Chapter 4

Some rational integers as representatives of equivalence classes having their recurred inverses

4.1 Introduction

In this chapter an elaborate attempt has been made to determine the inverse of a rational integer, which in turn is a recurring one with a recurred set, independent of \( p \).

If we consider the polynomial \( p(x) = ax - e_0; a = \{a_i\}, x, e_0 \in \Omega_p \) with \( a_0 \neq 0 \) then \( p'(x) = a \). As \( a_0 \neq 0 \) it follows from the Hensel's lemma that any root of \( p(x) \equiv 0 \) (mod \( p \)) can be improved to a root of mod \( p^n(n \geq 2) \). But \( ax \equiv e_0 \) (mod \( p \)) gives an infinite set of Diophantine equations together with a carry-out sequence, denoted by \([ax \equiv e_0 \text{ (mod } p)\]). In the sense of incongruence, unique solution of each of the Diophantine equations exist, which will provide the inverse of \( a \in \Omega_p \). We have to workout the process of solving Diophantine equations obtained from \( ax \equiv e_0 \) (mod \( p \)) in order, because the carry-out element for \((k+1)^{th}\) equation is generated during the process of solving \( k^{th} \) equation. Solving this set of equations up-to any desired step one can approximate the \( I_p(a) \) (inverse of \( a \) in \( \Omega_p \)) up-to any degree of \( p \). But the complete determination of \( I_p(a) \) is possible, if it happens to be a recurring \( p \)-adic integer. It may so happen that \( I_p(a) \) is recurring one but the order of the recurred set \( R \) is dependent on \( p \) [Theorem 4.3.5 (b)]. In order to make it more fascinating, in the next section we have made an attempt to identify those rational integers \( a \) for which \( I_p(a) \) is not only a recurring \( p \)-adic integer but also its recurred set \( R \) is independent of \( p \).

At this point, let us define a relation in the field of \( p \)-adic numbers \( \mathbb{Q}_p \) by,

\[
x \sim y \text{ if and only if } x = e_ky \text{ for some } k \geq -n_0 \text{ where } x, y \in \mathbb{Q}_p.
\]
The relation ~ so defined is an equivalence relation in \( \mathbb{Q}_p \), for

\[
x = e_0x \text{ and hence } x \sim x \text{ for any } x \in \mathbb{Q}_p
\]

\[
x \sim y \Rightarrow x = e_ky \text{ for some } k \geq -n_0 \Rightarrow y = e_{-k}x \Rightarrow y \sim x
\]

and

\[
x \sim y \text{ and } y \sim z \Rightarrow x = e_ny \text{ and } y = e_nz \text{ for some } m, n \geq -n_0 \Rightarrow x = e_{m+n}z \Rightarrow x \sim z
\]

On the other hand, \( I_p(e_kx) = e_{-k}I_p(x) \). Thus if for some rational integer \( x \) we can prove that \( I_p(x) \) is recurred one with a recurred set \( R \) which is independent of \( p \) then the inverse of each member of the equivalence class \( [x] \) will be a recurred one with a \( p \) independent recurred set. In the third section of this chapter we have determined a number of rational integers which can be considered as representatives of such equivalence classes. Again the inception of the concept **Functionally Recurred** has added an extra dimension to the carry-out sequences under scrutiny. In the course of development it has been seen that \( [ax \equiv e_0 \pmod{p}] \) happens to be functionally recurred in general.

### 4.2 Some definitions

**Definition 4.2.1.** A \( p \)-adic integer \( x = \{x_i\} \) is said to be a recurring \( p \)-adic integer of degree \( n \) if the terms of \( x \) after the \( n^{th} \) term satisfy the following:

\[
\begin{align*}
x_n &= x_{n+m} = x_{n+2m} = \ldots \\
x_{n+1} &= x_{n+m+1} = x_{n+2m+1} = \ldots \\
&\vdotswithin{=} \\
x_{n+m-1} &= x_{n+2m-1} = x_{n+3m-1} = \ldots
\end{align*}
\]

Then we write \( x = \{x_0, x_1, \ldots, x_{n-1}, R\} \) where \( R = (x_n, x_{n+1}, \ldots, x_{n+m-1}) \). The elements \( x_0, x_1, \ldots, x_{n-1} \) are said to be the leading elements and the set \( R \) is said to be the recurred set for \( x \), which is obviously an ordered set.

If an element \( x_0 \) (say) occupies \( k \) numbers of consecutive positions in the recurred set \( R \) then we write, \( R = (x_n, x_{n+k}, x_{n+k+1}, \ldots, x_{n+m-1}) \). We follow the same convention for the set of leading elements too.

Clearly a recurring \( p \)-adic integer is completely determined by its leading elements and by the recurred set \( R \).
Definition 4.2.2. A $p$-adic integer $x = \{x_t\}$ is said to be a functionally recurred $p$-adic integer of degree $n$ and of order $m$ if $x = \{x_0, x_1, \ldots, x_{n-1}, R_0, R_1, \ldots\}$ where $R_0 = (x_n, x_{n+1}, \ldots, x_{n+m-1})$ and for any $k \geq 1$ there exists a one to one function $f_k : R_0 \mapsto R_k$ such that

$$f_k(x_{n+i}) = x_{n+k+m+i} \quad ; \quad 0 \leq i \leq m - 1.$$ 

We denote such a functionally recurred $p$-adic integer as $\langle (x_0, x_1, \ldots, x_{n-1}, R_0) ; f_k \rangle$. In case of a functionally recurred $p$-adic integer of degree 0, we simply write $(R_0; f_k)$.

We follow the same notational convention for the leading elements and the elements in the recurred sets $R_k$ as in case of recurring $p$-adic integers.

Remark 4.2.3. For the complete determination of a functionally recurred $p$-adic integer we have to go through the following steps:

- To identify the leading elements $x_0, x_1, \ldots, x_{n-1}$ provided they do exist.
- To determine the elements of the recurred set $R_0$.
- To determine a one to one function $f_k : R_0 \mapsto R_k$ for any $k \geq 1$.

Remark 4.2.4. It should be noted that every recurring $p$-adic integer is a functionally recurred one under the identity map.

Definition 4.2.5. For $k \geq -n_0$ where $n_0$ is a positive integer, we define $e_k = \{x_t\} \in \mathbb{Q}_p$ by

$$x_k = 1 \quad \text{and} \quad x_i = 0 \quad \forall i \neq k$$

Remark 4.2.6. Clearly for $k \geq 0, e_k \in \Omega_p$ and

$$e_k = \{0^k, 1, R\} \quad \text{where} \quad R = (0)$$

It follows that $e_k$ is a recurring $p$-adic integer of degree $k+1$ with the recurred set $R$ of order 1.

By the Definition 3.2.3 of multiplication in $\Omega_p$ it is easy to see that,

$$e_i e_j = e_{i+j} \quad \text{and} \quad p e_i = e_{i+1} \quad \forall i, j$$

Definition 4.2.7. We define $e = \{x_t\} \in \Omega_p$ by $x_i = 1 \quad \forall i = 0, 1, 2, 3, \ldots$ Clearly $e$ is a recurring $p$-adic integer of degree 0 with the recurred set $R = (1)$ and $e = \sum_{i \geq 0} e_i$. 

54
Definition 4.2.8. For any $\alpha \in B = \{0, 1, 2, 3, \ldots, p-1\}$ and for any $x = \{x_i\} \in \Omega_p$ we define,

$$ax = y \iff \alpha x_i + b_i = b_{i+1}p + y_i \quad \forall i = 0, 1, 2, \ldots \text{ with } b_0 = 0$$

where $b = \{b_i\}$ is the carry-out sequence $[ax]$.

If we take $\alpha = \{\alpha, R\}$ with the recurred set $R = (0)$ then the product $ax$ defined above will coincide with the product in the ring $\Omega_p$.

In general, the carry-out sequence $[ax]$ of $ax$ for arbitrary $\alpha$ does not belong to $\Omega_p$. However the following theorem provides the conditions on the scalar $\alpha$, so that the carry-out sequence $[ax] \in \Omega_p$.

Theorem 4.2.9. For any $\alpha \in B = \{0, 1, 2, \ldots, p-1\}$ and for any $x \in \Omega_p$ the carry-out sequence $[\alpha x] \in \Omega_p$.

Proof: If $\alpha = 0$ then $[ax] = 0$ and therefore we are through.

Let us take $\alpha \neq 0$ and let $[\alpha x] = b, \alpha x = y$.

$$\therefore \alpha x_i + b_i = b_{i+1}p + y_i \quad \forall i = 0, 1, 2, \ldots \text{ with } b_0 = 0. \quad (4.2.1)$$

Clearly, $b_0 = 0 < \alpha$. If possible let $b_1 > \alpha$ so that

$$b_1p + y_0 > \alpha p + y_0$$

i.e. $\alpha x_0 > \alpha p + y_0$ using (1) for $i = 0$.

i.e. $\alpha(x_0 - p) > y_0$, a contradiction.

Assuming $b_m \leq \alpha$, we try to show that $b_{m+1} \leq \alpha$.

If $b_{m+1} > \alpha$ then

$$b_{m+1}p + y_m > \alpha p + y_m$$

i.e. $b_m > \alpha(p - x_m) + y_m > \alpha$
This contradicts our initial assumption that $b_m \leq \alpha$.

Thus by induction, $b_i \leq \alpha < p \quad \forall i = 0, 1, 2, 3, \ldots$

This completes the proof.

In the following result we have determined a recurring relation among $I_p(p-1), I_p(2)$ and $I_q(2)$ for two consecutive primes $p$ and $q$.

**Theorem 4.2.10.** If $p, q$ be two consecutive primes $(p > q)$ with $(2n - 1)$ number of composites between them, then

$$I_p(p-1) + I_p(2) = (n-1)e + I_q(2).$$

**Proof:** If we take $I_p(2) = x$ and $I_p(p-1) = y$ then

$$x_0 = \frac{p+1}{2}, \quad x_i = \frac{p-1}{2} \quad \forall i \geq 1$$

and $$y_0 = p-1, \quad y_i = p-2 \quad \forall i \geq 1$$

Taking $x+y=z$ and $|x+y|=b$ we obtain,

$$x_i + y_i + b_i = b_{i+1} + z_i \quad \forall i = 0, 1, 2, 3, \ldots \text{ with } b_0 = 0. \quad (4.2.2)$$

Substituting $i = 0$ in equation (4.2.2) we obtain,

$$z_0 + b_1p = p + (n - 1) + \frac{q+1}{2} \quad [\because p = q + 2n]$$

$$\therefore z_0 = (n - 1) + \frac{q+1}{2}, \quad b_1 = 1$$

Again substituting $i = 1$ in equation (4.2.2) we obtain,

$$z_1 + b_2p = p + (n - 1) + \frac{q-1}{2}$$

$$\therefore z_1 = (n - 1) + \frac{q-1}{2}, \quad b_2 = 1 \text{ and so on.}$$
Continuing this process,

\[ z_i = (n - 1) + \frac{q - 1}{2} \quad \forall i \geq 1 \]

This completes the proof.

4.3 Some equivalence classes represented by rational integers having inverses with a recurred set independent of \( p \)

All results in this section are used to determine those rational integers \( a \) for which \( I_p(a) \) is a recurring \( p \)-adic integer with a recurred set, the order of which is independent of \( p \). In the second part of Theorem 4.3.5 the existence of a rational integer \( \alpha \) has been shown for which \( I_p(\alpha) \) is a recurring \( p \)-adic integer but the order of the recurred set is dependent of \( p \). An attempt has always been made to incorporate the carry-out sequences with those results whenever their beautiful forms are found.

