.

Case 3 : When p is of the form $p = 7a + 3$ for some integer $a \geq 2$. Here, from (37) and (38),

$$1 = 7y - (x - ky)(7a + 3) = 7[y - (x - ky)a] - 3(x - ky), \tag{41}$$

$$1 = (x - ky)(7a + 3) - 7y = 3(x - ky) - 7[y - (x - ky)a]. \tag{42}$$

The minimum solution is obtained from (41) as follows:

$y - (x - ky)a = 1, x - ky = 2 \Longrightarrow y = 2a + 1$(and $x = k(2a + 1) + 2$).
Hence, in this case, the minimum m in (12) is $m = qy - 1 = q(2a + 1) - 1$.

Case 4 : When p is of the form $p = 7a + 4$ for some integer $a \geq 2$. In this case, from (37) and (38), we get respectively

$$1 = 7y - (x - ky)(7a + 4) = 7[y - (x - ky)a] - 4(x - ky), \tag{43}$$

$$1 = (x - ky)(7a + 4) - 7y = 4(x - ky) - 7[y - (x - ky)a]. \tag{44}$$

Clearly, the minimum solution is obtained from (44), which is

$y - (x - ky)a = 1, x - ky = 2 \Longrightarrow y = 2a + 1$(and $x = k(2a + 1) + 2$).

Hence, in this case, the minimum m in (12) is $m = qy - 1 = q(2a + 1) + 1$.

Case 5 : When p is of the form $p = 7a + 5$ for some integer $a \geq 2$. From (37) and (38), we have

$$1 = 7y - (x - ky)(7a + 5) = 7[y - (x - ky)a] - 5(x - ky), \tag{45}$$

$$1 = (x - ky)(7a + 5) - 7y = 5(x - ky) - 7[y - (x - ky)a]. \tag{46}$$

The minimum solution is obtained from (46), which is

$y - (x - ky)a = 2, x - ky = 3 \Longrightarrow y = 3a + 2$(and $x = k(3a + 2) + 3$).

Hence, in this case, the minimum m in (12) is $m = qy - 1 = q(3a + 2)$.

Case 6 : When p is of the form $p = 7a + 6$ for some integer $a \geq 2$. In this case, 7 divides $p + 1$. Then, the minimum solution is obtained from (37), which is $y = \frac{p+1}{7}$ (and $x - ky = 1$). Therefore, the minimum m in (12) is $m = qy - 1 = \frac{q(p+1)}{7} - 1$.

Corollary 2.14. Let p and q be two primes with $q > p \geq 13$. Let $q = (k + 1)p - 7$ for some integer $k \geq 1$.

Then,

$$Z(pq) = \begin{cases} \frac{q(p-1)}{7}, & \text{if } 7|(p-1); \\ q(3a+1), & \text{if } p = 7a+2; \\ q(2a+1), & \text{if } p = 7a+3; \\ q(2a+1)-1, & \text{if } p = 7a+4; \\ q(3a+2)-1, & \text{if } p = 7a+5; \\ \frac{q(p+1)}{7}, & \text{if } 7|(p+1). \end{cases}$$

Proof. From (2.1) and (2.2) with $\ell = 7$, we have respectively

$$[(k + 1)y - x]p - 7y = 1, \tag{47}$$

$$7y - [(k + 1)y - x]p = 1. \tag{48}$$

We now consider the following six possibilities:

Case 1 : When p is of the form $p = 7a + 1$ for some integer $a \geq 2$. In this case, 7 divides $p-1$. Then, the minimum solution is obtained from (47), which is $y = \frac{p-1}{7}$ (and$x = (k+1)y-1$). Therefore, the minimum m in (12) is $m = qy - 1 = \frac{q(p-1)}{7} - 1$.

Case 2 : When p is of the form $p = 7a + 2$ for some integer $a \geq 2$.

In this case, from (47) and (48), we get respectively

$$1 = [(k + 1)y - x](7a + 2) - 7y = 2[(k + 1)y - x] - 7[y - a\{(k + 1)y - x\}], \tag{49}$$

$$1 = 7y - [(k+1)y - x](7a+2) = 7[y - a\{(k+1)y - x\}] - 2[(k+1)y - x]. \quad (50)$$

Clearly, the minimum solution is obtained from (50), which is

$y - a\{(k+1)y - x\} = 1, (k+1)y - x = 3 \Longrightarrow y = 3a+1$(and $x = (k+1)(3a+1) - 3$).

