Mathematics and Computer Science
2023; 8(1): 11-18
http://www.sciencepublishinggroup.com/j/mcs
doi: 10.11648/j.mcs.20230801.12
ISSN: 2575-6036 (Print); ISSN: 2575-6028 (Online)

The $m\Theta$ Quadratic Character in the $m\Theta$ Set $\mathbb{Z}_{n\mathbb{Z}}$

Gabriel Cedric Pemha Binyam*, Laurence Um Emilie, Yves Jonathan Ndje

Department of Mathematics and Computer Sciences, Faculty of Sciences, University of Douala, Douala, Cameroon

Email address:

gpemha@yahoo.fr (Gabriel Cedric Pemha Binyam), laurence.um@gmail.com (Laurence Um Emilie),
nyjo.yves@gmail.com (Yves Jonathan Ndje)
*Corresponding author

To cite this article:

Gabriel Cedric Pemha Binyam, Laurence Um Emilie, Yves Jonathan Ndje. The $m\Theta$ Quadratic Character in the $m\Theta$ Set $\mathbb{Z}_{n\mathbb{Z}}$. *Mathematics and Computer Science*. Vol. 8, No. 1, 2023, pp. 11-18. doi: 10.11648/j.mcs.20230801.12

Received: September 2, 2022; **Accepted:** September 28, 2022; **Published:** January 23, 2023

Abstract: The modal Θ-valent logic is a logic that contains all the thesis of the classical logical calculus and, besides allows to express notions of possibility, of necessity, and more others. The modal Θ-valent sets are the supports in term of the structure of the Θ-valent rings. A Θ chr $(m\Theta)$ is a structure which is rich at the same time of inheritance in the meaning of the romanian academician Gr. C. Moisil, as the algebraic model of a such logic. The set $\mathbb{Z}_{n\mathbb{Z}}$ contains the set $\mathbb{Z}$ and the elements $x_{n\mathbb{Z}}$ such that the support of x is not congruent to 0 modulo n. In this paper the purpose is to define on $\mathbb{Z}_{p\mathbb{Z}} - \mathbb{Z}$, p prime, a notion of quadratic residues and quadratic character which respects its structure of $m\Theta s$. Hoping that this approach will bring something of interest to the notion of quadratic residues. First of all, we construct the modal Θ-valent congruences of $(\mathbb{Z}_{n\mathbb{Z}},\ F_\alpha)$. We characterize the $m\Theta$ set $(\mathbb{Z}_{n\mathbb{Z}},\ F_\alpha)$ and we then give some arithmetical and intrinsic $m\Theta$ parameters of $\mathbb{Z}_{n\mathbb{Z}}$ which lead us to the notion of factorial of m without n in $\mathbb{Z}_{n\mathbb{Z}}$, the $m\Theta$ quotient of $(\mathbb{Z}_{n\mathbb{Z}},\ F_\alpha)$ modulo $(p\mathbb{Z}_{n\mathbb{Z}})$ and a complete system of $m\Theta$ residues modulo $p\mathbb{Z}_{n\mathbb{Z}}$, $\mathbb{N}_{n,\,p}$. After that, we define a p-valent modal quadratic residue, p prime. We characterize some properties of p-valent modal quadratic character and p-valent modal quadratic residue of p^k which establish the difference between the $m\Theta$ Euler's theorem and the Euler's theorem in the classical arithmetic. Later, we establish the theorem for determining the p-valent modal quadratic character of $a \in \mathbb{Z}_{p\mathbb{Z}} - \mathbb{Z}$ with respect to p^k. This theorem is a non-classical version of Gauss's lemma. Finally, we establish an example introducing the law of quadratic reciprocity of Gauss.

Keywords: Modal Θ-valent Sets, Modal Θ-valent Congruences, Number Theory, p-valent Modal Residues

1. Introduction

Number theory is a branch of pure mathematics devoted primarily to the study of the integers and integer-valued functions [1, 2, 3]. It was Gauss who found the first complete proof of the quadratic reciprocity law [4, 5]. The proof of the quadratic reciprocity law is based on Gauss's lemma [16]. The theory of quadratic residues has proved to be very useful in several areas of mathematics [7, 8, 11, 12]. An integer a which is not a multiple of a prime p is called a quadratic residue modulo p if the quadratic equation $x^2 = a \, mod \, p$ has a solution [16].