**Theorem 4.3.1.** In the ring of \( p \)-adic integers \( \Omega_p \), the following results hold good:

(a) For \( p > 2 \), \( I_p(2) \) is a recurring \( p \)-adic integer of degree 1 and the order of the recurred set is 1 i.e. \( I_p(2) = \left\{ \frac{p+1}{2}, R \right\} \) where \( R = \left( \frac{p-1}{2} \right) \). Moreover,

\[ [2x \equiv e_0 \pmod{p}] = \{0, R'\} \quad \text{where,} \quad R' = (1) \]

(b) If \( 2\alpha = p + 1 \) then \( I_p(\alpha) \) is a recurring \( p \)-adic integer of degree 1 and the order of the recurred set \( R \) is 2 i.e. \( I_p(\alpha) = \{2, R\} \) where \( R = (p - 2, 1) \). Moreover,

\[ [\alpha x \equiv e_0 \pmod{p}] = \{0, R'\} \quad \text{where,} \quad R' = (1, \alpha - 1) \]

(c) \( I_p(p - 1) \) is a recurring \( p \)-adic integer of degree 1 and the order of the recurred set \( R \) is 1 i.e. \( I_p(p - 1) = \{p - 1, R\} \) where \( R = (p - 2) \). Moreover,

\[ [(p - 1)x \equiv e_0 \pmod{p}] = \{0, R'\} \quad \text{where,} \quad R' = R \]

**Proof:** (a) The relation \( 2x \equiv e_0 \pmod{p} \) gives,
\[2x_0 \equiv 1 \pmod{p} \implies x_0 = \frac{p+1}{2}, \quad b_1 = 1\]

\[2x_1 + 1 \equiv 0 \pmod{p} \implies x_1 = \frac{p-1}{2}, \quad b_2 = 1\]

\[2x_2 + 1 \equiv 0 \pmod{p} \implies x_2 = \frac{p-1}{2}, \quad b_3 = 1 \quad \text{and so on.}\]

\[\therefore J_p(2) = \left\{ \frac{p+1}{2}, R \right\} \quad \text{where} \quad R = \left( \frac{p-1}{2} \right)\]

and

\[\left[ 2x \equiv e_0 \pmod{p} \right] = \{0, R\} \quad \text{where} \quad R = (1)\]

(b) The relation \(\alpha x \equiv e_0 \pmod{p}\) gives,

\[\alpha x_0 \equiv 1 \pmod{p} \implies x_0 = 2, \quad b_1 = 1\]

\[\alpha x_1 \equiv 0 \pmod{p} \implies x_1 = p - 2, \quad b_2 = \alpha - 1\]

\[\alpha x_2 + \alpha - 1 \equiv 0 \pmod{p} \implies x_2 = 1, \quad b_3 = 1 \quad \text{and so on.}\]

\[\therefore J_p(\alpha) = \{2, R\} \quad \text{where} \quad R = (p - 2, 1)\]

and \([\alpha x \equiv e_0 \pmod{p}] = \{0, R'\} \quad \text{where} \quad R' = (1, \alpha - 1)\]

(c) The relation \((p-1)x \equiv e_0 \pmod{p}\) gives,

\[(p-1)x_0 \equiv 1 \pmod{p} \implies x_0 = p - 1, \quad b_1 = p - 2\]

\[(p-1)x_1 + (p-2) \equiv 0 \pmod{p} \implies x_1 = p - 2, \quad b_2 = p - 2 \quad \text{and so on.}\]

\[\therefore J_p(p-1) = \{p - 1, R\} \quad \text{where} \quad R = (p - 2)\]

and \([(p-1)x \equiv e_0 \pmod{p}] = \{0, R'\} \quad \text{where} \quad R' = R.\]
Corollary 4.3.2. (i) From (b) we obtain,

\[ I_p \left( \frac{p+1}{2} \right) = \{2, R\} \quad \text{where} \quad R = (p - 2, 1) \]

(ii) If \( p, q \) be any two primes such that \( 2q = p + 3 \) then \( I_q(q - 1) = I_p(2) \)

(iii) \( e + I_p(p - 1) = 0 \) and hence

\[ I_p(e) = -(p - 1)e_0 = e_0 + (p - 1) \sum_{i \geq 1} e_i \]

(iv) \( I_p(e_0 + (p - 2)e_1) = \{1, R\} \quad \text{where} \quad R = (2, 3, 4, \ldots, p - 1, 0) \)

Moreover the carry-out sequence \( [e^2] \) is functionally recurred one of degree 1 and of order \((p - 1)\).

Proof: As \((p - 1)^2 = e_0 + (p - 2)e_1\), it follows that

\[ I_p(e_0 + (p - 2)e_1) = I_p(p - 1)I_p(p - 1) = e.e \]

Suppose that \( x = e = y \quad \text{and} \quad xy = z \quad \text{with} \quad [xy] = b. \)

From definition it follows that

\[ z_i + b_{i+1}p = \sum_{j+k=i} x_j y_k + b_i \quad \forall i = 0, 1, 2, \ldots \quad \text{with} \quad b_0 = 0 \]

As \( \sum_{j+k=i} x_j y_k = (i + 1) \) the above relation can be written as

\[ z_i + b_{i+1}p = (i + 1) + b_i \quad \forall i = 0, 1, 2, \ldots \quad \text{with} \quad b_0 = 0 \quad (4.3.1) \]

Substituting \( i = 0, 1, \ldots, (p - 1) \) in equation \((4.3.1)\) we obtain

\[ z_0 + b_1p = 1 + 0.p \quad \Rightarrow \quad z_0 = 1 \quad ; \quad b_1 = 0 \]
\[ z_1 + b_2p = 2 + 0.p \quad \Rightarrow \quad z_1 = 2 \quad ; \quad b_2 = 0 \]
\[ \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \]
\[ z_{p-2} + b_{p-1}p = (p - 1) + 0.p \quad \Rightarrow \quad z_{p-2} = p - 1 \quad ; \quad b_{p-1} = 0 \]
\[ z_{p-1} + b_{p}p = 0 + 1.p \quad \Rightarrow \quad z_{p-1} = 0 \quad ; \quad b_{p} = 1 \]
Again by the substitution $i = p, p + 1, \ldots, 2p - 2$ in equation (4.3.1) we obtain

$$z_p + b_{p+1}p = 2 + 1.p \Rightarrow z_p = 2 \quad ; \quad b_{p+1} = 1$$

$$z_{p+1} + b_{p+2}p = 3 + 1.p \Rightarrow z_{p+1} = 3 \quad ; \quad b_{p+2} = 1$$

$$\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots$$

$$z_{2p-3} + b_{2p-2}p = (p - 1) + 1.p \Rightarrow z_{2p-3} = (p - 1) ; \quad b_{2p-2} = 1$$

$$z_{2p-2} + b_{2p-1}p = 0 + 2.p \Rightarrow z_{2p-2} = 0 \quad ; \quad b_{2p-1} = 2$$

and so on.

If we take $R_0 = \{b_i : 0 \leq i \leq (p-1)\}$ then for $k \geq 1$ the function $f_k : R_0 \mapsto R_k$ defined by

$$f_k(b_i) = k \quad 1 \leq i \leq (p-1)$$

will establish that the carry-out sequence $[c^2] = b$ is functionally recurred and therefore $[c^2] = (0, R_0 ; f_k)$ where $|R_0| = (p - 1)$.

This completes the proof.

**Remark 4.3.3.** If we take $I_p(e_0 + (p - 1)e_1 + (p - 2)e_2) = x = \{x_i\}$ then

$$x_i = \begin{cases} 
(i + 1) \pmod{p} & \text{if } 0 \leq i \leq (p - 1) \\
(i + n) \pmod{p} & \text{if } (n - 1)p - (n - 2) \leq i \leq n(p - 1) \text{ and } n(\geq 2) \in \mathbb{N}
\end{cases}$$

**Corollary 4.3.4.** For $p \geq 3$, $I_p(e_0 + (p - 1)e_1 + (p - 2)e_2)$ is a recurring one of degree $2(p-1)$

and $I_p(e_0 + (p - 1)e_1 + (p - 2)e_2) = \{1^2, 2^2, \ldots, (p - 1)^2, R\}$ where

$$R = (0, 1, 2^2, \ldots, (p - 1)^2)$$

**Proof:** We have,

$$e_0 + (p - 1)e_1 + (p - 2)e_2 = (p - 1)^2(e_0 + e_1)$$
\[ I_p(e_0 + (p-1)e_1 + (p-2)e_2) = I_p(p-1).I_p(p-1).I_p(e_0 + e_1) = e^2 I_p(e_0 + e_1) \]

Suppose that \( x = e^2 = I_p(e_0 + (p-2)e_1) \) and \( y = I_p(e_0 + e_1) \).

\[ : x_i = \begin{cases} 
(i + 1) \pmod{p} & \text{if } 0 \leq i \leq (p-1) \\
(i + n) \pmod{p} & \text{if } (n-1)p - (n-2) \leq i \leq n(p-1) \text{ and } n \geq 2 \in \mathbb{N} 
\end{cases} \]

and

\[ y_i = \begin{cases} 
1 & \text{if } i = 0 \\
p - 1 & \text{if } i \text{ is odd} \\
0 & \text{if } i \text{ is even} 
\end{cases} \]

Let \( xy = z \) and \([xy] = b \). It follows from the definition that

\[ z_i + b_{i+1}.p = \sum_{j+k=i} x_jy_k + b_i \quad \forall i = 0, 1, 2, \ldots \text{ with } b_0 = 0. \]

Considering the form of \( y \), the above relation can be put into the following form

\[ z_i + b_{i+1}.p = \begin{cases} 
x_i + (p-1) \sum_{s=1}^{\frac{i}{2}} x_{2s-1} + b_s & \text{if } i \text{ is even} \\
x_i + (p-1) \sum_{s=0}^{\frac{i-1}{2}} x_{2s} + b_s & \text{if } i \text{ is odd} 
\end{cases} \quad (4.3.2) \]

Substituting \( i = 0, 1, \ldots, 7 \) in equation (4.3.2) we get,
\[ z_0 = 1 \quad b_1 = \frac{1+1}{2} = \frac{1}{2} \]
\[ z_1 = 1 \quad b_2 = \frac{2}{2} \]
\[ z_2 = 2 \quad b_3 = \frac{3+1}{2} = \frac{3}{2} \]
\[ z_3 = 2 \quad b_4 = \frac{4}{2} \]
\[ z_4 = 3 \quad b_5 = \frac{5+1}{2} = \frac{5-1}{2} \]
\[ z_5 = 3 \quad b_6 = \frac{6}{2} \]
\[ z_6 = 4 \quad b_7 = 12 = \frac{7+1}{2} = \frac{7-1}{2} \]
\[ z_7 = 4 \quad b_8 = 16 = \frac{8}{2} \]

From the values of \( b_i \) evaluated so far we can conclude that

\[ b_{2n-1} = n(n-1) \quad \text{and} \quad b_{2n} = n^2 \]

and hence

\[ b_{p-3} = \left( \frac{p-3}{2} \right)^2 \]

Now substituting \( z = p - 3, p - 2, p - 1, p \) in equation (4.3.2) we get,

\[ z_{p-3} + b_{p-2} \cdot p = x_{p-3} + (p - 1) \sum_{s=1}^{x_{p-3}} x_{2s-1} + b_{p-3} \]

\[ = (p - 2) + (p - 1)(x_1 + x_2 + \ldots + x_{p-4}) + b_{p-3} \]

\[ = (p - 2) + 2(p - 1) \left( 1 + 2 + \ldots + \frac{p-3}{2} \right) + \left( \frac{p-3}{2} \right)^2 \]

\[ = \left( \frac{p^2 - 4p + 3}{4} \right) p + \left( \frac{p-1}{2} \right) \]

\[ : z_{p-3} = \frac{p-1}{2} \quad \text{and} \quad b_{p-2} = \frac{p^2 - 4p + 3}{4} = \left( \frac{p-1}{2} \right) \left( \frac{p-1}{2} - 1 \right) \]
\[ z_{p-2} + b_{p-1} = x_{p-2} + (p - 1) \sum_{s=0}^{\frac{p-3}{2}} x_{2s} + b_{p-2} \]

\[ = (p - 1) + (p - 1)(x_0 + x_2 + \ldots + x_{p-3}) + b_{p-2} \]

\[ = (p - 1) + (p - 1)(1 + 3 + \ldots + p - 2) + \left( \frac{p^2 - 4p + 3}{4} \right) \]

\[ = \left( \frac{p^2 - 2p + 1}{4} \right) p + \left( \frac{p - 1}{2} \right) \]

\[ \therefore z_{p-2} = \frac{p - 1}{2} \quad \text{and} \quad b_{p-1} = \frac{p^2 - 2p + 1}{4} = \left( \frac{p - 1}{2} \right)^2 \]

\[ z_{p-1} + b_p = x_{p-1} + (p - 1) \sum_{s=1}^{\frac{p-1}{2}} x_{2s-1} + b_{p-1} \]

\[ = 0 + (p - 1)(x_1 + x_3 + \ldots + x_{p-2}) + b_{p-1} \]

\[ = (p - 1)(2 + 4 + \ldots + (p - 1)) + \left( \frac{p - 1}{2} \right)^2 \]

\[ = \left( \frac{p^2 - 5}{4} \right) p + \left( \frac{p + 1}{2} \right) \]

\[ \therefore z_{p-1} = \frac{p + 1}{2} \quad \text{and} \quad b_p = \frac{p^2 - 5}{4} \]

By the substitution \( i = p, p + 1, \ldots, p + 6 \) in equation (4.3.2) it can be deduce that
\[ z_p = \frac{p + 1}{2} \quad b_{p+1} = \left(\frac{p - 1}{2}\right)^2 + 0 = \left(\frac{p - 1}{2}\right)^2 + \left(\frac{1 + 1}{2}\right)^2 - 1 \]

\[ z_{p+1} = \frac{p + 3}{2} \quad b_{p+2} = \frac{p^2 + 3}{4} = \frac{p^2 - 5}{4} + 2 \]

\[ z_{p+2} = \frac{p + 3}{2} \quad b_{p+3} = \frac{p^2 - 2p + 13}{4} = \left(\frac{p - 1}{2}\right)^2 + \left(\frac{3 + 1}{2}\right)^2 - 1 \]

\[ z_{p+3} = \frac{p + 5}{2} \quad b_{p+4} = \frac{p^2 + 19}{4} = \frac{p^2 - 5}{4} + 6 \]

\[ z_{p+4} = \frac{p + 5}{2} \quad b_{p+5} = \frac{p^2 - 2p + 33}{4} = \left(\frac{p - 1}{2}\right)^2 + \left(\frac{5 + 1}{2}\right)^2 - 1 \]

\[ z_{p+5} = \frac{p + 7}{2} \quad b_{p+6} = \frac{p^2 + 43}{4} = \frac{p^2 - 5}{4} + 12 \]

\[ z_{p+6} = \frac{p + 7}{2} \quad b_{p+7} = \frac{p^2 - 2p + 61}{4} = \left(\frac{p - 1}{2}\right)^2 + \left(\frac{7 + 1}{2}\right)^2 - 1 \]