Hence, in this case, the minimum m in (12) is $m = qy = q(3a+1)$.

Case 3 : When p is of the form $p = 7a+3$ for some integer $a \geq 2$.

Here, from (47) and (48),

$$1 = [(k+1)y - x](7a+3) - 7y = 3[(k+1)y - x] - 7[y - a\{(k+1)y - x\}], \quad (51)$$

$$1 = 7y - [(k+1)y - x](7a+3) = 7[y - a\{(k+1)y - x\}] - 3[(k+1)y - x]. \quad (52)$$

Then, (52) gives the minimum solution, which is:

$y - a\{(k+1)y - x\} = 1, (k+1)y - x = 2 \Longrightarrow y = 2a+1$(and $x = (k+1)(2a+1) - 2$).

Hence, in this case, the minimum m in (12) is $m = qy = q(2a+1)$.

Case 4 : When p is of the form $p = 7a+4$ for some integer $a \geq 2$.

Here, from (47) and (48),

$$1 = [(k+1)y - x](7a+4) - 7y = 4[(k+1)y - x] - 7[y - a\{(k+1)y - x\}], \quad (53)$$

$$1 = 7y - [(k+1)y - x](7a+4) = 7[y - a\{(k+1)y - x\}] - 4[(k+1)y - x]. \quad (54)$$

Clearly, the minimum solution is obtained from (53) as follows:

$y - a\{(k+1)y - x\} = 1, (k+1)y - x = 2 \Longrightarrow y = 2a+1$(and $x = (k+1)(2a+1) - 2$).

Hence, in this case, the minimum m in (12) is $m = qy - 1 = q(2a+1) - 1$.

Case 5 : When p is of the form $p = 7a+5$ for some integer $a \geq 2$.

In this case, from (47) and (48), we get respectively

$$1 = [(k+1)y - x](7a+5) - 7y = 5[(k+1)y - x] - 7[y - a\{(k+1)y - x\}], \quad (55)$$

$$1 = 7y - [(k+1)y - x](7a+5) = 7[y - a\{(k+1)y - x\}] - 5[(k+1)y - x]. \quad (56)$$

Then, (55) gives the following minimum solution:

$y - a\{(k+1)y - x\} = 2, (k+1)y - x = 3 \Longrightarrow y = 3a+2$ (and $x = (k+1)(3a+2) - 3$).

Hence, in this case, the minimum m in (12) is $m = qy - 1 = q(3a+2) - 1$.

Case 6 : When p is of the form $p = 7a+6$ for some integer $a \geq 2$. In this case, 7 divides $p+1$. Then, the minimum solution is obtained from (48), which is $y = \frac{p+1}{7}$ (and $x = (k+1)y - 1$). Therefore, the minimum m in (12) is $m = qy = \frac{q(p+1)}{7}$.

Corollary 2.15. Let p and q be two primes with $q > p \geq 13$. Let $q = kp + 8$ for some integer $k \geq 1$.

Then,

$$Z(pq) = \begin{cases} \frac{q(p-1)}{8}, & \text{if } 8|(p-1); \\ q(3a+1), & \text{if } p = 8a+3; \\ q(3a+2) - 1, & \text{if } p = 8a+5; \\ \frac{q(p+1)}{8} - 1, & \text{if } 8|(p+1). \end{cases}$$

Proof. From (2.1) and (2.2) with $\ell = 8$, we have respectively

$$8y - (x - ky)p = 1, \tag{57}$$

$$(x - ky)p - 8y = 1. \tag{58}$$

Now, for any prim $p \geq 13$, exactly one of the following four cases occur:

Case 1 : When p is of the form $p = 8a + 1$ for some integer $a \geq 2$.

In this case, 8 divides $p - 1$. Then, the minimum solution is obtained from (58), which is $y = \frac{p-1}{8}$ (and$x - ky = 1$).

