Acta Universitatis Apulensis No. 37/2014
ISSN: 1582-5329 pp. 15-30

To Professor ART Solarin on his 60th Birthday Celebration

# SOME NORMAL CONGRUENCES IN QUASIGROUPS DETERMINED BY LINEAR-BIVARIATE POLYNOMIALS OVER THE RING $\mathbb{Z}_N$

E. Ilojide and T. G. Jaiyéọlá

Abstract. In this work, two normal congruences are built on two quasigroups with underlining set $\mathbb{Z}_n^2$ relative to the linear-bivariate polynomial $P(x,y) = a + bx + cy$ that generates a quasigroup over the ring $\mathbb{Z}_n$. Four quasigroups are built using the normal congruences and these are shown to be homomorphic to the quasigroups with underlining set $\mathbb{Z}_n^2$. Some subquasigroups of the quasigroups with underlining set $\mathbb{Z}_n^2$ are also found.

2000 *Mathematics Subject Classification*: 20N02, 20N05.

*Keywords:* quasigroups, normal congruence, linear-bivariate polynomials.

## 1. Introduction

Let $G$ be a non-empty set. Define a binary operation $(\cdot)$ on $G$. $(G,\cdot)$ is called a groupoid if $G$ is closed under the binary operation $(\cdot)$. A groupoid $(G,\cdot)$ is called a quasigroup if the equations $a \cdot x = b$ and $y \cdot c = d$ have unique solutions for $x$ and $y$ for all $a,b,c,d \in G$. A quasigroup $(G,\cdot)$ is called a loop if there exists a unique element $e \in G$ called the identity element such that $x \cdot e = e \cdot x = x$ for all $x \in G$.

A function $f : S \times S \to S$ on a finite set $S$ of size $n > 0$ is said to be a Latin square (of order $n$) if for any value $a \in S$ both functions $f(a,\cdot)$ and $f(\cdot,a)$ are permutations of $S$. That is, a Latin square is a square matrix with $n^2$ entries of $n$ different elements, none of them occurring more than once within any row or column of the matrix.

**Definition 1.** *A pair of Latin squares $f_1(\cdot,\cdot)$ and $f_2(\cdot,\cdot)$ is said to be orthogonal if the pairs $\big(f_1(x,y), f_2(x,y)\big)$ are all distinct, as $x$ and $y$ vary.*

**Definition 2.** *An equivalence relation $\theta$ on a quasigroup $(G,\cdot)$ is called normal if it satisfies the following conditions:*

**(i)** *if $ca\theta cb$, then $a\theta b$;*

**(ii)** *if $ac\theta bc$, then $a\theta b$;*

**(iii)** *if $a\theta b$ and $c\theta d$, then $ac\theta bd$.*

*A normal equivalence relation is also called a normal congruence.*

The basic text books on quasigroups, loops are Pflugfelder [10], Bruck [1], Chein, Pflugfelder and Smith [2], Dene and Keedwell [3], Goodaire, Jespers and Milies [6], Sabinin [12], Smith [13], Jaíyéọlá [7] and Vasantha Kandasamy [15].

**Definition 3.** *(Bivariate Polynomial) A bivariate polynomial is a polynomial in two variables, $x$ and $y$ of the form $P(x,y) = \Sigma_{i,j} a_{ij} x^i y^j$.*

**Definition 4.** *(Bivariate Polynomial Representing a Latin Square) A bivariate polynomial $P(x,y)$ over $\mathbb{Z}_n$ is said to represent (or generate) a Latin square if $(\mathbb{Z}_n, *)$ is a quasigroup where $* : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ is defined by $x * y = P(x,y)$ for all $x, y \in \mathbb{Z}_n$.*

In 2001, Rivest [11] studied permutation polynomials (PPs) over the ring $(\mathbb{Z}_n, +, \cdot)$ where $n$ is a power of 2: $n = 2^w$. This is based on the fact that modern computers perform computations modulo $2^w$ efficiently (where $w = 2, 8, 16, 32$ or 64 is the word size of the machine), and so it was of interest to study PPs modulo a power of 2. Below are some important results from his work.

**Theorem 1.** *(Rivest [11]) A bivariate polynomial $P(x,y) = \Sigma_{i,j} a_{ij} x^i y^j$ represents a Latin square modulo $n = 2^w$, where $w \geq 2$, if and only if the four univariate polynomials $P(x,0)$, $P(x,1)$, $P(0,y)$, and $P(1,y)$ are all permutation polynomial modulo $n$.*

**Theorem 2.** *(Rivest [11]) There are no two polynomials $P_1(x,y)$, $P_2(x,y)$ modulo $2^w$ for $w \geq 1$ that form a pair of orthogonal Latin squares.*

In 2009, Vadiraja and Shankar [14] motivated by the work of Rivest continued the study of permutation polynomials over the ring $(\mathbb{Z}_n, +, \cdot)$ by studying Latin squares represented by linear and quadratic bivariate polynomials over $\mathbb{Z}_n$ when $n \neq 2^w$ with the characterization of some PPs. Some of the main results they got are stated below.

**Theorem 3.** *(Vadiraja and Shankar [14] A bivariate linear polynomial $a + bx + cy$ represents a Latin square over $\mathbb{Z}_n$, $n \neq 2^w$ if and only if one of the following equivalent conditions is satisfied:*

**(i)** *both $b$ and $c$ are coprime with $n$;*

**(ii)** *$a + bx$, $a + cy$, $(a + c) + bx$ and $(a + b) + cy$ are all permutation polynomials modulo $n$.*

**(iii)** *$b$ and $c$ are invertible in $(\mathbb{Z}_n, \cdot)$.*

**Theorem 4.** *(Vadiraja and Shankar [14]) If $P(x, y)$ is a bivariate polynomial having no cross term, then $P(x, y)$ gives a Latin square if and only if $P(x, 0)$ and $P(0, y)$ are permutation polynomials.*

**Theorem 5.** *(Vadiraja and Shankar [14]) Let $n$ be even and $P(x, y) = f(x) + g(y) + xy$ be a bivariate quadratic polynomial, where $f(x)$ and $g(y)$ are permutation polynomials modulo $n$. Then $P(x, y)$ does not give a Latin square.*

The authors were able to establish the fact that Rivest's result for a bivariate polynomial over $\mathbb{Z}_n$ when $n = 2^w$ is true for a linear-bivariate polynomial over $\mathbb{Z}_n$ when $n \neq 2^w$. Although the result of Rivest was found not to be true for quadratic-bivariate polynomials over $\mathbb{Z}_n$ when $n \neq 2^w$ with the help of counter examples, nevertheless some of such squares can be forced to be Latin squares by deleting some equal numbers of rows and columns.

Furthermore, Vadiraja and Shanhar [14] were able to find examples of pairs of orthogonal Latin squares generated by bivariate polynomials over $\mathbb{Z}_n$ when $n \neq 2^w$ which was found impossible by Rivest for bivariate polynomials over $\mathbb{Z}_n$ when $n = 2^w$.

The study of linear-bivariate polynomials that generate quasigroups over the ring $\mathbb{Z}_n$ has furthered been explored in different perspectives by Jaiyéọlá, Ilojide et. al. in [4, 8, 9, 5].