The initial values of \( b_i^e \) in this section motives to take

\[ b_{p+2n-1} = \left(\frac{p - 1}{2}\right)^2 + n^2 - 1 \quad \text{and} \quad b_{p+2n} = \left(\frac{p^2 - 5}{4}\right) + n(n + 1) \]

and hence

\[ b_{2p-3} = \left(\frac{p^2 - 5}{4}\right) + \left(\frac{p - 3}{2}\right) \left(\frac{p - 3}{2} + 1\right) = \frac{p^2 - 2p - 1}{2} \]

Now substituting \( i = 2p - 3, 2p - 2, 2p - 1, 2p \) in equation (4.3.2) we obtain,
\[ z_{2p-3} + b_{2p-3, p} = x_{2p-3} + (p - 1) \sum_{s=0}^{p-2} x_{2s} + b_{2p-3} \]

\[ = (p - 1) + (p - 1)(x_0 + x_2 + \ldots + x_{2p-4}) + b_{2p-3} \]

\[ = (p - 1) + (p - 1)[(1 + 3 + \ldots + p - 2) + (3 + 5 + \ldots + p - 2)] + b_{2p-3} \]

\[ = 2(p - 1)(1 + 3 + \ldots + p - 2) + \frac{p^2 - 2p - 1}{2} \]

\[ = \left( \frac{p^2 - 2p - 1}{2} \right) p + (p - 1) \]

\[
\therefore \, z_{2p-3} = p - 1 \text{ and } b_{2p-3} = \frac{p^2 - 2p - 1}{2} = \left( \frac{p - 1}{2} \right)^2 + \left( \frac{p - 1}{2} \right)^2 - 1
\]

\[ z_{2p-2} + b_{2p-2, p} = x_{2p-2} + (p - 1) \sum_{s=1}^{p-1} x_{2s-1} + b_{2p-2} \]

\[ = 0 + (p - 1)(x_1 + x_3 + \ldots + x_{2p-3}) + b_{2p-2} \]

\[ = (p - 1)(x_1 + x_3 + \ldots + x_{p-2} + x_{p+1} + x_{p+3} + \ldots + x_{2p-3}) + b_{2p-2} \]

\[ = (p - 1)[(2 + 4 + \ldots + p - 1) + (2 + 4 + \ldots + p - 1)] + b_{2p-2} \]

\[ = 4(p - 1) \left( 1 + 2 + \ldots + \frac{p - 1}{2} \right) + \frac{p^2 - 2p - 1}{2} \]

\[ = \left( \frac{p^2 - 3}{2} \right) p + 0 \]

\[
\therefore \, z_{2p-2} = 0 \text{ and } b_{2p-2} = \frac{p^2 - 3}{2}
\]
\[ z_{2p-1} + b_{2p} = x_{2p-1} + (p - 1) \sum_{s=0}^{p-1} x_{2s} + b_{2p-1} \]

\[ = 2 + (p - 1)(x_0 + x_2 + \ldots + x_{2p-2}) + b_{2p-1} \]

\[ = 2 + (p - 1)(x_0 + x_2 + \ldots + x_{p-3} + x_{p-1} + x_{p+1} + \ldots + x_{2p-2}) + b_{2p-1} \]

\[ = 2 + (p - 1)[(1 + 3 + \ldots + p - 2) + (3 + 5 + \ldots + p - 2)] + b_{2p-1} \]

\[ = 2 + (p - 1)[(p - 1)^2 - 1] + \frac{p^2 - 3}{2} \]

\[ = \left( \frac{p^2 - 2p + 1}{2} \right) p + 1 \]

\[ \therefore z_{2p-1} = 1 \quad \text{and} \quad b_{2p} = \frac{p^2 - 2p + 1}{2} \]

\[ z_{2p} + b_{2p+1} = x_{2p} + (p - 1) \sum_{s=1}^{p} x_{2s-1} + b_{2p} \]

\[ = 3 + (p - 1)(x_1 + x_3 + \ldots + x_{2p-1}) + b_{2p} \]

\[ = 3 + (p - 1)(x_1 + x_3 + \ldots + x_{p-2} + x_p + x_{p+2} + \ldots + x_{2p-1}) + b_{2p} \]

\[ = 3 + (p - 1)[(2 + 4 + \ldots + p - 1) + (2 + 4 + \ldots + p - 1) + 2] + b_{2p} \]

\[ = (2p + 1) + 4(p - 1) \left( 1 + 2 + \ldots + \frac{p - 1}{2} \right) + \frac{p^2 - 2p + 1}{2} \]

\[ = \left( \frac{p^2 + 1}{2} \right) p + 2 \]

\[ \therefore z_{2p} = 2 \quad \text{and} \quad b_{2p+1} = \frac{p^2 + 1}{2} \]

Continuing up to \( i = 2p + 6 \) we obtain.
The initial values of $b_i$ in this section motives to take

\[ b_{2p+2n-1} = \left( \frac{p^2 - 3}{2} \right) + n(n + 1) \quad \text{and} \quad b_{2p+2n} = \frac{(p - 1)^2}{2} + n(n + 2) \]

and hence

\[ b_{3p-5} = \frac{(p - 1)^2}{2} + \left( \frac{p - 5}{2} \right) \left( \frac{p - 5}{2} + 2 \right) \]

Now substituting $i = 3p - 5, 3p - 4, 3p - 3$ in equation (4.3.2) we obtain
\[ z_{3p-5} + b_{3p-4} \cdot p = x_{3p-5} + (p - 1) \sum_{s=1}^{3p-5} x_{2s-1} + b_{3p-5} \]

\[ = (p - 2) + (p - 1)(x_1 + x_3 + \ldots + x_{3p-6}) + b_{3p-5} \]

\[ = (p - 2) + (p - 1) [(x_1 + x_3 \ldots + x_{p-2})] + \]

\[ (p - 1) [(x_p + x_{p+2} + \ldots + x_{2p-3}) + (x_{2p-1} + x_{2p+1} + \ldots + x_{3p-6})] + b_{3p-5} \]

\[ = (p - 2) + (p - 1)[(2 + 4 + \ldots + p - 1) + (2 + 4 + \ldots + p - 1)] + \]

\[ (p - 1)(2 + 4 + \ldots + p - 3) + b_{3p-5} \]

\[ = (p - 2) + (p - 1)\left(6(1 + 2 + \ldots + \frac{p - 1}{2}) - (2p - 3)\right) + \]

\[ \frac{(p - 1)^2}{2} + \left(\frac{p - 5}{2}\right)\left(\frac{p - 5}{2} + 2\right) \]

\[ = \left(\frac{3p^2 - 4p - 3}{4}\right) + \frac{p - 1}{2} \]

\[ \therefore z_{3p-5} = \frac{p - 1}{2} \text{ and } b_{3p-4} = \frac{3p^2 - 4p - 3}{4} \]

68
$$z_{3p-4} + b_{3p-3}p = x_{3p-4} + (p - 1) \sum_{s=0}^{3p-5 \over 2} x_{2s} + b_{3p-4}$$

$$= (p - 1) + (p - 1)(x_0 + x_2 + \ldots + x_{3p-5}) + b_{3p-4}$$

$$= (p - 1) + (p - 1)[(x_0 + x_2 + \ldots + x_{p-3})] +$$

$$(p - 1)[(x_{p+1} + x_{p+3} + \ldots + x_{2p-4}) + (x_{2p} + x_{2p+2} + \ldots + x_{3p-5})] + b_{3p-4}$$

$$= (p - 1) + (p - 1)[(1 + 3 + \ldots + p - 2) + (3 + 5 + \ldots + p - 2)] +$$

$$(p - 1)(3 + 5 + \ldots + p - 2) + b_{3p-4}$$

$$= (p - 1) \left[ \frac{(p - 1)^2}{4} - 1 \right] + \frac{3p^2 - 4p - 3}{4}$$

$$= \left( \frac{3p^2 - 6p - 1}{4} \right) p + \left( \frac{p - 1}{2} \right)$$

$$\therefore z_{3p-4} = \frac{p - 1}{2} \quad \text{and} \quad b_{3p-3} = \frac{3p^2 - 6p - 1}{4}$$

$$z_{3p-3} + b_{3p-2}p = x_{3p-3} + (p - 1) \sum_{s=1}^{3p-2 \over 2} x_{2s-1} + b_{3p-3}$$

$$= 0 + (p - 1)(x_1 + x_3 + \ldots + x_{3p-4}) + b_{3p-3}$$

$$= (p - 1)[(x_1 + x_3 + \ldots + x_{p-2})] +$$

$$(p - 1)[(x_p + x_{p+2} + \ldots + x_{2p-3}) + (x_{2p-1} + x_{2p+1} + \ldots + x_{3p-4})] + b_{3p-3}$$

$$= (p - 1)[(2 + 4 + \ldots + p - 1) + (2 + 4 + \ldots + p - 1)] +$$

$$(p - 1)(2 + 4 + \ldots + p - 1) + \frac{3p^2 - 6p - 1}{4}$$

$$= \left( \frac{3p^2 - 11}{4} \right) p + \left( \frac{p + 1}{2} \right)$$

$$\therefore z_{3p-3} = \frac{p + 1}{2} \quad \text{and} \quad b_{3p-2} = \frac{3p^2 - 11}{4}$$

By the substitution $i = 3p - 2, 3p - 1, \ldots, 3p + 3$ in equation (4.3.2) it can be seen that
\[z_{3p-2} = \frac{p + 1}{2}, \quad b_{3p-1} = \frac{3p^2 - 6p - 1}{4}\]
\[z_{3p-1} = \frac{p + 3}{2}, \quad b_{3p} = \frac{3p^2 - 3}{4}\]
\[z_{3p} = \frac{p + 3}{2}, \quad b_{3p+1} = \frac{3p^2 - 6p + 11}{4}\]
\[z_{3p+1} = \frac{p + 5}{2}, \quad b_{3p+2} = \frac{3p^2 + 13}{4}\]
\[z_{3p+2} = \frac{p + 5}{2}, \quad b_{3p+3} = \frac{3p^2 - 6p + 31}{4}\]
\[z_{3p+3} = \frac{p + 7}{2}, \quad b_{3p+4} = \frac{3p^2 + 37}{4}\]

With the help of these initial values of \(b_i^p\) in this section we can conclude that

\[b_{3p+2n-1} = \frac{3p^2 - 6p - 1}{4} + n(n + 2) \quad \text{and} \quad b_{3p+2n} = \frac{3p^2 - 11}{4} + (n + 1)(n + 2)\]

Finally by the substitution \(i = 4p - 6, 4p - 5, 4p - 4\) in equation (4.3.2) we get

\[z_{4p-6} + b_{4p-5}p = x_{4p-6} + (p - 1) \sum_{s=1}^{\frac{3p-3}{2}} x_{2s-1} + b_{4p-6}\]

\[= (p - 2) + (p - 1)(x_1 + x_3 + \ldots + x_{4p-7}) + b_{4p-6}\]

\[= (p - 2) + (p - 1) [(x_1 + x_3 + \ldots + x_{p-2}) + (x_p + x_{p+2} + \ldots + x_{2p-3})] +\]

\[(p - 1) [(x_{2p-1} + x_{2p+1} + \ldots + x_{3p-4}) + (x_{3p-2} + x_{3p} + \ldots + x_{4p-7})] + b_{4p-6}\]

\[= (p - 2) + (p - 1)[4(2 + 4 + \ldots + p - 1) - (p - 1)] +\]

\[\frac{3p^2 - 6p - 1}{4} + \left(\frac{p - 5}{2}\right)\left(\frac{p - 5}{2} + 2\right)\]

\[= (p^2 - p - 2)p + (p - 1)\]

\[
\therefore z_{4p-6} = p - 1 \quad \text{and} \quad b_{4p-5} = p^2 - p - 2
\]
\[ z_{4p-5} + b_{4p-4} \cdot p = x_{4p-5} + (p - 1) \sum_{s=0}^{2p-3} x_{2s} + b_{4p-5} \]

\[ = (p - 1) + (p - 1)(x_0 + x_2 + \ldots + x_{4p-6}) + b_{4p-5} \]

\[ = (p - 1) + (p - 1) [(x_0 + x_2 + \ldots + x_{p-3}) + (x_{p+1} + x_{p+3} + \ldots + x_{2p-4})] + \]

\[ (p - 1) [(x_{2p} + x_{2p+2} + \ldots + x_{3p-5}) + (x_{3p-1} + x_{3p+1} + \ldots + x_{4p-6})] + b_{4p-5} \]

\[ = (p - 1) + (p - 1) [(1 + 3 + \ldots + p - 2) + (3 + 5 + \ldots + p - 2)] + \]

\[ (p - 1) [(3 + 5 + \ldots + p - 2) + (3 + 5 + \ldots + p - 2)] + (p^2 - p - 2) \]

\[ = (p^2 - 2p - 1)p + (p - 1) \]

\[ \therefore z_{4p-5} = p - 1 \text{ and } b_{4p-4} = p^2 - 2p - 1 \]

\[ z_{4p-4} + b_{4p-3} \cdot p = x_{4p-4} + (p - 1) \sum_{s=1}^{2p-2} x_{2s-1} + b_{4p-4} \]

\[ = 0 + (p - 1)(x_1 + x_3 + \ldots + x_{4p-7}) + b_{4p-6} \]

\[ = (p - 2) + (p - 1) [(x_1 + x_3 + x_{p-2}) + (x_p + x_{p+2} + \ldots + x_{2p-3})] + \]

\[ (p - 1) [(x_{2p-1} + x_{2p+1} + \ldots + x_{3p-4}) + (x_{3p-2} + x_{3p} + \ldots + x_{4p-5})] + b_{4p-4} \]

\[ = (p - 1)[4(2 + 4 + \ldots + p - 1) + (p^2 - 2p - 1)] \]

\[ = (p^2 - 3)p + 0 \]

\[ \therefore z_{4p-4} = 0 \text{ and } b_{4p-4} = p^2 - 3 \]

This completes the proof.