Therefore, the minimum m in (12) is $m = qy = \frac{q(p-1)}{8}$.

Case 2 : When p is of the form $p = 8a + 3$ for some integer $a \geq 2$.

In this case, from (57) and (58), we get respectively

$$1 = 8y - (x - ky)(8a + 3) = 8[y - (x - ky)a] - 3(x - ky), \tag{59}$$

$$1 = (x - ky)(8a + 3) - 8y = 3(x - ky) - 8[y - (x - ky)a]. \tag{60}$$

Clearly, the minimum solution is obtained from (60), which is

$y - (x - ky)a = 1, x - ky = 3 \Longrightarrow y = 3a + 1$ (and $x = k(3a + 1) + 3$).

Hence, in this case, the minimum m in (12) is $m = qy = q(3a + 1)$.

Case 3 : When p is of the form $p = 8a + 5$ for some integer $a \geq 2$.

From (57) and (58), We get

$$1 = 8y - (x - ky)(8a + 5) = 8[y - (x - ky)a] - 5(x - ky), \tag{61}$$

$$1 = (x - ky)(8a + 5) - 8y = 5(x - ky) - 8[y - (x - ky)a]. \tag{62}$$

The minimum solution is obtained from (61) as follows:

$y - (x - ky)a = 2, x - ky = 3 \Longrightarrow y = 3a + 2$ (and $x = k(3a + 2) + 3$).

Hence, in this case, the minimum m in (12) is $m = qy - 1 = q(3a + 2) - 1$.

Case 4 : When p is of the form $p = 8a + 7$ for some integer $a \geq 2$.

In this case, 8 divides $p - 1$. Then, the minimum solution is obtained from (57), which is $y = \frac{p+1}{8}$ (and$x - ky = 1$). Therefore, the minimum m in (12) is $m = qy - 1 = \frac{q(p+1)}{8} - 1$.

Corollary 2.16. Let p and q be two primes with $q > p \geq 13$. Let $q = (k + 1)p - 8$ for some integer $k \geq 1$.

Then,

$$Z(pq) = \begin{cases} \frac{q(p-1)}{8}, & \text{if } 8|(p-1); \\ q(3a+1) - 1, & \text{if } p = 8a + 3; \\ q(3a+2), & \text{if } p = 8a + 5; \\ \frac{q(p+1)}{8}, & \text{if } 8|(p+1). \end{cases}$$

Proof. From (2.1) and (2.2) with $\ell = p - 8$, we have respectively

$$[(k + 1)y - x]p - 8y = 1, \tag{63}$$

$$8y - [(k + 1)y - x]p = 1. \tag{64}$$

We now consider the four possibilities that may arise:

Case 1 : When p is of the form $p = 8a + 1$ for some integer $a \geq 2$.

In this case, 8 divides $p - 1$. Then, the minimum solution is obtained from (63), which is $y = \frac{p-1}{8}$ (and $x = (k+1)y - 1$). Therefore, the minimum m in (12) is $m = qy - 1 = \frac{q(p-1)}{8} - 1$.

Case 2 : When p is of the form $p = 8a + 3$ for some integer $a \geq 2$.

In this case, from (63) and (64), we get respectively

$$1 = [(k+1)y - x](8a+3) - 8y = 2[(k+1)y - x] - 8[y - a\{(k+1)y - x\}], \tag{65}$$

$$1 = 8y - [(k+1)y - x](8a+3) = 8[y - a\{(k+1)y - x\}] - 3[(k+1)y - x]. \tag{66}$$

Clearly, the minimum solution is obtained from (65), which is

$$y - a\{(k+1)y - x\} = 1, (k+1)y - x = 3 \Longrightarrow y = 3a + 1 (\text{and} x = (k+1)(3a+1) - 3).$$

Hence, in this case, the minimum m in (12) is $m = qy = q(3a+1) - 1$.

Case 3 : When p is of the form $p = 8a + 5$ for some integer $a \geq 1$.