**Theorem 6.** *(Theorem I.7.4, Pflugfelder [10]) An equivalence class $G = K_g$ with respect to a normal equivalence relation $\theta$ is a subquasigroup if and only if $g\theta g^2$.*

## 2. Main Results

### 2.1. Normal Congruences

**Theorem 7.** *Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$.*

**(a)** *Define $\circledcirc$ on $\mathbb{Z}_n \times \mathbb{Z}_n$ by $(x_1, y_1) \circledcirc (x_2, y_2) = (P(x_1, x_2), P(y_1, y_2))$. Then $(\mathbb{Z}_n \times \mathbb{Z}_n, \circledcirc)$ is a quasigroup.*

**(b)** *Define $\odot$ on $\mathbb{Z}_n \times \mathbb{Z}_n$ by $(x_1, y_1) \odot (x_2, y_2) = (P(x_1, y_2), P(x_2, y_1))$. Then $(\mathbb{Z}_n \times \mathbb{Z}_n, \odot)$ is a quasigroup.*

*Proof.* **(a) Closure** Consider $(x_1, y_1) \circledcirc (x_2, y_2) = (P(x_1, x_2), P(y_1, y_2)) \in (\mathbb{Z}_n \times \mathbb{Z}_n, \circledcirc)$.

**Left Cancelation Law** Let $(x,y) \circledcirc (x_1,y_1) = (x,y) \circledcirc (x_2,y_2)$. This implies $(P(x,x_1),P(y,y_1)) = (P(x,x_2),P(y,y_2))$ which implies $P(x,x_1) = P(x,x_2)$ and $P(y,y_1) = P(y,y_2)$ which imply $x_1 = x_2$ and $y_1 = y_2$ which imply $(x_1,y_1) = (x_2,y_2)$.

**Right Cancelation Law** Let $(x_1,y_1) \circledcirc (x,y) = (x_2,y_2) \circledcirc (x,y)$. This implies $(P(x_1,x),P(y_1,y)) = (P(x_2,x),P(y_2,y))$ which implies $P(x_1,x) = P(x_2,x)$ and $P(y_1,y) = P(y_2,y)$ which imply $x_1 = x_2$ and $y_1 = y_2$ which imply $(x_1,y_1) = (x_2,y_2)$.

We conclude that $(\mathbb{Z}_n \times \mathbb{Z}_n, \circledcirc)$ is a quasigroup.

**(b) Closure** Consider $(x_1,y_1) \odot (x_2,y_2) = (P(x_1,x_2),P(y_1,y_2)) \in (\mathbb{Z}_n \times \mathbb{Z}_n, \odot)$.

**Left Cancelation Law** Let $(x,y) \odot (x_1,y_1) = (x,y) \odot (x_2,y_2)$. This implies $(P(x,y_1),P(x_1,y)) = (P(x,y_2),P(x_2,y))$ which implies $P(x,y_1) = P(x,y_2)$ and $P(x_1,y) = P(x_2,y)$ which imply $x_1 = x_2$ and $y_1 = y_2$ which imply $(x_1,y_1) = (x_2,y_2)$.

**Right Cancelation Law** Let $(x_1,y_1) \odot (x,y) = (x_2,y_2) \odot (x,y)$. This implies $(P(x_1,y),P(x,y_1)) = (P(x_2,y),P(x,y_2))$ which implies $P(x_1,y) = P(x_2,y)$ and $P(x,y_1) = P(x,y_2)$ which imply $x_1 = x_2$ and $y_1 = y_2$ which imply $(x_1,y_1) = (x_2,y_2)$.

We conclude that $(\mathbb{Z}_n \times \mathbb{Z}_n, \odot)$ is a quasigroup.

**Theorem 8.** *Let $P(x,y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$. Define thosen relation ($\widetilde{thosen}$) on $\mathbb{Z}_n \times \mathbb{Z}_n$ such that $(x_1,y_1)\widetilde{thosen}(x_2,y_2)$ if and only if $P(x_1,y_2) = P(x_2,y_1)$. Then*

**(a)** *$\widetilde{thosen}$ is a normal congruence over $(\mathbb{Z}_n \times \mathbb{Z}_n, \circledcirc)$.*

**(b)** *if $b = c$, then $\widetilde{thosen}$ is a normal congruence over $(\mathbb{Z}_n \times \mathbb{Z}_n, \odot)$.*

*Proof.* **Reflexivity** Clearly, $(x_1,y_1)\widetilde{thosen}(x_1,y_1)$ since $P(x_1,y_1) = P(x_1,y_1)$.

**Symmetry** Suppose $(x_1,y_1)\widetilde{thosen}(x_2,y_2)$. This implies that $P(x_1,y_2) = P(x_2,y_1)$ which implies that $P(x_2,y_1) = P(x_1,y_2)$. Thus, $(x_2,y_2)\widetilde{thosen}(x_1,y_1)$.

**Transitivity** Suppose $(x_1,y_1)\widetilde{thosen}(x_2,y_2)$ and $(x_2,y_2)\widetilde{thosen}(x_3,y_3)$. Then we have $P(x_1,y_2) = P(x_2,y_1)$ and $P(x_2,y_3) = P(x_3,y_2)$. These imply that $bx_1 + cy_3 - cy_1 - bx_3 = 0 \Longrightarrow (x_1,y_1)\widetilde{thosen}(x_3,y_3)$. Hence, transitivity holds.

$\therefore$ $\widetilde{thosen}$ is an equivalence relation over $\mathbb{Z}_n \times \mathbb{Z}_n$.

**(a)** Let $(x_1, y_1),\ (x_2, y_2),\ (x_3, y_3), (x_4, y_4) \in \mathbb{Z}_n \times \mathbb{Z}_n$.

**(i)** Assume that $(x_3, y_3) \circledcirc (x_1, y_1)\widetilde{thosen}(x_3, y_3) \circledcirc (x_2, y_2)$. This implies

$$\Big(P(x_3, x_1), P(y_3, y_1)\Big)\widetilde{thosen}\Big(P(x_3, x_2), P(y_3, y_2)\Big) \Longleftrightarrow$$

$$bcx_1 + c^2y_2 = bcx_2 + c^2y_1 \tag{1}$$

By the way,

$$(x_1, y_1)\widetilde{thosen}(x_2, y_2) \Longleftrightarrow bcx_1 + c^2y_2 = bcx_2 + c^2y_1 \tag{2}$$

Equation 1 and Equation 2 are the same.

$$\therefore\ (x_3, y_3) \circledcirc (x_1, y_1)\widetilde{thosen}(x_3, y_3) \circledcirc (x_2, y_2) \Longrightarrow (x_1, y_1)\widetilde{thosen}(x_2, y_2).$$

**(ii)** Assume that $(x_1, y_1) \circledcirc (x_3, y_3)\widetilde{thosen}(x_2, y_2) \circledcirc (x_3, y_3)$. This implies

$$\Big(P(x_1, x_3), P(y_1, y_3)\Big)\widetilde{thosen}\Big(P(x_2, x_3), P(y_2, y_3)\Big) \Longleftrightarrow$$

$$b^2x_1 + bcy_2 = b^2x_2 + bcy_1 \tag{3}$$

By the way,

$$(x_1, y_1)\widetilde{thosen}(x_2, y_2) \Longleftrightarrow b^2x_1 + bcy_2 = b^2x_2 + bcy_1 \tag{4}$$