**Theorem 4.3.5.** (a) For \( p \geq 7, \) if \( 3\alpha = p + 1, \) then

\[ I_p(3) = \{\alpha, R\}, \quad \text{where} \quad R = (p - \alpha, \alpha - 1) \]

\[ \text{and } I_p(\alpha) = \{3, R\} \quad \text{where} \quad R = (p - 3, 2) \]

Moreover,

\[ [3x \equiv e_0 \pmod{p}] = \{0, R'\} \quad \text{where} \quad R' = (1, 2) \]

\[ \text{and } [\alpha x \equiv e_0 \pmod{p}] = \{0, R'\} \quad \text{where} \quad R' = (1, \alpha - 1) \]
(b) In case $3\alpha = 2p + 1$,

$$I_p(3) = \{\alpha, R\} \text{ where } R = (\alpha - 1)$$

and $[3x \equiv e_0 \pmod{p}] = \{0, R'\}$ where $R' = (2)$

However in case of $I_p(\alpha)$ the recurred set is dependent on $p$ and

$$I_p(\alpha) = \{3, p - 6, 11, p - 24, 47, p - 96, 191, p - 384, 767, p - 1536, \ldots\}$$

**Proof:** (a) The relation $3x \equiv e_0 \pmod{p}$ gives,

$$3x_0 \equiv 1 \pmod{p} \Rightarrow x_0 = \alpha, \quad b_1 = 1 \quad [\because 3\alpha = p + 1]$$

$$3x_1 + 1 \equiv 0 \pmod{p} \Rightarrow x_1 = p - \alpha, \quad b_2 = 2$$

$$3x_2 + 2 \equiv 0 \pmod{p} \Rightarrow x_2 = \alpha - 1, \quad b_3 = 1 \quad \text{and so on.}$$

On the other hand, the relation $\alpha x \equiv e_0 \pmod{p}$ gives,

$$\alpha x_0 \equiv 1 \pmod{p} \Rightarrow x_0 = 3, \quad b_1 = 1$$

$$\alpha x_1 + 1 \equiv 0 \pmod{p} \Rightarrow x_1 = p - 3, \quad b_2 = \alpha - 1$$

$$\alpha x_2 + \alpha - 1 \equiv 0 \pmod{p} \Rightarrow x_2 = 2, \quad b_3 = 1 \quad \text{and so on.}$$

(b) As $3\alpha = 2p + 1$, solving the Diophantine equations given by

$3x \equiv e_0 \pmod{p}$ it is easy to deduce the first part of the result.

The relation $\alpha x \equiv e_0 \pmod{p}$ gives,

$$\alpha x_0 \equiv 1 \pmod{p} \Rightarrow x_0 = 3, \quad b_1 = 2 \quad [\because 3\alpha = 2p + 1]$$

$$\alpha x_1 + 2 \equiv 0 \pmod{p} \Rightarrow x_1 = p - 6, \quad b_2 = \frac{2p - 11}{3}$$

$$\alpha x_2 + \frac{2p - 11}{3} \equiv 0 \pmod{p} \Rightarrow x_2 = 11, \quad b_3 = 8 \quad \text{and so on.}$$

This completes the proof.

**Remark 4.3.6.** Taking $p = 7$ we obtain,

$$I_7(5) = \{3, 1, 11, -17, 47, -89, 191, \ldots\}$$
Now \( 11 \equiv 4 \pmod{7}; -17 + 1 \equiv 5 \pmod{7}; 47 - 3 \equiv 2 \pmod{7}; -89 + 6 \equiv 1 \pmod{7}; 191 - 12 \equiv 4 \pmod{7} \) etc.

\[ \therefore I_7(5) = \{3, R\} \quad \text{where} \quad R = (1, 4, 5, 2). \]

Again taking \( p = 19 \), it can be seen that,

\[ I_{19}(13) = \{3, R\} \quad \text{where} \quad R = (13, 11, 14, 8, 1, 16, 5, 7, 4, 10, 17, 2) \]

This shows that the order of the recurred set is dependent of \( p \).

From Theorem 4.3.7 to Theorem 4.3.12 we have shown that \( I_p(a_k) \) is a recurring \( p \)-adic integer with a \( p \)-independent recurred set whenever

\[ a_k = \sum_{i=0}^{k} \alpha e_i; \alpha = 1, 2, 3, 4. \]

**Theorem 4.3.7.** For \( a_k = \sum_{i=0}^{k} e_i \in \Omega_p, I_p(a_k) \) is a recurring \( p \)-adic integer of degree 1 and of order \( (k + 1) \) i.e. \( I_p(a_k) = \{1, R_k\} \) where \( R_k = ((p - 1)^k, 0) \).

Furthermore the carry-out sequence \( [a_kx \equiv e_0 \pmod{p}] \) is also a recurring one of degree \( (k + 1) \) and of order 1 that is \( [a_kx \equiv e_0 \pmod{p}] = \{0, 0, 1, 2, \ldots, k-1, R_k\} \) where \( R_k' = (k) \)

**Proof:** Taking \( k = 1 \) we obtain \( a_1 = (e_0 + e_1) \). Solving the equations given by the relation \( a_1x \equiv e_0 \pmod{p} \) we get,

\[
\begin{align*}
x_0 & \equiv 1 \pmod{p} \Rightarrow x_0 = 1, \quad b_1 = 0 \\
x_1 + 1 & \equiv 0 \pmod{p} \Rightarrow x_1 = p - 1, \quad b_2 = 1 \\
x_2 + p & \equiv 0 \pmod{p} \Rightarrow x_2 = 0, \quad b_3 = 1 \\
x_3 + 1 & \equiv 0 \pmod{p} \Rightarrow x_3 = p - 1, \quad b_4 = 1
\end{align*}
\]
and so on.

\[ I_p(a_1) = \{1, p - 1, 0, \ldots\} = \{1, R_1\} \quad \text{where} \quad R_1 = (p - 1, 0) \]

Also

\[ [a_1 x \equiv e_0 \pmod{p}] = \{0, 0, R'_1\} \quad \text{where} \quad R'_1 = (1) \]

Taking \( k = 2 \) we obtain \( a_2 = (e_0 + e_1 + e_2) \). Solving the equations given by the relation \( a_2 x \equiv e_0 \pmod{p} \) we get,

\[
\begin{align*}
    x_0 &\equiv 1 \pmod{p} \Rightarrow x_0 = 1, \quad b_1 = 0 \\
    x_1 + 1 &\equiv 0 \pmod{p} \Rightarrow x_1 = p - 1, \quad b_2 = 1 \\
    x_2 + p + 1 &\equiv 0 \pmod{p} \Rightarrow x_2 = p - 1, \quad b_3 = 2 \\
    x_3 + 2p &\equiv 0 \pmod{p} \Rightarrow x_3 = 0, \quad b_4 = 2 \\
    x_4 + p + 1 &\equiv 0 \pmod{p} \Rightarrow x_4 = p - 1, \quad b_5 = 2
\end{align*}
\]

and so on.

\[ I_p(a_2) = \{1, p - 1, p - 1, 0, \ldots\} = \{1, R_2\} \quad \text{where} \quad R_2 = ((p - 1)^2, 0) \]

Also

\[ [a_2 x \equiv e_0 \pmod{p}] = \{0, 0, 1, R'_2\} \quad \text{where} \quad R'_2 = (2) \]

Thus the result holds for \( k = 1 \) and \( k = 2 \).

Assuming the result for \( k \), with the note that the relations \( a_k x \equiv e_0 \pmod{p} \) and \( a_{k+1} x \equiv e_0 \pmod{p} \) produce the same set of equations up-to \((k + 1)^{th}\) step, we can conclude that the solutions of the equations obtained from \( a_{k+1} x \equiv e_0 \pmod{p} \) up-to \((k + 1)^{th}\) step are,

\[
x_0 = 1, x_1 = p - 1, x_2 = p - 1, \ldots, x_k = p - 1 \quad \text{with} \quad b_{k+1} = k.
\]

Hence the equation obtained from \( a_{k+1} x \equiv e_0 \pmod{p} \) in \((k + 2)^{th}\) step is,

\[
\begin{align*}
    x_{k+1} + k(p - 1) + 1 + k &\equiv 0 \pmod{p} \quad \Rightarrow x_{k+1} = p - 1, \quad b_{k+2} = k + 1 \\
    x_{k+2} + (k + 1)(p - 1) + (k + 1) &\equiv 0 \pmod{p} \quad \Rightarrow x_{k+2} = 0, \quad b_{k+3} = k + 1 \\
    x_{k+3} + k(p - 1) + (k + 1) &\equiv 0 \pmod{p} \quad \Rightarrow x_{k+3} = p - 1, \quad b_{k+4} = k + 1
\end{align*}
\]
and so on.

\[ I_p(a_{k+1}) = \{1, R_{k+1}\} \quad \text{where} \quad R_{k+1} = ((p - 1)^{k+1}, 0) \]

and

\[ [a_{k+1}x \equiv e_0 \pmod{p}] = \{0, 0, 1, 2, 3, \ldots, k, R'_{k+1}\} \quad \text{where} \quad R'_{k+1} = (k + 1) \]

The result follows by induction.

**Corollary 4.3.8.** (i) Letting \( k \to \infty \) we can obtain the second part of the Corollary 4.3.2(iii).

(ii) \( I_p(e_0 + 2e_1 + e_2) = \{1, R\} \) where \( |R| = p + 1 \) and \( R = (p - 2, 2, p - 4, 4, p - 6, 6, \ldots, 1, (p - 1)^2, 0) \)

Further more the carry-out sequence \([I_p(e_0 + e_1).I_p(e_0 + e_1)]\) is a functionally recurred one with degree 0 and of order \((p + 1)\).

**Proof:** we have,

\[ I_p(e_0 + 2e_1 + e_2) = I_p(e_0 + e_1).I_p(e_0 + e_1) \]

Suppose that \( I_p(e_0 + e_1) = x, x^2 = z \quad \text{and} \quad [x^2] = b \). It follows from the Theorem 4.3.7 that

\[ x_i = \begin{cases} 1 & \text{if } i = 0 \\ p - 1 & \text{if } i \text{ is odd} \\ 0 & \text{if } i \text{ is even} \end{cases} \]

Thus from Definition 3.2.3

\[ z_i + b_{i+1.p} = \sum_{j+k=i} x_jx_k + b_i \quad \forall i = 0, 1, 2, \ldots \quad \text{with} \quad b_0 = 0. \]

Because of the form of \( x \) we can rewrite the above relation as

\[ z_i + b_{i+1.p} = \begin{cases} 1 & \text{if } i = 0 \\ \frac{i}{2}(p - 1)^2 + b_i & \text{if } i \text{ is even} \\ 2(p - 1) + b_i & \text{if } i \text{ is odd} \end{cases} \quad (4.3.3) \]

Substituting \( i = 0, 1, \ldots, 8 \) in equation (4.3.3) it can be seen that
\[ z_0 = 1 \quad ; \quad b_1 = 0 \]
\[ z_1 = p - 2 \quad ; \quad b_2 = 1 \]
\[ z_2 = 2 \quad ; \quad b_3 = p - 2 \]
\[ z_3 = p - 4 \quad ; \quad b_4 = 2 \]
\[ z_4 = 4 \quad ; \quad b_5 = 2(p - 2) \]
\[ z_5 = p - 6 \quad ; \quad b_6 = 3 \]
\[ z_6 = 6 \quad ; \quad b_7 = 3(p - 2) \]
\[ z_7 = p - 8 \quad ; \quad b_8 = 4 \]
\[ z_8 = 8 \quad ; \quad b_9 = 4(p - 2) \]

From the initial values of \( b_i \) we can have the following expression

\[
 b_i = \begin{cases} 
 \frac{i}{2} & \text{if } i \text{ is even} \\
 \left( \frac{i-1}{2} \right) p - (i-1) & \text{if } i \text{ is odd} 
\end{cases} \quad \text{if } 0 \leq i \leq p
\]