In this case, from (63) and (64), we get respectively

$$1 = [(k+1)y - x](8a+5) - 8y = 5[(k+1)y - x] - 8[y - a\{(k+1)y - x\}], \tag{67}$$

$$1 = 8y - [(k+1)y - x](8a+5) = 8[y - a\{(k+1)y - x\}] - 5[(k+1)y - x]. \tag{68}$$

The minimum solution is obtained from (68) as follows:

$$y - a\{(k+1)y - x\} = 2, (k+1)y - x = 3 \Longrightarrow y = 3a + 2 (\text{and} x = (k+1)(3a+2) - 3).$$

Hence, in this case, the minimum m in (12) is $m = qy = q(3a+2)$.

Case 4 : When p is of the form $p = 8a + 7$ for some integer $a \geq 2$.

In this case, 8 divides $p + 1$. Then, the minimum solution is obtained from (64), which is $y = \frac{p+1}{8}$ (and $x = (k+1)y - 1$). Therefore, the minimum m in (12) is $m = qy = \frac{q(p+1)}{8}$.

We now consider the case when n is a composite number. Let

$Z(n) = m_0$ for some integer $m_0 \geq 1$. Then, n divides $\frac{m_0(m_0+1)}{2}$.

We now consider the following two cases that may arise :

Case 1 : m_0 is even (so that $m_0 + 1$ is odd).

(1) Let n be even. In this case, n does not divide $\frac{m_0}{2}$, for otherwise,

$$\frac{n|m_0}{2} \Longrightarrow \frac{n|m_0(m_0+1)}{2} \Longrightarrow Z(n) \leq (m_0 - 1).$$

(2) Let n be odd. In such a case, n does not divide m_0.

Case 2 : m_0 is odd (so that $m_0 + 1$ is even).

(1) Let n be even. Then, n does not divide m_0.

(2) Let n be odd. Here, n does not divide m_0, for

$$n|m_0 \Longrightarrow \frac{n|m_0(m_0-1)}{2} \Longrightarrow Z(n) \leq (m_0 - 1).$$

Thus, if n is a composite number, n does not divide m_0.

Now let

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i} p_{i+1}^{\alpha_{i+1}} \cdots p_s^{\alpha_s}$$

be the representation of n in terms of its distinct prime factors $p_1, p_2, \cdots p_i, p_{i+1}, \cdots p_s$, not necessarily ordered. Then, one of m_0 and $m_0 + 1$ is of the form

$$2^{\beta} p_1^{\beta_1} p_2^{\beta_2} \cdots p_i^{\beta_i} q_{i+1}^{\beta_{i+1}} \cdots q_s^{\beta_s}$$

for some $1 \leq i < s$; $\beta_j \geq \alpha_j$ for $1 \leq j < i$, and the other one is of the form

$$p_{i+1}^{\gamma_{i+1}} \cdots p_s^{\gamma_s}, r_{s+1}^{\gamma_{s+1}} \cdots r_u^{\gamma_u} \gamma_j \geq \alpha_j$$

for $i + 1 \leq j < s$; where $q_{i+1}, \cdots q_s$ and $r_{s+1}, \cdots r_u$ are all distinct primes, not necessarily ordered.

§3. Some Observations

Some observations about the Pseudo-Smarandache Function are given below :

Remark 3.1. Kashihara raised the following questions (see Problem 7 in [1]) :
(1) Is there any integer n such that $Z(n) > Z(n+1) > Z(n+2) > Z(n+3)$?
(2) Is there any integer n such that $Z(n) < Z(n+1) < Z(n+2) < Z(n+3)$?
The following examples answer the questions in the affirmative:

$$(1) \quad Z(256) = 511 > 256 = Z(257) > Z(258) = 128 > 111 = Z(259) > Z(260) = 39,$$

$$(2) \quad Z(159) = 53 < 64 = Z(160) < Z(161) = 69 < 80 = Z(162) < Z(163) = 162.$$

These examples show that even five consecutive increasing or decreasing terms are available in the sequence $\{Z(n)\}$.