Equation 3 and Equation 4 are the same.

$$\therefore\ (x_1, y_1) \circledcirc (x_3, y_3)\widetilde{thosen}(x_2, y_2) \circledcirc (x_3, y_3) \Longrightarrow (x_1, y_1)\widetilde{thosen}(x_2, y_2).$$

**(iii)** Suppose $(x_1, y_1)\widetilde{thosen}(x_2, y_2)$ and $(x_3, y_3)\widetilde{thosen}(x_4, y_4)$. These imply

$$P(x_1, y_2) = P(x_2, y_1) \text{ and } P(x_3, y_4) = P(x_4, y_3) \Longleftrightarrow$$

$$b^2x_1 + bcx_3 + bcy_2 + c^2y_4 - b^2x_2 - bcx_4 - bcy_1 - c^2y_3 = 0. \tag{5}$$

But,

$$(x_1, y_1) \circledcirc (x_3, y_3)\widetilde{thosen}(x_2, y_2) \circledcirc (x_4, y_4) \Longleftrightarrow$$

$$b^2x_1 + bcx_3 + bcy_2 + c^2y_4 - b^2x_2 - bcx_4 - bcy_1 - c^2y_3 = 0 \tag{6}$$

Equation 5 and Equation 6 are the same.

$$\therefore\ (x_1, y_1)\widetilde{thosen}(x_2, y_2) \text{ and } (x_3, y_3)\widetilde{thosen}(x_4, y_4) \Longrightarrow$$
$$(x_1, y_1) \circledcirc (x_3, y_3)\widetilde{thosen}(x_2, y_2) \circledcirc (x_4, y_4).$$

We therefore conclude that $\widetilde{thosen}$ is a normal congruence over $(\mathbb{Z}_n \times \mathbb{Z}_n, \circledcirc)$.

**(b)** We have already shown that $\widetilde{thosen}$ is an equivalence relation. It remains to show that if $b = c$, then $\widetilde{thosen}$ satisfies the three conditions of a normal congruence relative to $(\mathbb{Z}_n \times \mathbb{Z}_n, \odot)$. Now, let $(x_1, y_1),\ (x_2, y_2),\ (x_3, y_3),\ (x_4, y_4) \in \mathbb{Z}_n \times \mathbb{Z}_n$.

**(i)** $(x_1, y_1) \odot (x_2, y_2)\widetilde{thosen}(x_1, y_1) \odot (x_3, y_3) \Longrightarrow \Big(P(x_1, y_2), P(x_2, y_1)\Big)\widetilde{thosen} \Big(P(x_1, y_3), P(x_3, y_1)\Big) \Longleftrightarrow P\Big(P(x_1, y_2), P(x_3, y_1)\Big) = P\Big(P(x_1, y_3), P(x_2, y_1)\Big) \Longleftrightarrow P(a + bx_1 + cy_2, a + bx_3 + cy_1) = P(a + bx_1 + cy_3, a + bx_2 + cy_1) \Longleftrightarrow a + b(a + bx_1 + cy_2) + c(a + bx_3 + cy_1) = a + b(a + bx_1 + cy_3) + c(a + bx_2 + cy_1) \Longleftrightarrow bcx_3 + bcy_2 = bcx_2 + bcy_3$. $(x_2, y_2)\widetilde{thosen}(x_3, y_3) \Longleftrightarrow P(x_2, y_3) = P(x_3, y_2) \Longleftrightarrow a + bx_2 + cy_3 = a + bx_3 + cy_2 \Longleftrightarrow bx_2 + cy_3 = bx_3 + cy_2$. Multiplying both sides by $b$ gives $b^2x_2 + bcy_3 = b^2x_3 + bcy_2$. So, if $b = c$, $(x_1, y_1) \odot (x_2, y_2)\widetilde{thosen}(x_1, y_1) \odot (x_3, y_3) \Longrightarrow (x_2, y_2)\widetilde{thosen}(x_3, y_3)$.

**(ii)** $(x_2, y_2) \odot (x_1, y_1)\widetilde{thosen}(x_3, y_3) \odot (x_1, y_1) \Longrightarrow \Big(P(x_2, y_1), P(x_1, y_2)\Big)\widetilde{thosen} \Big(P(x_3, y_1), P(x_1, y_3)\Big) \Longleftrightarrow P\Big(P(x_2, y_1), P(x_1, y_3)\Big) = P\Big(P(x_3, y_1), P(x_1, y_2)\Big) \Longleftrightarrow P(a + bx_2 + cy_1, a + bx_1 + cy_3) = P(a + bx_3 + cy_1, a + bx_1 + cy_2) \Longleftrightarrow a + b(a + bx_2 + cy_1) + c(a + bx_1 + cy_3) = a + b(a + bx_3 + cy_1) + c(a + bx_1 + cy_2) \Longleftrightarrow b^2x_2 + c^2y_3 = b^2x_3 + c^2y_2$. $(x_2, y_2)\widetilde{thosen}(x_3, y_3) \Longrightarrow P(x_2, y_3) = P(x_3, y_2) \Longleftrightarrow a + bx_2 + cy_3 = a + bx_3 + cy_2 \Longleftrightarrow bx_2 + cy_3 = bx_3 + cy_2$. Multiplying both sides by $b$ gives $b^2x_2 + bcy_3 = b^2x_3 + bcy_2$. So, if $b = c$, $(x_2, y_2) \odot (x_1, y_1)\widetilde{thosen}(x_3, y_3) \odot (x_1, y_1) \Longrightarrow (x_2, y_2)\widetilde{thosen}(x_3, y_3)$.

**(iii)** $(x_1, y_1)\widetilde{thosen}(x_2, y_2)$ and $(x_3, y_3)\widetilde{thosen}(x_4, y_4) \Longrightarrow P(x_1, y_2) = P(x_2, y_1)$ and $P(x_3, y_4) = P(x_4, y_3) \Longleftrightarrow a + bx_1 + cy_2 = a + bx_2 + cy_1$ and $a + bx_3 + cy_4 = a + bx_4 + cy_3 \Longleftrightarrow bx_1 + cy_2 - bx_2 - cy_1 = 0$ and $bx_3 + cy_4 - bx_4 - cy_3 = 0 \Longrightarrow bx_1 + cy_2 - bx_2 - cy_1 - bx_3 - cy_4 + bx_4 + cy_3 = 0$. Multiplying both sides by $b$ gives $b^2x_1 + bcy_2 - b^2x_2 - bcy_1 - b^2x_3 - bcy_4 + b^2x_4 + bcy_3 = 0$.
$(x_1, y_1) \odot (x_3, y_3)\widetilde{thosen}(x_2, y_2) \odot (x_4, y_4) \Longrightarrow \Big(P(x_1, y_3), P(x_3, y_1)\Big)\widetilde{thosen} \Big(P(x_2, y_4), P(x_4, y_2)\Big) \Longleftrightarrow P\Big(P(x_1, y_3), P(x_4, y_2)\Big) =$

$P\Big(P(x_2, y_4), P(x_3, y_1)\Big) \iff P(a + bx_1 + cy_3, a + bx_4 + cy_2) = P(a + bx_2 + cy_4, a + bx_3 + cy_1) \iff a + b(a + bx_1 + cy_3) + c(a + bx_4 + cy_2) = a + b(a + bx_2 + cy_4) + c(a + bx_3 + cy_1) \iff b^2x_1 + bcy_3 + bcx_4 + c^2y_2 - b^2x_2 - bcy_4 - bcx_3 - c^2y_1 = 0$. So, if $b = c$, $(x_1, y_1)\widetilde{thosen}(x_2, y_2)$ and $(x_3, y_3)\widetilde{thosen}(x_4, y_4) \implies (x_1, y_1) \odot (x_3, y_3)\widetilde{thosen}(x_2, y_2) \odot (x_4, y_4)$.