Hence

\[
 b_{p-2} = \left( \frac{p-3}{2} \right) p - (p-3) = \frac{p^2 - 5p + 6}{2}
\]

Substituting \( i = p - 2, p - 1, p, p + 1 \) in equation (4.3.3) we get

\[
 z_{p-2} + b_{p-1}p = 2(p-1) + \frac{p^2 - 5p + 6}{2}
\]

\[
 = \left( \frac{p-1}{2} \right) p + 1
\]

\[
 z_{p-1} + b_pp = \left( \frac{p-1}{2} \right) (p-1)^2 + \frac{p-1}{2}
\]

\[
 = \left( \frac{p^2 - 3p + 2}{2} \right) p + (p-1)
\]

\[
 z_p + b_{p+1}p = 2(p-1) + \frac{p^2 - 3p + 2}{2}
\]

\[
 = \left( \frac{p-1}{2} \right) p + (p-1)
\]

\[
 z_p = p - 1 \quad \text{and} \quad b_{p+1} = \frac{p-1}{2}
\]

\[
 \therefore z_p = p - 1 \quad \text{and} \quad b_{p+1} = \frac{p-1}{2}
\]

\[
 76
\]
\[ z_{p+1} + b_{p+2}p = \left( \frac{p+1}{2} \right) (p-1)^2 + \frac{p-1}{2} \]
\[ = \left( \frac{p-1}{2} \right) p^2 + 0 \]

\[ \therefore z_{p+1} = 0 \quad \text{and} \quad b_{p+2} = \left( \frac{p-1}{2} \right) p \]

Similarly by the substitution \( i = p + 2, p + 3, \ldots, p + 7 \) in equation (4.3.3) we obtain

\[ z_{p+2} = p - 2 \quad ; \quad b_{p+3} = \frac{p+1}{2} \]
\[ z_{p+3} = 2 \quad ; \quad b_{p+4} = \frac{p^2 + p - 4}{2} \]
\[ z_{p+4} = p - 4 \quad ; \quad b_{p+5} = \frac{p+3}{2} \]
\[ z_{p+5} = 4 \quad ; \quad b_{p+6} = \frac{p^2 + 3p - 8}{2} \]
\[ z_{p+6} = p - 6 \quad ; \quad b_{p+7} = \frac{p+5}{2} \]
\[ z_{p+7} = 6 \quad ; \quad b_{p+8} = \frac{p^2 + 5p - 12}{2} \]

From the above initial values of \( b_i^p \) in this section we can write

\[ b_i = \begin{cases} 
  \frac{z - 2}{2} & \text{if} \ i \ \text{is even} \\
  \left( \frac{i - 1}{2} \right) p - (i - 2) & \text{if} \ i \ \text{is odd}
\end{cases} \quad \text{if} \ (p + 1) \leq z \leq (2p + 1) \]

Hence

\[ b_{2p-1} = \left( \frac{2p - 2}{2} \right) p - (2p - 3) = p^2 - 3p + 3 \]

By the substitution of \( i = 2p - 1, 2p, 2p + 1, 2p + 2 \) in equation (4.3.3) we get

\[ z_{2p-1} + b_{2p}p = 2(p - 1) + p^2 - 3p + 3 \]
\[ = (p - 1)p + 1 \]

\[ \therefore z_{2p-1} = 1 \quad \text{and} \quad b_{2p} = p - 1 \]
\[ z_{2p} + b_{2p+1} = p(p-1)^2 + (p-1) \]
\[ = (p-1)^2 + (p-1) \]
\[ \therefore z_{2p} = p - 1 \quad \text{and} \quad b_{2p+1} = (p-1)^2 \]

\[ z_{2p+1} + b_{2p+2} = 2(p-1) + (p-1)^2 \]
\[ = (p-1)p + (p-1) \]
\[ \therefore z_{2p+1} = p - 1 \quad \text{and} \quad b_{2p+2} = p - 1 \]

\[ z_{2p+2} + b_{2p+3} = (p+1)(p-1)^2 + (p-1) \]
\[ = (p-1)p^2 + 0 \]
\[ \therefore z_{2p+2} = 0 \quad \text{and} \quad b_{2p+3} = p(p-1) \]

Similarly by the substitution of \( i = 2p + 3, 2p + 4, \ldots, 2p + 6 \) it can be seen that

\[ z_{2p+3} = p - 2 \quad ; \quad b_{2p+4} = p \]

\[ z_{2p+4} = 2 \quad ; \quad b_{2p+5} = p^2 - 2 \]

\[ z_{2p+5} = p - 4 \quad ; \quad b_{2p+6} = p + 1 \]

\[ z_{2p+6} = 4 \quad ; \quad b_{2p+7} = p^2 + p - 4 \]

The initial values of \( b_i^* \) in this section suggested that

\[ b_i = \begin{cases} 
\frac{i - 4}{2} & \text{if } i \text{ is even} \\
\left(\frac{i - 1}{2}\right)p - (i - 3) & \text{if } i \text{ is odd}
\end{cases} \quad 2(p+1) \leq i \leq (3p+2) \]

Thus the values of \( b_i^* \) for the entire sections are given by

\[ b_i = \begin{cases} 
\frac{i - 2n}{2} & \text{if } i \text{ is even} \\
\left(\frac{i - 1}{2}\right)p - (i - n - 1) & \text{if } i \text{ is odd}
\end{cases} \quad n(p+1) \leq i \leq ((n+1)p + n) \]

Hence \([x^2] = b = \{R_0, R_1, \ldots\} \text{ where}\)

\[ R_0 = \{0, 0, 1, p - 2, \ldots, \frac{p-1}{2}, \frac{p-1}{2} (p-2)\} = \{b_i : 0 \leq i \leq p\} \]

78
For $k \geq 1$ the function $f_k : R_0 \mapsto R_k$ defined by

$$f_k(b_i) = \begin{cases} 
\frac{k(p + 1) + (i - 2k)}{2} & \text{if } i \text{ is even} \\
\left(\frac{k(p + 1) + (i - 1)}{2}\right)(p - (kp + i - 1)) & \text{if } i \text{ is odd}
\end{cases}$$

proves that $[x^2]$ is a functionally recurred one.

**Theorem 4.3.9.** For $a_k = \sum_{i=0}^{k} 2e_i \in \Omega_p$, $I_p(a_k)$ is a recurring one of degree 1 and of order $(k + 1)$, that is,

$$I_p(a_k) = \left\{ \frac{p + 1}{2}, R_k \right\} \text{ where } R_k = \left(\frac{p - 1}{2}, \frac{p - 1}{2}\right)$$

Furthermore $[a_kx \equiv e_0 \pmod{p}]$ is also a recurring one of degree $(k + 1)$ and of order 1, that is,

$$[a_kx \equiv e_0 \pmod{p}] = \{0, 1, 3, 5, \ldots, 2k - 1, R'_k\} \text{ where } R'_k = (2k + 1).$$

**Proof:** For $k = 0$, $a_0 = 2e_0$ and hence for $x = \{x_i\} \in \Omega_p$ we have,

$$a_0x = \{2x_0, 2x_1, 2x_2, \ldots\}$$

Thus the relation $a_0x \equiv e_0 \pmod{p}$ gives,

$$2x_0 \equiv 1 \pmod{p} \Rightarrow x_0 = \frac{p + 1}{2}, \quad b_1 = 1$$

$$2x_1 + 1 \equiv 0 \pmod{p} \Rightarrow x_1 = \frac{p - 1}{2}, \quad b_2 = 1$$

$$2x_2 + 1 \equiv 0 \pmod{p} \Rightarrow x_2 = \frac{p - 1}{2}, \quad b_3 = 1$$

and so on.

$$\therefore I_p(a_0) = \left\{ \frac{p + 1}{2}, R_0 \right\} \text{ where } R_0 = \left(\frac{p - 1}{2}\right)$$

Also,

$$[a_0x \equiv e_0 \pmod{p}] = \{0, R'_0\} \text{ where } R'_0 = (1)$$

79
For \( k = 1 \), \( a_1 = 2e_0 + 2e_1 \) and hence for \( x = \{x_i\} \in \Omega_p \) we have,

\[
a_0 x = \{2x_0, 2x_1 + 2x_0, 2x_2 + 2x_1, \ldots\}
\]

Thus the relation \( a_1 x \equiv e_0 \) (mod \( p \)) gives,

\[
2x_0 \equiv 1 \pmod{p} \Rightarrow x_0 = \frac{p+1}{2} \quad b_1 = 1
\]

\[
2x_1 + p + 2 \equiv 0 \pmod{p} \Rightarrow x_1 = p - 1 \quad b_2 = 3
\]

\[
2x_2 + 2p + 1 \equiv 0 \pmod{p} \Rightarrow x_2 = \frac{p-1}{2} \quad b_3 = 3
\]

and so on.

\[
I_p(a_1) = \left\{ \frac{p+1}{2}, R_1 \right\} \quad \text{where} \quad R_1 = \left( p-1, \frac{p-1}{2} \right)
\]

Also,

\[
[a_1 x \equiv e_0 \pmod{p}] = \left\{ 0, 1, R'_1 \right\} \quad \text{where} \quad R'_1 = (3)
\]

For \( k = 2 \), \( a_2 = 2e_0 + 2e_1 + 2e_2 \) and hence for \( x = \{x_i\} \in \Omega_p \) we have,

\[
a_2 x = \{2x_0, 2x_1 + 2x_0, 2x_2 + 2x_1 + 2x_0, \ldots\}
\]

Thus the relation \( a_2 x \equiv e_0 \) (mod \( p \)) gives,

\[
2x_0 \equiv 1 \pmod{p} \Rightarrow x_0 = \frac{p+1}{2} \quad b_1 = 1
\]

\[
2x_1 + p + 2 \equiv 0 \pmod{p} \Rightarrow x_1 = p - 1 \quad b_2 = 3
\]

\[
2x_2 + 3p + 2 \equiv 0 \pmod{p} \Rightarrow x_2 = p - 1 \quad b_3 = 5
\]

\[
2x_3 + 4p + 1 \equiv 0 \pmod{p} \Rightarrow x_3 = \frac{p-1}{2} \quad b_4 = 5
\]

and so on.

\[
I_p(a_2) = \left\{ \frac{p+1}{2}, R_2 \right\} \quad \text{where} \quad R_2 = \left( (p-1)^2, \frac{p-1}{2} \right)
\]

Also,

\[
[a_2 x \equiv e_0 \pmod{p}] = \left\{ 0, 1, 3, R'_2 \right\} \quad \text{where} \quad R'_2 = (5)
\]

Thus the result holds for \( k = 0, 1, 2 \).

Assuming the result for \( k \), with the note that the relations \( a_k x \equiv e_0 \pmod{p} \) and \( a_{k+1} x \equiv e_0 \pmod{p} \),
(mod p) produce the same set of equations up-to (k + 1)th step, we can conclude that the solutions of the equations obtain from \(a_{k+1}x \equiv e_0 \, (\text{mod } p)\) up-to (k + 1)th step are,

\[
x_0 = \frac{p + 1}{2}, x_1 = p - 1, x_2 = p - 1, \ldots, x_k = p - 1 \quad \text{and} \quad b_{k+1} = 2k + 1
\]

Hence the equation obtained from \(a_{k+1}x \equiv e_0 \, (\text{mod } p)\) in (k + 2)th step is,

\[
2x_{k+1} + 2\left(\frac{p + 1}{2}\right) + 2k(p - 1) + (2k + 1) \equiv 0 \quad (\text{mod } p) \Rightarrow x_{k+1} = p - 1, \quad b_{k+2} = 2k + 3
\]

\[
\therefore \quad 2x_{k+2} + 2(k + 1)(p - 1) + (2k + 3) \equiv 0 \quad (\text{mod } p) \Rightarrow x_{k+2} = \frac{p - 1}{2}, \quad b_{k+3} = 2k + 3
\]

\[
\therefore \quad 2x_{k+3} + 2k(p - 1) + 2\left(\frac{p - 1}{2}\right) + (2k + 3) \equiv 0 \quad (\text{mod } p) \Rightarrow x_{k+3} = p - 1, \quad b_{k+4} = 2k + 3
\]

and so on.

\[
\therefore \quad I_p(a_{k+1}) = \left\{\frac{p + 1}{2}, R_{k+1}\right\} \quad \text{where} \quad R_{k+1} = \left((p - 1)^{k+1}, \frac{p - 1}{2}\right)
\]

and \([a_{k+1}x \equiv e_0 \, (\text{mod } p)] = \{0, 1, 3, 5, \ldots, 2k + 1, R'_{k+1}\}\) where \(R'_{k+1} = (2k + 3)\)

The result follows by induction.