Remark 3.2 Kashihara raises the following question (see Problem 5 in [1]) : Given any integer $m_0 \geq 1$, how many n are there such that $Z(n) = m_0$?
Given any integer $m_0 \backslash 3$, let

$$Z^{-1}(m_0) = \{n : n \in N, Z(n) = m_0\}, \tag{2.3}$$

with

$$Z^{-1}(1) = \{1\}, Z^{-1}(2) = \{3\}. \tag{2.4}$$

Thus, for example, $Z^{-1}(8) = \{8, 12, 18, 36\}$.
By Lemma 2.1,

$$n_{\max} \equiv \frac{m_0(m_0+1)}{2} \in Z^{-1}(m_0).$$

This shows that the set $Z^{-1}(m_0)$ is non-empty; moreover, $n_{\max}$ is the biggest element of $Z^{-1}(m_0)$, so that $Z^{-1}(m_0)$ is also bounded. Clearly, $n \in Z^{-1}(m_0)$ only if n divides $f(m_0) \equiv$

$m_0(m_0+1)/2$. This is a necessary condition, but is not sufficient. For example, $4|36 \equiv f(8)$ but $4 \notin Z^{-1}(8)$. The reason is that $Z(n)$ is not bijective. Let

$$Z^{-1} \equiv \sum_{m=1}^{\infty} Z^{-1}(m)$$

Let $n \in Z^{-1}$. Then, there is one and only one mo such that $n \in Z^{-1}(m_0)$, that is, there is one and only one mo such that $Z(n) = m_0$.
However, we have the following result whose proof is almost trivial : $n \in Z^{-1}(m_0)(n \neq 1, 3)$ if and only if the following two conditions are satisfied
(1) n divides $m_0(m_0+1)/2$,
(2) n does not divide $m(m+1)/2$ for any m with $3 \leq m \leq m_0 - 1$.
Since $4|28 \equiv f(7)$, it therefore follows that $4 \notin Z^{-1}(8)$.
Given any integer $m_0 \geq 1$, let $C(m_0)$ be the number of integers n such that $Z(n) = m_0$, that is, $C(m_0)$ denotes the number of elements of $Z^{-1}(m_0)$. Then,

$$1 \leq C(m_0) \leq d(m_0(m_0+1)/2) - 1 \quad form_0 \geq 3; \quad C(1) = 1, \quad C(2) = 2,$$

where, for any integer n, $d(n)$ denotes the number of divisors of n including 1 and n. Now, let $p \geq 3$ be a prime. Since, by Lemma 1.2, $Z(p) = p - 1$, we see that $p \in Z^{-1}(p-1)$ for all $p \geq 3$. Let $n \in Z^{-1}(p-1)$. Then, n divides $p(p-1)/2$. This shows that n must divide p, for otherwise

$$n|\frac{p-1}{2} \Rightarrow n|\frac{(p-1)(p-2)}{2} \Rightarrow Z(n) \leq p-2,$$

contradicting the assumption. Thus, any element of $Z^{-1}(p-1)$ is a multiple of p. In particular, p is the minimum element of $Z^{-1}(p-1)$. Thus, if $p \geq 5$ is a prime, then $Z^{-1}(p-1)$ contains at least two elements, namely, p and $p(p-1)/2$. Next, let p be a prime factor of $m_0(m_0+1)/2$. Since, by Lemma 1.2, $Z(p) = p-1$, we see that $p \in Z^{-1}(m_0)$ if and only if $p - 1 \geq m_0$, that is, if and only if $p \geq m_0 + 1$.

Remark 3.3. Ibstedt[2] provides a table of values of $Z(n)$ for $1 \leq n \leq 1000$. A closer look at these values reveal some facts about the values of $Z(n)$. These observations are given in the conjectures below, followed by discussions in each case.

Conjecture 1. $Z(n) = 2n - 1$ if and only if $n = 2^k$ for some integer $k \geq 0$.
Let, for some integer $n \geq 1$,

$$Z(n) = m_0, \text{ where } m_0 = 2n - 1.$$

Note that the conjecture is true for $n = 1$ (with $k = 0$). Also, note that n must be composite. Now, since $m_0 = 2n - 1$, and since $n|\frac{m_0(m_0+1)}{2}$, it follows that
n does not divide m_0, and $n|\frac{m_0+1}{2}$; moreover, by virtue of the definition of $Z(n)$, n does not divide m_0, and $n|\frac{m+1}{2}$ for all $1 \leq m \leq m_0 - 1$.
Let