$\therefore$ $\widetilde{thosen}$ is a normal congruence over $(\mathbb{Z}_n \times \mathbb{Z}_n, \odot)$.

**Theorem 9.** *Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$. Define $\sim$ on $\mathbb{Z}_n \times \mathbb{Z}_n$ such that $(x_1, y_1) \sim (x_2, y_2)$ if and only if $P(x_1, y_1) = P(x_2, y_2)$. Then*

**(a)** *$\sim$ is a normal congruence over $(\mathbb{Z}_n \times \mathbb{Z}_n, \circledcirc)$.*

**(b)** *if $b = c$, then $\sim$ is a normal congruence over $(\mathbb{Z}_n \times \mathbb{Z}_n, \odot)$.*

*Proof.* **Reflexivity** Clearly, $(x_1, y_1) \sim (x_1, y_1)$ since $P(x_1, y_1) = P(x_1, y_1)$.

**Symmetry** Suppose $(x_1, y_1) \sim (x_2, y_2)$. This implies $P(x_1, y_1) = P(x_2, y_2)$ which implies $P(x_2, y_2) = P(x_1, y_1)$ which implies $(x_2, y_2) \sim (x_1, y_1)$.

**Transitivity** Suppose $(x_1, y_1) \sim (x_2, y_2)$ and $(x_2, y_2) \sim (x_3, y_3)$. Then we have $P(x_1, y_1) = P(x_2, y_2)$ and $P(x_2, y_2) = P(x_3, y_3)$. These imply that $bx_1 + cy_1 - bx_3 - cy_3 = 0$. Also, $(x_1, y_1) \sim (x_3, y_3)$ gives $bx_1 + cy_1 - bx_3 - cy_3 = 0$. Hence, transitivity holds.

**(a)** Let $(x_1, y_1)$, $(x_2, y_2)$, $(x_3, y_3)$, $(x_4, y_4) \in \mathbb{Z}_n \times \mathbb{Z}_n$.

**(i)** Assume that $(x_3, y_3) \circledcirc (x_1, y_1) \sim (x_3, y_3) \circledcirc (x_2, y_2)$. This implies

$$\Big(P(x_3, x_1), P(y_3, y_1)\Big) \sim \Big(P(x_3, x_2), P(y_3, y_2)\Big) \iff$$

$$bcx_1 + c^2y_1 = bcx_2 + c^2y_2. \tag{7}$$

$$(x_1, y_1) \sim (x_2, y_2) \iff bcx_1 + c^2y_1 = bcx_2 + c^2y_2. \tag{8}$$

Equation 7 and Equation 8 are the same. $\therefore$ $(x_3, y_3) \circledcirc (x_1, y_1) \sim (x_3, y_3) \circledcirc (x_2, y_2) \implies (x_1, y_1) \sim (x_2, y_2)$.

**(ii)** Assume that $(x_1, y_1) \circledcirc (x_3, y_3) \sim (x_2, y_2) \circledcirc (x_3, y_3)$ which implies

$$\Big(P(x_1, x_3), P(y_1, y_3)\Big) \sim \Big(P(x_2, x_3), P(y_2, y_3)\Big) \iff$$

$$b^2x_1 + bcy_1 = b^2x_2 + bcy_2. \tag{9}$$

$$(x_1, y_1) \sim (x_2, y_2) \Longleftrightarrow b^2x_1 + bcy_1 = b^2x_2 + bcy_2. \tag{10}$$

Equation 9 and Equation 10 are the same. $\therefore$ $(x_1, y_1) \circledcirc (x_3, y_3) \sim (x_2, y_2) \circledcirc (x_3, y_3) \Longrightarrow (x_1, y_1) \sim (x_2, y_2)$.

**(iii)** Suppose $(x_1, y_1) \sim (x_2, y_2)$ and $(x_3, y_3) \sim (x_4, y_4)$. This implies $P(x_1, y_1) = P(x_2, y_2)$ and $P(x_3, y_3) = P(x_4, y_4)$ which imply

$$b^2x_1 + bcx_3 + bcy_1 + c^2y_3 - b^2x_2 - bcx_4 - bcy_2 - c^2y_4 = 0 \tag{11}$$

$(x_1, y_1) \circledcirc (x_3, y_3) \sim (x_2, y_2) \circledcirc (x_4, y_4) \Longleftrightarrow$

$$b^2x_1 + bcx_3 + bcy_1 + c^2y_3 - b^2x_2 - bcx_4 - bcy_2 - c^2y_4 = 0 \tag{12}$$

Equation 11 and Equation 12 are the same. $\therefore$ $(x_1, y_1) \sim (x_2, y_2)$ and $(x_3, y_3) \sim (x_4, y_4) \Longrightarrow (x_1, y_1) \circledcirc (x_3, y_3) \sim (x_2, y_2) \circledcirc (x_4, y_4)$.

We therefore conclude that $\sim$ is a normal congruence over $(\mathbb{Z}_n \times \mathbb{Z}_n, \circledcirc)$.

**(b)** We have already shown that $\sim$ is an equivalence relation. It remains to show that if $b = c$, then $\sim$ satisfies the three conditions of a normal congruence relative to $(\mathbb{Z}_n \times \mathbb{Z}_n, \odot)$. Let $(x_1, y_1)$, $(x_2, y_2)$, $(x_3, y_3)$, $(x_4, y_4) \in (\mathbb{Z}_n \times \mathbb{Z}_n)$.