The notion of modal Θ-valent set noted $(\mathbb{Z}_{n\mathbb{Z}},\ F_\alpha)$ is defined by F. Ayissi Eteme in [10]. This article presents the intrinsic methodology of $(\mathbb{Z}_{n\mathbb{Z}},\ F_\alpha)$ as an introductory example of the use of Θ-valent chrysippian modal logic in the construction, Θ-valent chrysippian mathematical structures. With the hope that these deploy hidden results in the essential and anatomical inadequacy of the bivalence of classical, unimodal logic.

Perhaps the most popular of all proofs of the Quadratic Reciprocity Law [6] is based on a result known as Gauss' Lemma. The purpose of this paper is to define on the $m\Theta$ set $\mathbb{Z}_{p\mathbb{Z}} - \mathbb{Z}$, a notion of the quadratic residues which respects its structure of $m\Theta$ set [9].

In the section 2, these are the preliminaries on the modal Θ-valent congruences of $(\mathbb{Z}_{n\mathbb{Z}},\ F_\alpha)$. Section 3 presents the notion of $m\Theta$ quadratic residues, afterwards the notion of p-valent modal quadratic character. Section 4 is devoted to establish the theorem for determining the $m\Theta$ quadratic character.

2. Preliminaries

2.1. The $m\Theta$ Set $(\mathbb{Z}_{n\mathbb{Z}}, F_\alpha)$ [13]

Let us set $x_{n\mathbb{Z}} = (p+\alpha r)_{\alpha\in I_*}$ where $x \in \mathbb{Z} \setminus n\mathbb{Z}$ $(x = pn+r;\ p,\ r \in \mathbb{Z};\ 1 \le r \le n-1)$.

$$x_{n\mathbb{Z}} \in \begin{cases} \mathbb{Z}^2 & if\ n = 2; \\ \mathbb{Z}^{n-1} & if\ n \ge 3. \end{cases}$$

Let us set

$$\mathbb{Z}_{n\mathbb{Z}} = \mathbb{Z} \cup \{x_{n\mathbb{Z}} : \neg\,(x \equiv 0\,(mod\,n))\}\,.$$

We define for all $\alpha \in I_*$;

$$\begin{array}{rccl} F_\alpha\colon & \mathbb{Z}_{n\mathbb{Z}} & \longrightarrow & \mathbb{Z}_{n\mathbb{Z}} \\ & a & \longmapsto & \begin{cases} a & if\ a \in \mathbb{Z} \\ b_1 + \alpha b_2 & if\ a = b_{n\mathbb{Z}},\ b \in \mathbb{Z}\setminus n\mathbb{Z} \end{cases} \end{array}$$

Where $b = b_1 n + b_2;\ b_2,\ b_1 \in \mathbb{Z};\ 1 \le b_2 \le n-1$.
$(\mathbb{Z}_{n\mathbb{Z}}, F_\alpha)$ is a $m\Theta$ set such that $\mathrm{C}(\mathbb{Z}_{n\mathbb{Z}}, F_\alpha) = \mathbb{Z}$.

2.2. The $m\Theta$ Congruences of $(\mathbb{Z}_{n\mathbb{Z}}, F_\alpha)$

Let $p \in \mathbb{N}^*$ and let ρ_p be defined on $\mathbb{Z}_{n\mathbb{Z}}$ as follows:

$$\forall x, y \in \mathbb{Z}_{n\mathbb{Z}}, x\rho_p y \Longleftrightarrow \forall \alpha \in I_*, F_\alpha x = F_\alpha y\,(mod\,p)\,.$$

Proposition 2.1. [14] ρ_p defined on $\mathbb{Z}_{n\mathbb{Z}}$ as above is an equivalence relation on $\mathbb{Z}_{n\mathbb{Z}}$ compatible with the structure of $m\Theta$ set $(\mathbb{Z}_{n\mathbb{Z}}, F_\alpha)$.

Proof [14]

Notation 2.1. We shall denote $x\rho_p y$ *by* $x \equiv y\,(p\mathbb{Z}_{n\mathbb{Z}})$.