$$Z(2n) = m_1.$$

We want to show that $m_1 = 2m_o + 1$. Since $n|\frac{m_0+1}{2}$, it follows that $2n|\frac{2(m_0+1)}{2} = \frac{(2m_0+1)+1}{2}$; moreover, $2n$ does not divide

$$\frac{2(m+1)}{2} = \frac{(2m+1)+1}{2}$$

for all $1 \leq m \leq m_0 - 1$.
Thus,

$$m_1 = 2m_0 + 1 = 2(2n - 1) + 1 = 2^2 n - 1.$$

All these show that

$$Z(n) = 2n - 1 \Rightarrow Z(2n) = 2^2 n - 1.$$

Continuing this argument, we see that

$$Z(n) = 2n - 1 \Rightarrow Z(2^k n) = 2^{k+1} n - 1.$$

Since $Z(1) = 1$, it then follows that $Z(2^k) = 2^{k+1} - 1$.

Conjecture 2. $Z(n) = n - 1$ if and only if $n = p^k$ for some prime $p \geq 3$ and integer $k \geq 1$.
Let, for some integer $n \geq 2$,

$$Z(n) = m_0, \text{ where } m_0 = n - 1.$$

Then, $2|m_0$ and $n|(m_0 + 1)$; moreover, n does not divide $m + 1$ for any $1 \leq m \leq m_0 - 1$.
Let

$$Z(n^2) = m_1.$$

Since $n|(m_0 + 1)$, it follows that

$$n^2 | (m_0 + 1)^2 = (m_0^2 + 2m_0) + 1;$$

moreover, n^2 does not divide$|(m + 1)^2 = (m^2 + 2m) + 1$ for all $1 \leq m \leq m_0 - 1$.
Thus,

$$m_1 = m_0^2 + 2m_0 = (n - 1)^2 + 2(n - 1) = n^2 - 1,$$

so that(since $2|m_0 \Rightarrow 2|m_1$)

$$Z(n) = n - 1 \Rightarrow Z(n^2) = n^2 - 1.$$

Continuing this argument, we see that

$$Z(n) = n - 1 \Rightarrow Z(n^{2k}) = n^{2k} - 1.$$

Next, let

$$Z(n^{2k+1}) = m_2 \text{ for some integer } k \geq 1.$$

Since $n|(m_0 + 1)$, it follows that

$$n^{2k+1} | (m_0 + 1)^{2k+1} = [(m_0 + 1)^{2k+1} - 1] + 1;$$

moreover,
n^{2k+1} does not divide

$$|(m + 1)^{2k+1} = [(m + 1)^{2k+1} - 1] + 1$$

for all $1 \leq m \leq m_0 - 1$. Thus,

$$m_2 = (m_0 + 1)^{2k+1} - 1 = n^{2k+1} - 1,$$

so that (since $2|m_0 \Rightarrow 2|m_2$)

$$Z(n) = n - 1 \Rightarrow Z(n^{2k+1}) = n^{2k+1} - 1.$$

All these show that

$$Z(n) = n - 1 \Rightarrow Z(n^k) = n^k - 1.$$

Finally, since $Z(p) = p - 1$ for any prime $p \geq 3$, it follows that $Z(p^k) = p^k - 1$.

Conjecture 3. If n is not of the form 2^k for some integer $k \geq 0$, then $Z(n) < n$. First note that, we can exclude the possibility that $Z(n) = n$, because

$$n|\frac{n(n+1)}{2} \Rightarrow n|\frac{n(n-1)}{2} \Rightarrow Z(n) \leq n - 1.$$

So, let

$$Z(n) = m_0 \text{ with } m_0 > n.$$

Note that, n must be a composite number, not of the form p^k ($p \geq 3$ is prime, $k \geq 0$). Let

$$m_0 = an + b \text{ for some integers } a \geq 1, 1 \leq b \leq n1.$$

Then,

$$m_0(m_0 + 1) = (an + b)(an + b + 1) = n(a^2n + 2ab + a) + b(b + 1).$$

Therefore,

$$n|m_0(m_0 + 1) \text{ if and only if } b + 1 = n.$$

But, by Conjecture 1, $b + 1 = n$ leads to the case when n is of the form 2^k.