**(i)** $(x_1, y_1) \odot (x_2, y_2) \sim (x_1, y_1) \odot (x_3, y_3) \Longrightarrow \Big(P(x_1, y_2), P(x_2, y_1)\Big) \sim \Big(P(x_1, y_3), P(x_3, y_1)\Big) \Longleftrightarrow P\Big(P(x_1, y_2), P(x_2, y_1)\Big) = P\Big(P(x_1, y_3), P(x_3, y_1)\Big) \Longleftrightarrow P(a+bx_1+cy_2, a+bx_2 + cy_1) = P(a + bx_1 + cy_3, a + bx_3 + cy_1) \Longleftrightarrow a + b(a + bx_1 + cy_2) + c(a + bx_2 + cy_1) = a + b(a + bx_1 + cy_3) + c(a + bx_3 + cy_1) \Longleftrightarrow$

$$bcx_2 + bcy_2 = bcx_3 + bcy_3 \tag{13}$$

$(x_2, y_2) \sim (x_3, y_3) \Longleftrightarrow P(x_2, y_2) = P(x_3, y_3) \Longleftrightarrow a + bx_2 + cy_2 = a + bx_3 + cy_3 \Longleftrightarrow bx_2 + cy_2 = bx_3 + cy_3$. Multiplying both sides by $b$ gives

$$b^2x_2 + bcy_2 = b^2x_3 + bcy_3 \tag{14}$$

So, if $b = c$, Equation 13 and Equation 14 are the same. $\therefore$ $(x_1, y_1) \odot (x_2, y_2) \sim (x_1, y_1) \odot (x_3, y_3) \Longrightarrow (x_2, y_2) \sim (x_3, y_3)$.

**(ii)** $(x_2, y_2) \odot (x_1, y_1) \sim (x_3, y_3) \odot (x_1, y_1) \Longrightarrow \Big(P(x_2, y_1), P(x_1, y_2)\Big) \sim \Big(P(x_3, y_1), P(x_1, y_3)\Big) \Longleftrightarrow P\Big(P(x_2, y_1), P(x_1, y_2)\Big) = P\Big(P(x_3, y_1), P(x_1, y_3)\Big) \Longleftrightarrow P(a+bx_2+cy_1, a+bx_1 + cy_2) = P(a + bx_3 + cy_1, a + bx_1 + cy_3) \Longleftrightarrow a + b(a + bx_2 + cy_1) + c(a + bx_1 + cy_2) = a + b(a + bx_3 + cy_1) + c(a + bx_1 + cy_3) \Longleftrightarrow$

$$b^2x_2 + c^2y_2 = b^2x_3 + c^2y_3. \tag{15}$$

$(x_2, y_2) \sim (x_3, y_3) \Longrightarrow P(x_2, y_2) = P(x_3, y_3) \Longleftrightarrow a + bx_2 + cy_2 = a + bx_3 + cy_3 \Longleftrightarrow bx_2 + cy_2 = bx_3 + cy_3$. Multiplying both sides by $b$ gives

$$b^2x_2 + bcy_2 = b^2x_3 + bcy_3. \tag{16}$$

So, if $b = c$, Equation 15 and Equation 16 are the same. $\therefore$ $(x_2, y_2) \odot (x_1, y_1) \sim (x_3, y_3) \odot (x_1, y_1) \Longrightarrow (x_2, y_2) \sim (x_3, y_3)$.

**(iii)** $(x_1, y_1) \sim (x_2, y_2)$ and $(x_3, y_3) \sim (x_4, y_4) \Longrightarrow P(x_1, y_1) = P(x_2, y_2)$ and $P(x_3, y_3) = P(x_4, y_4) \Longleftrightarrow a+bx_1+cy_1 = a+bx_2+cy_2$ and $a+bx_3+cy_3 = a + bx_4 + cy_4 \Longleftrightarrow bx_1 + cy_1 - bx_2 - cy_2 = 0$ and $bx_3 + cy_3 - bx_4 - cy_4 = 0 \Longrightarrow bx_1 + cy_1 - bx_2 - cy_2 - bx_3 - cy_3 + bx_4 + cy_4 = 0$. Multiplying both sides by $b$ gives

$$b^2x_1 + bcy_1 - b^2x_2 - bcy_2 - b^2x_3 - bcy_3 + b^2x_4 + bcy_4 = 0 \tag{17}$$

$(x_1, y_1) \odot (x_3, y_3) \sim (x_2, y_2) \odot (x_4, y_4) \Longrightarrow [P(x_1, y_3), P(x_3, y_1)] \sim [P(x_2, y_4), P(x_4, y_2)] \Longleftrightarrow P[P(x_1, y_3), P(x_3, y_1)] = P[P(x_2, y_4), P(x_4, y_2)] \Longleftrightarrow P(a + bx_1 + cy_3, a + bx_3 + cy_1) = P(a + bx_2 + cy_4, a + bx_4 + cy_2) \Longleftrightarrow a + b(a + bx_1 + cy_3) + c(a + bx_3 + cy_1) = a + b(a + bx_2 + cy_4) + c(a + bx_4 + cy_2) \Longleftrightarrow$

$$b^2x_1 + bcy_3 + bcx_3 + c^2y_1 - b^2x_2 - bcy_4 - bcx_4 - c^2y_2 = 0 \tag{18}$$

So, if $b = c$, Equation 17 and Equation 18 are the same. Thus, $(x_1, y_1) \sim (x_2, y_2)$ and $(x_3, y_3) \sim (x_4, y_4) \Longrightarrow (x_1, y_1) \odot (x_3, y_3) \sim (x_2, y_2) \odot (x_4, y_4)$.

$\therefore$ $\sim$ is a normal congruence over $(\mathbb{Z}_n \times \mathbb{Z}_n, \odot)$.

### 2.2. Quotient Quasigroups

**Theorem 10.** *Let $P(x,y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$.*

**(a)** *If $\mathbb{Z}_n^2/\widetilde{thosen} = \{[K_z]\}_{z\in\mathbb{Z}_n^2}$ and for all $K_{z_1}, K_{z_2} \in \mathbb{Z}_n^2/\widetilde{thosen}$, $*$ is defined on $\mathbb{Z}_n^2/\widetilde{thosen}$ as $K_{z_1} * K_{z_2} = K_{z_1 \circledcirc z_2}$, then $(\mathbb{Z}_n^2/\widetilde{thosen}, *)$ is a quasigroup.*

**(b)** *$\widetilde{thosen}$ induces an homomorphism from $(\mathbb{Z}_n^2, \circledcirc)$ to $(\mathbb{Z}_n^2/\widetilde{thosen}, *)$.*

*Proof.* **(a) Left Cancelation Law** Let $K_{z_1} * K_{z_2} = K_{z_1} * K_{z_3}$, where $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2)$, $z_3 = (x_3, y_3)$. This implies

$$K_{(x_1,y_1)} * K_{(x_2,y_2)} = K_{(x_1,y_1)} * K_{(x_3,y_3)} \Longrightarrow$$
$$K_{(x_1,y_1)\circledcirc(x_2,y_2)} = K_{(x_1,y_1)\circledcirc(x_3,y_3)} \Longrightarrow$$
$$(x_1, y_1) \circledcirc (x_2, y_2)\widetilde{thosen}(x_1, y_1) \circledcirc (x_3, y_3) \Longrightarrow (x_2, y_2)\widetilde{thosen}(x_3, y_3) \Longrightarrow$$
$$K_{(x_2,y_2)} = K_{(x_3,y_3)} \Longrightarrow K_{z_2} = K_{z_3}.$$

**Right Cancelation Law** Let $K_{z_2} * K_{z_1} = K_{z_3} * K_{z_1}$, where $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2)$, $z_3 = (x_3, y_3)$. This implies

$$K_{(x_2,y_2)} * K_{(x_1,y_1)} = K_{(x_3,y_3)} * K_{(x_1,y_1)} \Longrightarrow$$
$$K_{(x_2,y_2)\circledcirc(x_1,y_1)} = K_{(x_3,y_3)\circledcirc(x_1,y_1)} \Longrightarrow$$
$$(x_2, y_2) \circledcirc (x_1, y_1)\widetilde{thosen}(x_3, y_3) \circledcirc (x_1, y_1) \Longrightarrow (x_2, y_2)\widetilde{thosen}(x_3, y_3) \Longrightarrow$$
$$K_{(x_2,y_2)} = K_{(x_3,y_3)} \Longrightarrow K_{z_2} = K_{z_3}.$$

We conclude that $(\mathbb{Z}_n^2/\widetilde{thosen}, *)$ is a quasigroup.