**Corollary 4.3.10.** (i) Letting \(k \to \infty\) we obtain,

\[
I_p(2e) = \left(\frac{p + 1}{2}\right)e_0 + (p - 1)\sum_{i \geq 1} e_i
\]

(ii) \(\frac{p - 1}{2} + I_p(2e) = 0\) and hence

\[
I_p\left(\frac{p - 1}{2}\right) = -2e = (p - 2)e_0 + (p - 3)\sum_{i \geq 1} e_i = \{p - 2, R\} \quad \text{where} \quad R = (p - 3).
\]

(iii) \(I_p(2) + I_p\left(\frac{p - 1}{2}\right) = \left\{\frac{p - 3}{2}, R\right\} \quad \text{where} \quad R = \left(\frac{p - 5}{2}\right).\) In particular, \(2I_0(2) = e_0\)

(iv) \(I_p\left(\frac{p + 1}{2}\right) - I_p\left(\frac{p - 1}{2}\right)\) is a recurring \(p\)-adic integer of degree zero with the recurred set \(R = (4, 0)\).

(v) \(I_p\left(\frac{p - 1}{2}\right) - I_p\left(\frac{p + 1}{2}\right) = \{p - 4, R\} \quad \text{where} \quad R = (p - 1, p - 5).\)
(vi) \( I_p \left( \frac{p+1}{2} \right) + I_p \left( \frac{p-1}{2} \right) \) is not invertible in \( \Omega_p \).

(vii) \( I_p \left( \frac{p^2-1}{4} \right) = \{p-4, R\} \) where \( R = (p-1, p-5) \).

Moreover if \( \left[ I_p \left( \frac{p+1}{2} \right) \right] \left[ I_p \left( \frac{p-1}{2} \right) \right] = b = \{b_i\} \) then

\[
b_i = \begin{cases} 
0 & \text{if } i = 0 \\
\left( \frac{i-1}{2} \right) p - \left( \frac{3i-5}{2} \right) & \text{if } i \text{ is odd} \\
\frac{i}{2} (p-3) & \text{if } i \text{ is even}
\end{cases}
\]

Also \( \left[ I_p \left( \frac{p+1}{2} \right) \right] \left[ I_p \left( \frac{p-1}{2} \right) \right] = b = \{b_i\} \) is functionally recurred one of degree 2 and of order 2.

**Proof:** Clearly \( I_p \left( \frac{p^2-1}{4} \right) = I_p \left( \frac{p+1}{2} \right) I_p \left( \frac{p-1}{2} \right) \).

Suppose that \( x = I_p \left( \frac{p+1}{2} \right) = \{2, R\} \) where \( R = (p-2, 1) \)

and \( y = I_p \left( \frac{p-1}{2} \right) = \{p-2, R\} \) where \( R = (p-3) \)

It follows that

\[
x_i = \begin{cases} 
2 & \text{if } i = 0 \\
p - 2 & \text{if } i \text{ is odd} \\
1 & \text{if } i \text{ is even}
\end{cases}
\]

and

\[
y_0 = p - 2, y_i = p - 3 \forall i \geq 1
\]

If we take \( xy = z \) and \([xy] = b\) then

\[
z_i + b_{i+1}p = \sum_{j+k=i} x_j y_k + b_i \quad \forall i = 0, 1, 2, \ldots \tag{4.3.4}
\]

i.e. \( z_i + b_{i+1}p = (p-3) \sum_{j=0}^{i-1} x_j + (p-2)x_i + b_i \quad \forall i = 0, 1, 2, \ldots \tag{4.3.5} \)

In equation (4.3.5) by the substitution \( i = 0 \) we obtain

\[
z_0 + b_1p = 2(p-2) + 0 = 1.p + (p-4)
\]
It follows that $z_0 = p - 4$ and $b_1 = 1$.

Similarly in equation (4.3.5) by the substitution $i = 1, 2, 3, 4, 5, 6$, it can be easily seen that

\[
\begin{align*}
  z_1 &= p - 1 \quad ; \quad b_2 = p - 3 \\
  z_2 &= p - 5 \quad ; \quad b_3 = p - 2 \\
  z_3 &= p - 1 \quad ; \quad b_4 = 2(p - 3) \\
  z_4 &= p - 5 \quad ; \quad b_5 = 2p - 5 \\
  z_5 &= p - 1 \quad ; \quad b_6 = 3(p - 3) \\
  z_6 &= p - 5 \quad ; \quad b_7 = 3p - 8
\end{align*}
\]

Thus the result holds for $i = 0, 1, \ldots, 6$.

Preliminary enquiry suggested that

\[
b_i = \begin{cases} 
  0 & \text{if } i = 0 \\
  \left(\frac{i - 1}{2}\right)p - \left(\frac{3i - 5}{2}\right) & \text{if } i \text{ is odd} \\
  \frac{i}{2}(p - 3) & \text{if } i \text{ is even}
\end{cases}
\]

We now follow the induction on $i$. Assuming the result for $i = m$, we consider the following two cases:

**Case I**: Suppose that $m$ is odd. Then

\[
z_m = p - 1 \quad \text{and} \quad b_{m+1} = \left(\frac{m + 1}{2}\right)(p - 3).
\]

In equation (4.3.5) by the substitution $i = m + 1$ we obtain
$z_{m+1} + b_{m+2} = (p-3) \sum_{j=0}^{m} x_j + (p-2)x_{m+1} + b_{m+1}$

$= (p-3) \left[ 2 + \sum_{j=1}^{m} x_j \right] + (p-2)(p-1) + \left( \frac{m+1}{2} \right)(p-3)$

$= (p-3) \left[ 2 + \left( \frac{m-1}{2} \right)(p-1) + (p-2) \right] + (p-2) + \left( \frac{m+1}{2} \right)(p-3)$

$= \left( \frac{m+1}{2} \right)p^2 + \left( \frac{1-3m}{2} \right)p - 5$

$= \left\{ \left( \frac{m+1}{2} \right)p - \left( \frac{3m+1}{2} \right) \right\}p + (p-5)$

$\therefore z_{m+1} = p - 5$ and $b_{m+2} = \left\{ \left( \frac{m+1}{2} \right)p - \left( \frac{3m+1}{2} \right) \right\}$

**Case II:** Suppose that $m$ is even. So,

$z_m = p - 5$ and $b_{m+1} = \left( \frac{m}{2} \right)p - \left( \frac{3m-2}{2} \right)$.

In equation (4.3.5) by the substitution $i = m+1$ we obtain,

$z_{m+1} + b_{m+2} = (p-3) \sum_{j=0}^{m} x_j + (p-2)x_{m+1} + b_{m+1}$

$= (p-3) \left[ 2 + \sum_{j=1}^{m} x_j \right] + (p-2)(p-1) + \frac{m}{2}p - \left( \frac{3m-2}{2} \right)$

$= (p-3)\left[ 2 + \frac{m}{2}(p-1) \right] + (p^2 - 4p + 4) + \frac{m}{2}p - \left( \frac{3m-2}{2} \right)$

$= \left( \frac{m+2}{2} \right)p^2 + \left( \frac{m}{2} - 2m - 2 \right)p - 1$

$= \left\{ \left( \frac{m+2}{2} \right)p - \left( \frac{3m+6}{2} \right) \right\}p + (p-1)$

$= \left( \frac{m+2}{2} \right)(p-3)p + (p-1)$

$\therefore z_{m+1} = p - 1$ and $b_{m+2} = \left( \frac{m+2}{2} \right)(p-3)$.
Thus the result follows by induction.

We now consider the function \( f_k : R_0 \rightarrow R_k \) defined by

\[
\begin{align*}
f_k(b_i) &= \begin{cases} 
(k + 1)b_i & \text{if } i = 2 \\
(k + 1)b_i - k & \text{if } i = 3
\end{cases}
\end{align*}
\]

where \( R_0 = (b_2, b_3) = (p - 3, p - 2) \)

\[
\therefore \left[ I_p \left( \frac{p + 1}{2} \right) \right] I_p \left( \frac{p - 1}{2} \right) = (0, 1, R_0) ; f_k
\]

**Theorem 4.3.11.** For the rational integer

\[
a_k = \sum_{i=0}^{k} 3c_i \in \Omega_p
\]

\( I_p(a_k) \) is a recurring \( p \)-adic integer of degree 1.

Let \( I_p(a_k) = \{ x_0, R_k \} \).

**Case I:** If \( 3 \mid (p + 1) \) then \( x_0 = \frac{p + 1}{3} \) and \( |R_k| = 3(k + 1) \) or \( 2(k + 1) \) according as \( k \) is odd or even respectively.

(i) In case \( k \) is odd we write \( R_k = (x_1, x_2, \ldots, x_{k+1}, x_{k+2}, \ldots, x_{2k+2}, x_{2k+3}, \ldots, x_{3k+3}) \)

i.e. we divide \( R_k \) into three segments of equal lengths.

In the 1st segment, elements occupying odd positions are \( \frac{p - 2}{3} \) except the last one i.e. \( x_{k+1} \) which is always 0.

In the 2nd segment, all the elements occupying odd positions are \( \frac{2p - 1}{3} \), while all the elements occupying even positions are \( \frac{2p - 1}{3} \) except \( x_{2k+2} \) which is always 0.

In the 3rd segment, the last element is \( \frac{p - 2}{3} \) and all other elements in this segment are \( p - 1 \).

(ii) In case \( k \) is even we write \( R_k = (x_1, x_2, \ldots, x_{k+1}, x_{k+2}, \ldots, x_{2k+2}) \)

In the 1st segment, elements occupying odd positions are \( \frac{p - 2}{3} \) except the last one i.e. \( x_{k+1} \)
which is equal to \(\frac{2p - 1}{3}\), while all the elements occupying even positions are \(\frac{2p - 1}{3}\).

In the 2\textsuperscript{nd} segment, the last element is \(\frac{p - 2}{3}\) and all other elements are \(p - 1\).

**Case II:** If \(3 \mid (2p + 1)\) then \(x_0 = \frac{2p + 1}{3}\) and \(|R_k| = (k + 1)\) and it is given by,

\[
R_k = \left(\frac{(p - 1)^k}{3}, \frac{2(p - 1)}{3}\right)
\]

Moreover,

\[ [a_k x \equiv e_0 \pmod{p}] = \{0, 2, 5, 8, 11, \ldots, 3k - 1, R'_k\} \quad \text{where} \quad R'_k = (3k + 2) \]

**Proof:** We know that either \(3 \mid (p+1)\) or \(3 \mid (2p+1)\). This motivates us to consider these two cases separately during the process of evaluation of the Diophantine equations evolving from the relation \(a_0 x \equiv e_0 \pmod{p}\).

For \(k = 0, a_0 = 3e_0\) and hence for \(x = \{x_i\} \in \Omega_p\)

\[ a_0 x = \{3x_0, 3x_1, 3x_2, \ldots\} \]

**Case I:** Suppose that \((p + 1)\) is divisible by 3 i.e. \(p + 1 = 3m\) for some \(m \in \mathbb{Z}\).

Now,

\[
3x_0 \equiv 1 \pmod{p} \Rightarrow x_0 = \frac{p + 1}{3} \quad b_1 = 1
\]

\[
3x_1 + 1 \equiv 0 \pmod{p} \Rightarrow x_1 = \frac{2p - 1}{3} \quad b_2 = 2[:: 2p - 1 = 3(2m - 1)]
\]

\[
3x_2 + 2 \equiv 0 \pmod{p} \Rightarrow x_2 = \frac{p - 2}{3} \quad b_3 = 1[:: p - 2 = 3(m - 1)]
\]

and so on.

\[ \vdots \]

\[
J_p(a_0) = \left\{\frac{p + 1}{3}, R_0\right\} \quad \text{where} \quad R_0 = \left(\frac{2p - 1}{3}, \frac{p - 2}{3}\right)
\]

and \([a_0 x \equiv e_0 \pmod{p}] = \{0, R'_0\} \quad \text{where} \quad R'_0 = (1, 2)\]

**Case II:** Suppose that \((2p + 1)\) is divisible by 3 i.e. \(2p + 1 = 3m\) for some \(m \in \mathbb{Z}\).

Now,
\[3x_0 \equiv 1 \pmod{p} \Rightarrow x_0 = \frac{2p + 1}{3} \quad b_1 = 2\]

\[3x_1 + 2 \equiv 0 \pmod{p} \Rightarrow x_1 = \frac{2(p - 1)}{3} \quad b_2 = 2[\because 2(p - 1) = 3(m - 1)]\]

and so on.

\[\therefore I_p(a_0) = \left\{ \frac{2p + 1}{3}, R_0 \right\} \quad \text{where} \quad R_0 = \left( \frac{2(p - 1)}{3} \right)\]

and \([a_0 x \equiv e_0 \pmod{p}] = \left\{ 0, R'_0 \right\} \quad \text{where} \quad R'_0 = (2)\]

For \(k = 1, a_1 = 3e_0 + 3e_1\) and hence for \(x = \{x_i\} \in \Omega_p\)

\[a_1 x = \{3x_0, 3x_1 + 3x_0, 3x_2 + 3x_1, \ldots\}\]

**Case I:** Suppose that \((p + 1)\) is divisible by 3 i.e. \(p + 1 = 3m\) for some \(m \in \mathbb{Z}\).

Now,

\[3x_0 \equiv 1 \pmod{p} \Rightarrow x_0 = \frac{p + 1}{3} \quad b_1 = 1\]

\[3x_1 + p + 2 \equiv 0 \pmod{p} \Rightarrow x_1 = \frac{p - 2}{3} \quad b_2 = 2[\because p - 2 = 3(m - 1)]\]

\[3x_2 + p \equiv 0 \pmod{p} \Rightarrow x_2 = 0 \quad b_3 = 1\]

\[3x_3 + 1 \equiv 0 \pmod{p} \Rightarrow x_3 = \frac{2p - 1}{3} \quad b_4 = 2\]

\[3x_4 + 2p + 1 \equiv 0 \pmod{p} \Rightarrow x_4 = \frac{2p - 1}{3} \quad b_5 = 4\]

\[3x_5 + 2p + 3 \equiv 0 \pmod{p} \Rightarrow x_5 = p - 1 \quad b_6 = 5\]

and so on.

\[\therefore I_p(a_1) = \left\{ \frac{p + 1}{3}, R_1 \right\} \quad \text{where} \quad R_1 = \left( \frac{p - 2}{3}, 0, \left( \frac{2p - 1}{3} \right)^2, (p - 1), \frac{p - 2}{3} \right)\]

Let us assume that the result holds for \(k\). We now consider the following two cases:

(a) Let \(k\) be odd.