Remark 3.4. Kashihara proposes (see Problem 4(a) in [1]) to find all the values of n such that $Z(n) = Z(n + 1)$. In this connection, we make the following conjecture :

Conjecture 4. For any integer $n \geq 1$, $Z(n) \neq Z(n + 1)$. Let

$$Z(n) = Z(n + 1) = m_0 \text{ for some } n \in N, m_0 \geq 1. \tag{69}$$

Then, neither n nor $n + 1$ is a prime.

To prove this, let $n = p$, where p is a prime. Then, by Lemma 1.2, $Z(n) = Z(p) = p - 1$.

$$n + 1 = p + 1 \text{ does not divide } \frac{p(p-1)}{2} \Rightarrow Z(n + 1) \neq p - 1 = Z(n).$$

Similarly, it can be shown that $n + 1$ is not a prime. Thus, both n and $n + 1$ are composite numbers.

From (68), we see that both n and $n + 1$ divide $m_0(m_0 + 1)/2$. Let

$$\frac{m_0(m_0 + 1)}{2} = an \text{ for some integer } a \geq 1.$$

Since $n + 1$ divides $m_0(m_0 + 1)$ and since $n + 1$ does not divide n, it follows that $n + 1$ must divide a. So, let

$$a = b(n + 1) \text{ for some integer } b \geq 1.$$

Then,

$$\frac{m_0(m_0+1)}{2} = abn(n+1),$$

which shows that

$$n(n+1) \text{ must divide } \frac{m_0(m_0+1)}{2}. \tag{70}$$

From (69), we see that

$$Z(n(n+1)) \leq m_0,$$

which, together with Lemma 1.5 (that $Z(n(n+1)) \geq Z(n)$), gives

$$Z(n(n+1)) = m_0. \tag{71}$$

From (70), we see that

$$n(n+1)\frac{m_0(m_0+1)}{2} \Rightarrow \frac{n(n+1)}{2} | \frac{m_0(m_0+1)}{2} \Rightarrow Z(\frac{n(n+1)}{2}) \leq m_0.$$

Thus, by virtue of Lemma 2.1, $Z(\frac{n(n+1)}{2}) = n \leq m_0 = Z(n)$. It can easily be verified that neither n nor $n+1$ can be of the form $2k$. Thus, if Conjecture 3 is true then Conjecture 4 is also true.

Remark 3.5. An integer $n > 0$ is called f-perfect if

$$n = \sum_{i=1}^{k} f(d_i),$$

where $d_1 \equiv 1, d_2, \ldots, d_k$ are the proper divisors of n, and f is an arithmetical function. In particular, n is Pseudo-Smarandache perfect if

$$n = \sum_{i=1}^{k} Z(d_i).$$

In [4], Ashbacher reports that the only Pseudo-Smarandache perfect numbers less than $1,000,000$ are $n = 4, 6, 471544$. However, since $n = 471544$ is of the form $n = 8p$ with $p = 58943$, its only perfect divisors are $1, 2, 4, 8, p, 2p$ and $4p$. Since $8|(p+1) = 58944$, it follows from Lemma 1.2, Theorem 2.1 and Theorem 2.7 that

$$Z(p) = p-1, \quad Z(2p) = p, \quad Z(4p) = p,$$

so that

$$n = 471544 > \sum_{i=1}^{k} Z(d_i),$$

so that $n = 471544$ is not Pseudo-Smarandache perfect.

References

[1] Kashihara, Kenichiro, Comments and Topics on Smarandache Notions and Problems, USA, Erhus University Press, 1996.

[2] Ibstedt, Henry, Surfing on the Ocean of Numbers-A Few Smarandache Notions and Similar Topics, USA, Erhus University Press, 1997.

[3] Gioia, Anthony A, The Theory of Numbers - An Introduction, NY, USA, Dover Publications Inc., 2001.

[4] Ashbacher, Charles, On Numbers that are Pseudo-Smarandache and Smarandache perfect, Smarandache Notions Journal, **14**(2004), pp. 40 - 41.