**(b)** Define $\alpha : (\mathbb{Z}_n^2, \circledcirc) \longrightarrow (\mathbb{Z}_n^2/\widetilde{thosen}, *)$ by $\alpha[(x, y)] = K_{(x,y)}$. Consider

$$\alpha[(x_1, y_1)\circledcirc(x_2, y_2)] = K_{(x_1,y_1)\circledcirc(x_2,y_2)} = K_{(x_1,y_1)}*K_{(x_2,y_2)} = \alpha[(x_1, y_1)]*\alpha[(x_2, y_2)].$$

Thus, $\alpha$ is an homomorphism.

**Theorem 11.** *Let $P(x,y) = a + bx + by$ represent a quasigroup over $\mathbb{Z}_n$.*

**(a)** *If $\mathbb{Z}_n^2/\widetilde{thosen} = \{[K_z]\}_{z\in\mathbb{Z}_n^2}$ and for all $K_{z_1}, K_{z_2} \in \mathbb{Z}_n^2/\widetilde{thosen}$, $*$ is defined on $\mathbb{Z}_n^2/\widetilde{thosen}$ as $K_{z_1} * K_{z_2} = K_{z_1 \odot z_2}$, then $(\mathbb{Z}_n^2/\widetilde{thosen}, *)$ is a quasigroup.*

**(b)** *$\widetilde{thosen}$ induces an homomorphism from $(\mathbb{Z}_n^2, \odot)$ to $(\mathbb{Z}_n^2/\widetilde{thosen}, *)$.*

*Proof.* **(a) Left Cancelation Law** Let $K_{z_1} * K_{z_2} = K_{z_1} * K_{z_3}$, where $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2)$, $z_3 = (x_3, y_3)$. This implies

$$K_{(x_1,y_1)} * K_{(x_2,y_2)} = K_{(x_1,y_1)} * K_{(x_3,y_3)} \Longrightarrow$$
$$K_{(x_1,y_1)\odot(x_2,y_2)} = K_{(x_1,y_1)\odot(x_3,y_3)} \Longrightarrow$$
$$(x_1, y_1) \odot (x_2, y_2)\widetilde{thosen}(x_1, y_1) \odot (x_3, y_3) \Longrightarrow (x_2, y_2)\widetilde{thosen}(x_3, y_3) \Longrightarrow$$
$$K_{(x_2,y_2)} = K_{(x_3,y_3)} \Longrightarrow K_{z_2} = K_{z_3}.$$

**Right Cancelation Law** Let $K_{z_2} * K_{z_1} = K_{z_3} * K_{z_1}$, where $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2)$, $z_3 = (x_3, y_3)$. This implies

$$K_{(x_2,y_2)} * K_{(x_1,y_1)} = K_{(x_3,y_3)} * K_{(x_1,y_1)} \Longrightarrow$$
$$K_{(x_2,y_2)\odot(x_1,y_1)} = K_{(x_3,y_3)\odot(x_1,y_1)} \Longrightarrow$$
$$(x_2, y_2) \odot (x_1, y_1)\widetilde{thosen}(x_3, y_3) \odot (x_1, y_1) \Longrightarrow (x_2, y_2)\widetilde{thosen}(x_3, y_3) \Longrightarrow$$
$$K_{(x_2,y_2)} = K_{(x_3,y_3)} \Longrightarrow K_{z_2} = K_{z_3}.$$

We conclude that $(\mathbb{Z}_n^2/\widetilde{thosen}, *)$ is a quasigroup.

**(b)** Define $\alpha : (\mathbb{Z}_n^2, \odot) \longrightarrow (\mathbb{Z}_n^2/\widetilde{thosen}, *)$ by $\alpha[(x, y)] = K_{(x,y)}$. Consider

$$\alpha[(x_1, y_1)\odot(x_2, y_2)] = K_{(x_1,y_1)\odot(x_2,y_2)} = K_{(x_1,y_1)}*K_{(x_2,y_2)} = \alpha[(x_1, y_1)]*\alpha[(x_2, y_2)].$$

Thus, $\alpha$ is an homomorphism.

**Theorem 12.** *Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$.*

**(a)** *If $\mathbb{Z}_n^2/\sim = \{[K_z]\}_{z\in\mathbb{Z}_n^2}$ and for all $K_{z_1}, K_{z_2} \in \mathbb{Z}_n^2/\sim$, $*$ is defined on $\mathbb{Z}_n^2/\sim$ as $K_{z_1} * K_{z_2} = K_{z_1 \circledcirc z_2}$, then $(\mathbb{Z}_n^2/\sim, *)$ is a quasigroup.*

**(b)** *$\sim$ induces an homomorphism from $(\mathbb{Z}_n^2, \circledcirc)$ to $(\mathbb{Z}_n^2/\sim, *)$.*

*Proof.* **(a) Left Cancelation Law** Let $K_{z_1} * K_{z_2} = K_{z_1} * K_{z_3}$, where $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2)$, $z_3 = (x_3, y_3)$. This implies

$$K_{(x_1,y_1)} * K_{(x_2,y_2)} = K_{(x_1,y_1)} * K_{(x_3,y_3)} \Longrightarrow$$
$$K_{(x_1,y_1)\circledcirc(x_2,y_2)} = K_{(x_1,y_1)\circledcirc(x_3,y_3)} \Longrightarrow$$
$$(x_1, y_1) \circledcirc (x_2, y_2) \sim (x_1, y_1) \circledcirc (x_3, y_3) \Longrightarrow (x_2, y_2) \sim (x_3, y_3) \Longrightarrow$$
$$K_{(x_2,y_2)} = K_{(x_3,y_3)} \Longrightarrow K_{z_2} = K_{z_3}.$$

**Right Cancelation Law** Let $K_{z_2} * K_{z_1} = K_{z_3} * K_{z_1}$, where $z_1 = (x_1, y_1), z_2 = (x_2, y_2), z_3 = (x_3, y_3)$. This implies

$$\begin{gathered} K_{(x_2,y_2)} * K_{(x_1,y_1)} = K_{(x_3,y_3)} * K_{(x_1,y_1)} \Longrightarrow \\ K_{(x_2,y_2)\circledcirc(x_1,y_1)} = K_{(x_3,y_3)\circledcirc(x_1,y_1)} \Longrightarrow \\ (x_2, y_2) \circledcirc (x_1, y_1) \sim (x_3, y_3) \circledcirc (x_1, y_1) \Longrightarrow (x_2, y_2) \sim (x_3, y_3) \Longrightarrow \\ K_{(x_2,y_2)} = K_{(x_3,y_3)} \Longrightarrow K_{z_2} = K_{z_3}. \end{gathered}$$

We conclude that $(\mathbb{Z}_n^2/\sim, *)$ is a quasigroup.