As we know the relations \(a_{k+1}x \equiv e_0 \pmod{p}\) and \(a_kx \equiv e_0 \pmod{p}\) generate the same
set of equations up-to \((k + 1)th\) step, the solutions of the equations obtained from \(a_{k+1}x \equiv e_0 \pmod{p}\) up-to \((k + 1)th\) steps are given by,

\[
x_0 = \frac{p + 1}{3}, x_1 = \frac{p - 2}{3}, x_2 = \frac{2p - 1}{3}, \ldots, x_k = \frac{p - 2}{3}
\]

with \(b_{k+1} = \frac{3k + 1}{2}\). 

Therefore the equation obtained from $a_{k+1}x \equiv e_0 \pmod{p}$ in $(k + 2)^{th}$ step is given by,

$$3x_{k+1} + 3\left(\frac{k + 1}{2}\right)\left(\frac{p - 2}{3}\right) + 3\left(\frac{k - 1}{2}\right)\left(\frac{2p - 1}{3}\right) + 3\left(\frac{p + 1}{3}\right) + \left(\frac{3k + 1}{2}\right) \equiv 0 \pmod{p}.$$ 

that is $3x_{k+1} + \left(\frac{3k + 1}{2}\right)p + 1 \equiv 0 \pmod{p}$.

$$\therefore x_{k+1} = \frac{2p - 1}{3}, \ b_{k+2} = \frac{3k + 5}{2}$$

Next,

$$3x_{k+2} + 3\left(\frac{k + 1}{2}\right)\left(\frac{p - 2}{3}\right) + \left(\frac{2p - 1}{3}\right) + \left(\frac{3k + 5}{2}\right) \equiv 0 \pmod{p}$$

that is, $3x_{k+2} + \left(\frac{3(k + 1)}{2}\right)p + 1 \equiv 0 \pmod{p}$.

$$\therefore x_{k+2} = \frac{2p - 1}{3}, \ b_{k+3} = \frac{3k + 7}{2}.$$ 

Continuing this process we can see that,

$$x_{k+3} = p - 1, \ b_{k+4} = \frac{3k + 11}{2}$$

$$x_{k+4} = p - 1, \ b_{k+5} = \frac{3k + 13}{2}$$

$$\ldots \ldots \ldots$$

$$x_{2k+3} = p - 1, \ b_{2k+4} = 3k + 5$$

$$x_{2k+4} = \frac{p - 2}{3}, \ b_{2k+5} = 3k + 4$$

and so on.

Hence,

$$I_p(a_{k+1}) = \left\{ \frac{p + 1}{3}, R_{k+1} \right\} \quad \text{where} \quad |R_{k+1}| = 2(k + 2)$$

and $R_{k+1} = \left( \begin{array}{c} p - 2 \end{array} \begin{array}{c} 2p - 1 \end{array} \begin{array}{c} 2p - 1 \end{array} \begin{array}{c} \cdots \end{array} \begin{array}{c} (p - 1)^{k+1} \end{array} \begin{array}{c} p - 2 \end{array} \begin{array}{c} 3 \end{array} \begin{array}{c} 3 \end{array} \begin{array}{c} 3 \end{array} \begin{array}{c} (k+2)\text{times} \end{array} \begin{array}{c} (k+2)\text{times} \end{array} \right)$
Thus the result holds for \((k + 1)\).

(b) Let \(k\) be even.

The solutions of the equations obtained from \(a_{k+1}x \equiv e_0 \pmod{p}\) up-to \((k + 1)\)th steps are given by,

\[
\begin{align*}
x_0 &= \frac{p+1}{3},
x_1 &= \frac{p-2}{3},
x_2 &= \frac{2p-1}{3}, 
\ldots ,
x_k &= \frac{2p-1}{3},
\end{align*}
\]

with \(b_{k+1} = \frac{3k+2}{2}\).

Thus the equation obtained from \(a_{k+1}x \equiv e_0 \pmod{p}\) in \((k + 2)\)th step is given by,

\[
3x_{k+1} + 3\left(\frac{k}{2}\right)\left(\frac{p-2}{3} + \frac{2p-1}{3}\right) + 3\left(\frac{p+1}{3}\right) + \left(\frac{3k+2}{2}\right) \equiv 0 \pmod{p}.
\]

that is \(3x_{k+1} + \left(\frac{3k+2}{2}\right) p + 2 \equiv 0 \pmod{p}\).

\[
\therefore x_{k+1} = \frac{p-2}{3}, \quad b_{k+2} = \frac{3k+4}{2}.
\]

Next, \(3x_{k+2} + 3\left(\frac{k}{2} + 1\right)\left(\frac{p-2}{3}\right) + 3\frac{k}{2}\left(\frac{2p-1}{3}\right) + \left(\frac{3k+4}{2}\right) \equiv 0 \pmod{p}.
\]

that is \(3x_{k+2} + \left(\frac{3k+2}{2}\right) p \equiv 0 \pmod{p},\)

\[
\therefore x_{k+2} = 0, \quad b_{k+3} = \frac{3k+2}{2}.
\]

Continuing this process it can be seen that,
\[ x_{k+3} = \frac{2p - 1}{3}, \quad b_{k+4} = \frac{3k + 4}{2} \]

\[ x_{k+4} = \frac{p - 2}{3}, \quad b_{k+5} = \frac{3k + 2}{2} \]

\[ x_{k+5} = \frac{2p - 1}{3}, \quad b_{k+6} = \frac{3k + 4}{2} \]

\[ \ldots \ldots \ldots \ldots \ldots \]

\[ \ldots \ldots \ldots \ldots \ldots \]

\[ x_{2k+3} = \frac{2p - 1}{3}, \quad b_{2k+4} = \frac{3k + 4}{2} \]

Now

\[ 3x_{2k+4} + 3 \cdot \frac{k}{2} \left( \frac{p - 2}{3} \right) + 3 \left( \frac{k}{2} + 1 \right) \left( \frac{2p - 1}{3} \right) + \left( \frac{3k + 4}{2} \right) \equiv 0 \pmod{p}. \]

that is, \( 3x_{2k+4} + \left( \frac{3k + 4}{2} \right) p + 1 \equiv 0 \pmod{p} \).

\[ \because x_{2k+4} = \frac{2p - 1}{3}, \quad b_{2k+5} = \frac{3k + 8}{2}. \]

Next,

\[ 3x_{2k+5} + 3 \cdot \frac{k}{2} \left( \frac{p - 2}{3} \right) + 3 \left( \frac{k}{2} + 1 \right) \left( \frac{2p - 1}{3} \right) + \left( \frac{3k + 8}{2} \right) \equiv 0 \pmod{p}. \]

that is, \( 3x_{2k+5} + \left( \frac{3k + 4}{2} \right) p + 3 \equiv 0 \pmod{p} \).

\[ \therefore x_{2k+5} = p - 1, \quad b_{2k+6} = \frac{3k + 10}{2}. \]

Continuing this process it can be seen that,

\[ x_{2k+6} = p - 1, \quad b_{2k+7} = \frac{3k + 14}{2} \]

\[ \ldots \ldots \ldots \ldots \ldots \]

\[ \ldots \ldots \ldots \ldots \ldots \]

\[ x_{2k+4} = p - 1, \quad b_{3k+5} = \frac{6k + 8}{2} \]

\[ x_{3k+5} = p - 1, \quad b_{3k+6} = 3k + 5 \]

91
Next,

\[ 3x_{3k+6} + 3(k + 1)(p - 1) + (3k + 5) \equiv 0 \pmod{p} \]

that is, \( 3x_{3k+6} + 3(k + 1)p + 2 \equiv 0 \pmod{p} \)

\[ \therefore x_{3k+6} = \frac{p-2}{3}, \quad b_{3k+7} = 3k + 4 \]

and so on.

Hence the result holds for \((k + 1)\).

Thus the result follows by induction.

\textbf{Case II:} Let \(3 \mid (2p + 1)\).

It can be seen that the result holds for \(k = 1\) and \(k = 2\).

Let the result holds for \(k\).

The solutions of the equations obtained from \(a_{k+1}x \equiv e_0 \pmod{p}\) up-to \((k + 1)^{th}\) steps are given by,

\[ x_0 = \frac{2p+1}{3}, \quad x_1 = p - 1, \quad x_2 = p - 1, \ldots, x_k = p - 1 \text{ with } \]

\[ b_{k+1} = 3k + 2. \]

Now,

\[ 3x_{k+1} + 3 \left( \frac{2p+1}{3} \right) + 3k(p - 1) + (3k + 2) \equiv 0 \pmod{p} \]

that is, \(3x_{k+1} + (3k + 2)p + 3 \equiv 0 \pmod{p}\)

\[ \therefore x_{k+1} = p - 1, \quad b_{k+2} = 3k + 5 \]

Also,

\[ 3x_{k+2} + 3(k+1)(p - 1) + (3k + 5) \equiv 0 \pmod{p}. \]
that is, \(3x_{k+2} + (3k + 1)p + 2 \equiv 0 \pmod{p}\).

\[x_{k+2} = \frac{2(p-1)}{3}, \quad b_{k+3} = 3k + 5.\]

and so on.

\(I_p(a_{k+1}) = \left\{ \frac{2p+1}{3}, R_{k+1} \right\}\) where \(R_{k+1} = \left( (p-1)^{k+1}, \frac{2(p-1)}{3} \right)\)

and \([a_{k+1}x \equiv e_0 \pmod{p}] = \{0, 2, 5, 8, \ldots, 3k + 2, R'_{k+1} \}\) where \(R'_{k+1} = (3k + 5)\).

The result follows by induction.

**Theorem 4.3.12.** For the rational integer \(a_k = \sum_{i=0}^{k} 4e_i \in \Omega_p; I_p(a_k)\) is a recurring \(p\)-adic integer of degree 1 with the recurred se \(R_k\) and it is given by,

\[(a) \quad I_p(a_k) = \left\{ \frac{p+1}{4}, R_k \right\}\) where \(R_k = \left( \left( \frac{p-1}{2} \right)^k, 3p-1, \frac{3(p-1)}{4}, \frac{p-3}{4} \right)\), provided \(4 \mid (p+1)\).

\[(b) \quad I_p(a_k) = \left\{ \frac{3p+1}{4}, R_k \right\}\) where \(R_k = \left( (p-1)^k, \frac{3(p-1)}{4} \right)\), provided \(4 \mid (p-1)\).

**Proof:** (a) Let \(4 \mid (p+1)\).

It can be easily seen that the result holds for \(k = 1\) and \(k = 2\). Let us assume that the result holds for \(k\). The solutions of the equations obtained from \(a_{k+1}x \equiv e_0 \pmod{p}\) up-to \((k+1)\)th steps are,

\[x_0 = \frac{p+1}{4}, x_1 = \frac{p-1}{2}, x_2 = \frac{p-1}{2}, \ldots, x_k = \frac{p-1}{2}\]

with \(b_{k+1} = 2k + 1\).

Now,

\[4x_{k+1} + (p+1) + 2k(p-1) + (2k+1) \equiv 0 \pmod{p}\]

93
i.e. \( 4x_{k+1} + (2k + 1)p + 2 \equiv 0 \pmod{p} \)

\[
\therefore x_{k+1} = \frac{p - 1}{2}, \quad b_{k+2} = 2k + 3.
\]

Next,

\[4x_{k+2} + 2(k + 1)(p - 1) + (2k + 3) \equiv 0 \pmod{p}\]

i.e. \( 4x_{k+2} + 2(k + 1)p + 1 \equiv 0 \pmod{p} \)

\[
\therefore x_{k+2} = \frac{3p - 1}{4}, \quad b_{k+3} = 2k + 5.
\]

Again,

\[4x_{k+3} + 2k(p - 1) + (3p - 1) + (2k + 5) \equiv 0 \pmod{p}\]

i.e. \( 4x_{k+3} + (2k + 3)p + 4 \equiv 0 \pmod{p} \)

\[
\therefore x_{k+3} = p - 1, \quad b_{k+4} = 2k + 7.
\]

Continuing this process it can be seen that,

\[
x_{k+4} = p - 1, \quad b_{k+5} = 2k + 9
\]

\[
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\]

\[
x_{2k+3} = p - 1, \quad b_{2k+4} = 4k + 7
\]

Lastly,

\[4x_{2k+4} + 4(k + 1)(p - 1) + (4k + 7) \equiv 0 \pmod{p}\]

\[
\therefore x_{2k+4} = \frac{p - 3}{4}, \quad b_{2k+5} = 4k + 5 \quad \text{and so on.}
\]

Thus the result follows by induction.
(b) Let $4 \mid (p - 1)$
It is easy to see that the result holds for $k = 1$ and $k = 2$. Assuming the result for $k$, the solutions of the equations obtained from $a_{k+1}x \equiv c_0 \pmod{p}$ up-to $(k+1)^{th}$ steps are given by,

$$x_0 = \frac{3p + 1}{4}, x_1 = p - 1, x_2 = p - 1, \ldots, x_k = p - 1$$

with $b_{k+1} = 4k + 3$.