**(b)** Define $\alpha : (\mathbb{Z}_n^2, \circledcirc) \longrightarrow (\mathbb{Z}_n^2/\sim, *)$ by $\alpha[(x, y)] = K_{(x,y)}$. Consider

$$\alpha[(x_1, y_1)\circledcirc(x_2, y_2)] = K_{(x_1,y_1)\circledcirc(x_2,y_2)} = K_{(x_1,y_1)}*K_{(x_2,y_2)} = \alpha[(x_1, y_1)]*\alpha[(x_2, y_2)].$$

Thus, $\alpha$ is an homomorphism.

**Theorem 13.** *Let $P(x, y) = a + bx + by$ represent a quasigroup over $\mathbb{Z}_n$.*

**(a)** *If $\mathbb{Z}_n^2/\sim = \{[K_z]\}_{z\in\mathbb{Z}_n^2}$ and for all $K_{z_1}, K_{z_2} \in \mathbb{Z}_n^2/\sim$, $*$ is defined on $\mathbb{Z}_n^2/\sim$ as $K_{z_1} * K_{z_2} = K_{z_1\odot z_2}$, then $(\mathbb{Z}_n^2/\sim, *)$ is a quasigroup.*

**(b)** *$\sim$ induces an homomorphism from $(\mathbb{Z}_n^2, \odot)$ to $(\mathbb{Z}_n^2/\sim, *)$.*

*Proof.* **(a) Left Cancelation Law** Let $K_{z_1} * K_{z_2} = K_{z_1} * K_{z_3}$, where $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2), z_3 = (x_3, y_3)$. This implies

$$\begin{gathered} K_{(x_1,y_1)} * K_{(x_2,y_2)} = K_{(x_1,y_1)} * K_{(x_3,y_3)} \Longrightarrow \\ K_{(x_1,y_1)\odot(x_2,y_2)} = K_{(x_1,y_1)\odot(x_3,y_3)} \Longrightarrow \\ (x_1, y_1) \odot (x_2, y_2) \sim (x_1, y_1) \odot (x_3, y_3) \Longrightarrow (x_2, y_2) \sim (x_3, y_3) \Longrightarrow \\ K_{(x_2,y_2)} = K_{(x_3,y_3)} \Longrightarrow K_{z_2} = K_{z_3}. \end{gathered}$$

**Right Cancelation Law** Let $K_{z_2} * K_{z_1} = K_{z_3} * K_{z_1}$, where $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2), z_3 = (x_3, y_3)$. This implies

$$\begin{gathered} K_{(x_2,y_2)} * K_{(x_1,y_1)} = K_{(x_3,y_3)} * K_{(x_1,y_1)} \Longrightarrow \\ K_{(x_2,y_2)\odot(x_1,y_1)} = K_{(x_3,y_3)\odot(x_1,y_1)} \Longrightarrow \\ (x_2, y_2) \odot (x_1, y_1) \sim (x_3, y_3) \odot (x_1, y_1) \Longrightarrow (x_2, y_2) \sim (x_3, y_3) \Longrightarrow \\ K_{(x_2,y_2)} = K_{(x_3,y_3)} \Longrightarrow K_{z_2} = K_{z_3}. \end{gathered}$$

We conclude that $(\mathbb{Z}_n^2/\sim, *)$ is a quasigroup.

**(b)** Define $\alpha : (\mathbb{Z}_n^2, \odot) \longrightarrow (\mathbb{Z}_n^2/\sim, *)$ by $\alpha[(x,y)] = K_{(x,y)}$. Consider

$$\alpha[(x_1,y_1)\odot(x_2,y_2)] = K_{(x_1,y_1)\odot(x_2,y_2)} = K_{(x_1,y_1)} * K_{(x_2,y_2)} = \alpha[(x_1,y_1)]*\alpha[(x_2,y_2)].$$

Thus, $\alpha$ is an homomorphism.

**Theorem 14.** *Let $P(x,y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$.*

**(a)** $K_{(x,y)} \in (\mathbb{Z}_n^2/\sim, *)$ *is a subquasigroup of* $(\mathbb{Z}_n^2, \circledcirc) \Longleftrightarrow b(x-y) + c(P(x,x) - P(y,y)) = 0$.

**(b)** $K_{(x,x)} = \{(y,y)\}_{y\in\mathbb{Z}_n}$ *is a subquasigroup of* $(\mathbb{Z}_n^2, \circledcirc)$.

**(c)** $(b+cb+c^2) = 0$ *if and only if* $K_{(x,y)} \in (\mathbb{Z}_n^2/\sim, *)$ *is a subquasigroup of* $(\mathbb{Z}_n^2, \circledcirc)$.

*Proof.* **(a)** By Theorem 6, it suffices to show that $(x,y) \sim (x,y)^2$ i.e. $(x,y) \sim (x,y) \circledcirc (x,y)$. This implies $(x,y) \sim \big(P(x,x), P(y,y)\big) \Leftrightarrow P\big(x, P(x,x)\big) = P\big(y, P(y,y)\big) \Leftrightarrow a + bx + cP(x,x) = a + by + cP(y,y) \Leftrightarrow b(x-y) + c[P(x,x) - P(y,y)] = 0$ as required. Moreover,

**(b)** $K_{(x,x)} = \{(y,z)|(x,x) \sim (y,z)\} = \{(y,z)|P(x,y) = P(x,z)\} = \{(y,z)|a + bx + cy = a + bx + cz\} = \{(y,z)|cy = cz\} = \{(y,z)|y = z\} = \{(y,y)\}_{y\in\mathbb{Z}_n}$.

**(c)** $b(x-y) + c[P(x,x) - P(y,y)] = 0 \Longleftrightarrow b(x-y) + c[a + bx + cx - (a + by + cy)] = 0 \Leftrightarrow (x-y)[b + bc + c^2] = 0$.

**Theorem 15.** *Let $P(x,y) = a + bx + by$ represent a quasigroup over $\mathbb{Z}_n$.*

**(a)** $K_{(x,y)} \in (\mathbb{Z}_n^2/\sim, *)$ *is a subquasigroup of* $(\mathbb{Z}_n^2, \odot) \Longleftrightarrow x = y$.

**(b)** $K_{(x,x)} = \{(y,y)\}_{y\in\mathbb{Z}_n}$ *is a subquasigroup of* $(\mathbb{Z}_n^2, \odot)$.

*Proof.* **(a)** By Theorem 6, it suffices to show that $(x,y) \sim (x,y)^2$ i.e. $(x,y) \sim (x,y) \odot (x,y)$. This implies $(x,y) \sim \big(P(x,y), P(x,y)\big) \Longleftrightarrow P(x, P(x,y)) = P(y, P(x,y)) \Longleftrightarrow a + bx + cP(x,y) = a + by + cP(x,y) \Longleftrightarrow x = y$ as required.

**(b)** $K_{(x,x)} = \{(y,z)|(x,x) \sim (y,z)\} = \{(y,z)|P(x,y) = P(x,z)\} = \{(y,z)|a + bx + cy = a + bx + cz\} = \{(y,z)|cy = cz\} = \{(y,z)|y = z\} = \{(y,y)\}_{y\in\mathbb{Z}_n}$.

**Theorem 16.** *Let $P(x,y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$.*

**(a)** $K_{(x,y)} \in (\mathbb{Z}_n^2/\widetilde{thosen}, *)$ *is a subquasigroup of* $(\mathbb{Z}_n^2, \circledcirc) \Longleftrightarrow b[x - P(x,x)] = c[y - P(y,y)]$.

**(b)** *If* $P(x,x) = x + c$ *and* $P(y,y) = b + y$, *then* $K_{(x,y)} \in \mathbb{Z}_n^2/\widetilde{thosen}$ *is a subquasigroup of* $(\mathbb{Z}_n^2, \circledcirc)$.

**(c)** *If* $P(x,x) = x$ *and* $P(y,y) = y$, *then* $K_{(x,y)} \in (\mathbb{Z}_n^2/\sim, *)$ *is a subquasigroup of* $(\mathbb{Z}_n^2, \circledcirc)$. *Conversely, if* $K_{(x,y)} \in (\mathbb{Z}_n^2/\widetilde{thosen}, \backslash *)$ *is a subquasigroup of* $(\mathbb{Z}_n^2, \circledcirc)$, *then,* $P(x,x) = x \Longleftrightarrow P(y,y) = b$.

*Proof.* **(a)** By Theorem 6, it suffices to show that $(x,y)\widetilde{thosen}(x,y)^2$ i.e. $(x,y)\widetilde{thosen}(x,y) \circledcirc (x,y)$. This implies $(x,y)\widetilde{thosen}\Big(P(x,x), P(y,y)\Big) \Longleftrightarrow P(x, P(y,y)) = P(P(x,x), y) \Longleftrightarrow a + bx + cP(y,y) = a + bP(x,x) + cy \Longleftrightarrow b[x - P(x,x)] = c[y - P(y,y)]$ as required. Moreover,

**(b)** If $P(x,x) = x + c$ and $P(y,y) = b + y$, the last equation is satisfied.

**(c)** If $P(x,x) = x$ and $P(y,y) = y$, the last equation is also satisfied.

**Theorem 17.** *Let* $P(x,y) = a + bx + by$ *represent a quasigroup over* $\mathbb{Z}_n$.

**(a)** $K_{(x,y)} \in (\mathbb{Z}_n^2/\widetilde{thosen}, *)$ *is a subquasigroup of* $(\mathbb{Z}_n^2, \odot) \Longleftrightarrow x = y$.

**(b)** $K_{(x,x)} = \{(y,y)\}_{y\in\mathbb{Z}_n}$ *is a subquasigroup of* $(\mathbb{Z}_n^2, \odot)$.

*Proof.* **(a)** By Theorem 6, it suffices to show that $(x,y)\widetilde{thosen}(x,y)^2$ i.e. $(x,y)\widetilde{thosen}(x,y) \odot (x,y)$. This implies $(x,y)\widetilde{thosen}\Big(P(x,y), P(x,y)\Big) \Longleftrightarrow P(x, P(x,y)) = P(P(x,y), y) \Longleftrightarrow a + bx + cP(x,y) = a + bP(x,y) + cy \Longleftrightarrow b[x - P(x,y)] - c[y - P(x,y)] = 0 \Longleftrightarrow x = y$ as required.

**(b)** $K_{(x,x)} = \{(y,z)|(x,x)\widetilde{thosen}(y,z)\} = \{(y,z)|P(x,z) = P(y,x)\} = \{(y,z)|a + bx + cz = a + by + cx\} = \{(y,z)|b(x-y) = b(x-z)\} = \{(y,z)|y = z\} = \{(y,y)\}_{y\in\mathbb{Z}_n}$.

## References

[1] R. H. Bruck, *A survey of binary systems*, Springer-Verlag, Berlin-Göttingen-Heidelberg (1966),185pp.

[2] O. Chein, H. O. Pflugfelder, J. D. H. Smith, *Quasigroups and loops : Theory and applications*, Heldermann Verlag(1990), 568pp.

[3] J. Dene, A. D. Keedwell, *Latin squares and their applications*, the English University press Ltd. (1974), 549pp.

[4] E. Ilojide, T. G. Jaiyeola, O. O. Owojori, *Varieties of groupoids and quasigroups generated by linear-bivariate polynomials over the ring* $\mathbb{Z}_n$, Int. J. Math. Combin. 2 (2011), 79-97.

[5] E. Ilojide, T. G. Jaiyeola, S. A. Akinleye, *On the right, left and middle linear-bivariate polynomials of a linear-bivariate polynomial that generates a quasigroup over the ring* $\mathbb{Z}_n$, J. Nig. Math. Soc. 31 (2012), 107-118.

[6] E. G. Goodaire, E. Jespers, C. P. Milies, *Alternative loop rings*, NHMS(184), Elsevier (1996), 387pp.

[7] T. G. Jaiyeola, *A study of new concepts in smarandache quasigroups and loops*, Pro. Inform. Learn.(ILQ), Ann Arbor, USA (2009), 127pp.

[8] T. G. Jaiyeola, E. Ilojide, *On a group of linear-bivariate polynomials that generate quasigroups over the ring* $\mathbb{Z}_n$, Anal. Univ. De Vest Din Timisoara, Seria Matematica-Informatica. 50, 2 (2012), 45-53.

[9] T. G. Jaiyeola, E. Ilojide, B. A. Popoola, *On the isotopy structure of elements of the group* $\mathcal{P}_p(\mathbb{Z}_n)$, J. Nig. Math. Soc. 32 (2013), 317-329.

[10] H. O. Pflugfelder, *Quasigroups and loops : Introduction*, Sigma series in Pure Math. 7, Heldermann Verlag, Berlin (1990), 147pp.

[11] R. L. Rivest, *Permutation polynomials Modulo* $2^w$, Fin. Fields and Applic. 7 (2001), 287-292.

[12] L. V. Sabinin, *Smooth quasigroups and loops*, Kluver Academic Publishers, Dordrecht (1999), 249pp.

[13] J. D. H. Smith, *An introduction to quasigroups and their representations*, Taylor and Francis Group (2007), LLC.

[14] G. R. Vadiraja Bhatta, B. R. Shankar, *Permutation Polynomials modulo n,* $n \neq 2^w$ *and Latin Squares*, Int. J. Math. Combin. 2 (2009), 58-65.

[15] W. B. Vasantha Kandasamy, *Smarandache loops*, Dept. Math., Indian Institute of Technology, Madras, India (2002), 128pp.

E. Ilojide
Department of Mathematics,
Federal University of Agriculture,
Abeokuta 110101, Nigeria.
email: *emmailojide@yahoo.com, ilojidee@unaab.edu.ng*

T. G. Jaiyéọlá
Department of Mathematics,
Obafemi Awolowo University,
Ile Ife 220005, Nigeria.
email: *jaiyeolatemitope@yahoo.com, tjayeola@oauife.edu.ng*