Now,

$$4x_{k+1} + (3p + 1) + 4k(p - 1) + (4k + 3) \equiv 0 \pmod{p}$$

i.e. $4x_{k+1} + (4k + 3)p + 4 \equiv 0 \pmod{p}$

$\therefore x_{k+1} = p - 1, b_{k+2} = 4k + 7$.

Next,

$$4x_{k+2} + 4(k + 1)(p - 1) + (4k + 7) \equiv 0 \pmod{p}$$

i.e. $4x_{k+2} + 4(k + 1)p + 3 \equiv 0 \pmod{p}$

$\therefore x_{k+2} = \frac{3(p - 1)}{4}, b_{k+3} = 4k + 8$ and so on.

This shows that the result holds for $k + 1$.

The result follows by induction.

**Theorem 4.3.13.** If $\alpha, \beta \in B_0 = \{1, 2, 3, \ldots, p - 1\}$ such that $\alpha \beta = p - 1$ then

- (a) $I_p(\alpha) = \{p - \beta, R\}$ where $R = (p - \beta - 1)$

and $[\alpha x \equiv c_0 \pmod{p}] = \{0, R'\}$ where $R' = (\alpha - 1)$

- (b) $I_p(\beta) = \{p - \alpha, R\}$ where $R = (p - \alpha - 1)$
and \( \beta x \equiv e_0 \pmod{p} \) = \( \{0, R'\} \) where \( R' = (\beta - 1) \)

**Proof:** The relation \( \alpha x \equiv e_0 \pmod{p} \) gives us,

\[
\alpha x_0 \equiv 1 \pmod{p} \Rightarrow x_0 = p - \beta, b_1 = \alpha - 1
\]

\[
\alpha x_1 + \alpha - 1 \equiv 0 \pmod{p} \Rightarrow x_1 = p - \beta - 1, b_2 = \alpha - 1 \text{ and so on.}
\]

This proves (a).

Interchanging the roles of \( \alpha \) and \( \beta \) we get (b).

**Theorem 4.3.14.** (Generalization of Theorem 4.3.1(b) and Theorem 4.3.5(a))

If \( \alpha, \beta \) be two rational integers such that \( \alpha \beta = p + 1 \) then,

\[
I_p(\alpha) = \{\beta, R\} \text{ where } R = (p - \beta, \beta - 1)
\]

and \( I_p(\beta) = \{\alpha, R\} \) where \( R = (p - \alpha, \alpha - 1) \).

**Corollary 4.3.15.** If \( p, q_1, q_2, q_3 \) are all distinct primes and \( \alpha_1, \alpha_2, \alpha_3 \) are composites such that

\[
q_1\alpha_1 = q_2\alpha_2 = q_3\alpha_3 = p + 1
\]

then for \( j \neq k \), \( I_p(\alpha_j\alpha_k) \) is a recurring \( p \)-adic integer with a recurred set independent of \( p \).

**Proof:** Using some preliminary results of number theory it can be seen that,

\[
\alpha_j\alpha_k = \beta e_0 + \beta e_1 \text{ where } \beta = \gcd(\alpha_j, \alpha_k)
\]

By Theorems[ 4.3.7- 4.3.12] \( I_p(\alpha_j\alpha_k) \) is a recurring \( p \)-adic integer with a recurred set independent of \( p \).
Corollary 4.3.16. (a) If \( p, q_1, q_2, q_3 \) are all distinct primes such that \( q_1 \alpha_1 = q_2 \alpha_2 = q_3 \alpha_3 = p + 1 \) then \( I_p(\alpha_1 \alpha_2 \alpha_3) \) is a recurring \( p \)-adic integer with a recurred set independent of \( p \).

(b) If for a prime \( p \), \( 2\alpha = p + 1 \) and \( \alpha \) is even then \( I_p(\alpha^2) \) is a recurring \( p \)-adic integer with a recurred set independent of \( p \).

Remark 4.3.17. Let us conclude this chapter with the observation that the sum of the degree of \( I_p(a) \) and the order of the recurred set \( R \) of \( I_p(a) \) is always equal to the sum of the degree of \( [ax \equiv e_0 \pmod{p}] \) and the order of the recurred set \( R' \) of \( [ax \equiv e_0 \pmod{p}] \) in each result incorporated in this chapter.

Moreover, we are left the most important question "Can we prove that for
\[
\alpha_k = \sum_{i=0}^{k} \alpha \varepsilon_i, \forall \alpha \in B = \{1, 2, 3, \ldots, p - 1\}, I_p(\alpha_k) \text{ a recurring } p \text{-adic integer with a } p-\text{independent recurred set } R?"

We are trying to deal with the problem stated above as follows: Let us consider \( x, y \in \Omega_p(p \geq 7) \) such that \( x - y = e_0 \). It follows that \( I_p(xy) = I_p(y) - I_p(x) \). This simple technique can be employed to evaluate the inverse of \( \alpha = \{\alpha, R\} \) where \( R = (0) \) with a composite value of \( \alpha \in B = \{1, 2, \ldots, p - 1\} \).

For instance if we choose \( x = \{3, R\} \) and \( y = \{2, R\} \) with \( R = (0) \) then
\[
x - y = x + \psi(y) = \{3, R\} + \{p - 2, R'\} \text{ where } R' = (p - 1) = \{1, R\} = e_0
\]
\[
\therefore I_p(xy) = I_p(y) - I_p(x) = I_p(y) + \psi(I_p(x))
\]
By Theorem 3.3.2(a) \( I_p(y) = \left\{ \frac{p + 1}{2}, R_1 \right\} \) where \( R_1 = \left(\frac{p - 1}{2}\right) \).

By Theorem 4.3.5(a) \( I_p(x) = \left\{ \frac{p + 1}{3}, R_2 \right\} \) where \( R_2 = \left(\frac{2p - 1}{3}, \frac{p - 2}{3}\right) \) or \( \left\{ \frac{2p + 1}{3}, R_3 \right\} \).
where $R_3 = \left(\frac{2(p-1)}{3}\right)$ according as $3 \mid p + 1$ or $3 \mid 2p + 1$ respectively.

In case $3 \mid p + 1$, by the Definition 2.2.7 we get,

$$
\psi(I_p(x)) = \left\{ \frac{2p-1}{3}, R_4 \right\}
\quad \text{where} \quad R_4 = \left(\frac{p-2}{3}, \frac{2p-1}{3}\right)
$$

$$
\therefore I_p(xy) = \left\{ \frac{p+1}{6}, R_5 \right\}
\quad \text{where} \quad R_5 = \left(\frac{5p-1}{6}, \frac{p-5}{6}\right)
$$

Here

$$
[I_p(y) - I_p(x)] = \{0, R'\} \quad \text{where} \quad R' = (1, 0)
$$

In case $3 \mid 2p + 1$, by the Definition 2.2.7 we get,

$$
\psi(I_p(x)) = \left\{ \frac{p-1}{3}, R_6 \right\}
\quad \text{where} \quad R_6 = \left(\frac{p-1}{3}\right)
$$

$$
\therefore I_p(xy) = \left\{ \frac{5p+1}{6}, R_7 \right\}
\quad \text{where} \quad R_7 = \left(\frac{5p-5}{6}\right)
$$

Here

$$
[I_p(y) - I_p(x)] = 0
$$

Thus it enable us to solve the problem for $\alpha = 6$ and $k = 0$.

In the same way if we choose $x, y \in \Omega_p (p \geq 13)$ such that $x = \{4, R\}$ and $y = \{3, R\}$ with $R = (0)$ then clearly $x - y = e_0$ and therefore

$$
I_p(xy) = I_p(y) - I_p(x) = I_p(y) + \psi(I_p(x))
$$

By Theorem 4.3.5(a) $I_p(y) = \left\{ \frac{p+1}{4}, R_1 \right\}$ where $R_1 = \left(\frac{2p-1}{3}, \frac{p-2}{3}\right)$ or $\left\{ \frac{2p+1}{3}, R_2 \right\}$

where $R_2 = \left(\frac{2(p-1)}{3}\right)$ according as $3 \mid p + 1$ or $3 \mid 2p + 1$ respectively.

By Theorem 4.3.12 $I_p(x) = \left\{ \frac{p+1}{4}, R_3 \right\}$ where $R_3 = \left(\frac{3p-1}{4}, \frac{p-3}{4}\right)$ or $\left\{ \frac{3p+1}{4}, R_4 \right\}$

where $R_4 = \left(\frac{3(p-1)}{4}\right)$ according as $4 \mid p + 1$ or $4 \mid p - 1$ respectively.

From the Definition 2.2.7 we have

$$
\psi(I_p(x)) = \left\{ \frac{3p-1}{4}, R_5 \right\}
\quad \text{where} \quad R_5 = \left(\frac{p-3}{4}, \frac{3p-1}{4}\right)
\quad \text{or} \quad \left\{ \frac{p-1}{4}, R_6 \right\}
$$
where \( R_6 = \left( \frac{p - 1}{4} \right) \) according as \( 4 \mid p + 1 \) or \( 4 \mid p - 1 \) respectively.
We now consider the following cases:

**Case I:** Suppose that $3 \mid (2p + 1)$ and $4 \mid (p - 1)$. Then

$$I_p(xy) = I_p(y) - I_p(x) = I_p(y) + \psi(I_p(x))$$

$$= \left\{ \frac{2p+1}{3}, R_2 \right\} + \left\{ \frac{p-1}{4}, R_6 \right\}$$

$$= \left\{ \frac{11p+1}{12}, R_7 \right\} \text{ where } R_7 = \left( \frac{11(p-1)}{12} \right)$$

**Case II:** Suppose that $3 \mid (2p + 1)$ and $4 \mid (p + 1)$. Then

$$I_p(xy) = I_p(y) - I_p(x) = I_p(y) + \psi(I_p(x))$$

$$= \left\{ \frac{2p+1}{3}, R_2 \right\} + \left\{ \frac{3p-1}{4}, R_5 \right\}$$

$$= \left\{ \frac{5p+1}{12}, R_8 \right\} \text{ where } R_8 = \left( \frac{11p-5}{12}, \frac{5p-11}{12} \right)$$

**Case III:** Suppose that $3 \mid (p + 1)$ and $4 \mid (p - 1)$. Then

$$I_p(xy) = I_p(y) - I_p(x) = I_p(y) + \psi(I_p(x))$$

$$= \left\{ \frac{p+1}{3}, R_1 \right\} + \left\{ \frac{p-1}{4}, R_6 \right\}$$

$$= \left\{ \frac{7p+1}{12}, R_9 \right\} \text{ where } R_9 = \left( \frac{11p-7}{12}, \frac{7p-11}{12} \right)$$
**Case IV:** Suppose that $3 \mid (2p + 1)$ and $4 \mid (p + 1)$. Then

$$I_p(xy) = I_p(y) - I_p(x)$$

$$= I_p(y) + \psi(I_p(x))$$

$$= \left\{ \frac{p + 1}{3}, R_1 \right\} + \left\{ \frac{3p - 1}{4}, R_6 \right\}$$

$$= \left\{ \frac{p + 1}{12}, R_{10} \right\} \text{ where } R_{10} = \left\{ \frac{11p - 1}{12}, \frac{p - 11}{12} \right\}$$

Thus we can conclude that the evaluation of $I_p(a_0)$ is possible for $\alpha = 12$ in the ring $\Omega_p$.

But the most pertinent question remains unaddressed, that is, “Can we determine $I_p(a_k)$ where $a_k = \sum_{t=0}^{k} \alpha e_t$ for all $\alpha \in B = \{1, 2, 3, \cdots, p - 1\}$, and $\alpha$ is not a composite one?” It is evident that if we could determine $I_p(a_k)$ where $a_k = \sum_{t=0}^{k} \alpha e_t$ for all $\alpha \in B = \{1, 2, 3, \cdots, p - 1\}$, and at the same time $\alpha$ is not a composite one, then the technique developed earlier could be employed in determining the $I_p(a_k)$ whenever $a_k = \sum_{t=0}^{k} \alpha e_t$ for all $\alpha \in B = \{1, 2, 3, \cdots, p - 1\}$, and $\alpha$ is a composite one.