Definition 2.1. [14] If $p \ge n$, we define the $m\Theta$ quotient of $(\mathbb{Z}_{n\mathbb{Z}}, F_\alpha)$ modulo $(p\mathbb{Z}_{n\mathbb{Z}})$as follows:

$$\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}} = \left\{\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}}; x \in \mathbb{Z}_{n\mathbb{Z}}\right\}.$$

Proposition 2.2. [15] $(\mathbb{Z}_{n\mathbb{Z}}, F_\alpha)$ is the $m\Theta$ set of $m\Theta$ relative integers.

$\forall \alpha \in I_*$;

$$\begin{array}{rccl} \frac{F_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}}\colon & \frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}} & \longrightarrow & \frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}} \\ & \frac{x}{p\mathbb{Z}_{n\mathbb{Z}}} & \longmapsto & \frac{F_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}}\left(\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}}\right) = \frac{F_\alpha x}{p\mathbb{Z}} \end{array}$$

Then $\left(\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}, \frac{F_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}}\right)$ is a $m\Theta$ set if and only if $p \ge n-1$.

Proof [15]

Lemma 2.1. [13] According to the proposition 2.2 above, the following axioms are equivalent:

1. $p \ge n-1$;
2. $\forall \alpha, \beta \in I_*,\ if\ \alpha \ne \beta$ then $\frac{F_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}} \ne \frac{F_\beta}{p\mathbb{Z}_{n\mathbb{Z}}}$.

Proof [13]

Proposition 2.3. If $2 \le n \le p$, then $(\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}, \frac{F_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}})$ is a $m\Theta s$ which contains np elements.

Proof Let us set $\mathbb{Z}_{0\Theta} = \mathbb{Z}$ and $\mathbb{Z}_{r\Theta} = \{x_{n\mathbb{Z}};\ x \in \mathbb{Z}\ and\ x \equiv r(mod\,n)\}$ with $1 \le r \le n-1$.

1. If $r \ne r' : 0 \le r,\ r' \le n-1,\ \mathbb{Z}_{r\Theta} \cap \mathbb{Z}_{r'\Theta} = \emptyset$.
   $\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}} = \cup_{r=0}^{n-1} \frac{\mathbb{Z}_{r\Theta}}{p\mathbb{Z}_{n\mathbb{Z}}}$ and $card\,\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}} = \sum_{r=1}^{n-1} card\,\frac{\mathbb{Z}_{r\Theta}}{p\mathbb{Z}_{n\mathbb{Z}}}$.
   In particular, $\frac{\mathbb{Z}_{0\Theta}}{p\mathbb{Z}_{n\mathbb{Z}}} = \frac{\mathbb{Z}}{p\mathbb{Z}_{n\mathbb{Z}}} = \frac{\mathbb{Z}}{p\mathbb{Z}}$; therefore $card\,\frac{\mathbb{Z}_{0\Theta}}{p\mathbb{Z}_{n\mathbb{Z}}} = p$.
2. If $x = qn + r$ and $y = q'n + r$; with $0 \le r \le n-1$, $\frac{x_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}, \frac{y_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}} \in \frac{\mathbb{Z}_{r\Theta}}{p\mathbb{Z}_{n\mathbb{Z}}} \Longleftrightarrow q \equiv q'(mod\,n)$; therefore $card\,\frac{\mathbb{Z}_{r\Theta}}{p\mathbb{Z}_{n\mathbb{Z}}} = p$.
   Hence,
$$card\,\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}} = np.$$

Proposition 2.4. [9] $\forall x, y \in \mathbb{Z}_{n\mathbb{Z}}$

1. If $x \in \mathbb{Z}$ and $x \equiv y\,(p\mathbb{Z}_{n\mathbb{Z}})$ then $y \in \mathbb{Z}$;
2. If $x \notin \mathbb{Z}$ and $x \equiv y\,(p\mathbb{Z}_{n\mathbb{Z}})$ then $y \notin \mathbb{Z}$.

Proof [9]

Proposition 2.5. [14] If $x, y \in \mathbb{Z}_{n\mathbb{Z}}$, the following axioms are equivalent:

1. $x \equiv y\,(p\mathbb{Z}_{n\mathbb{Z}})$;
2. $\begin{cases} x \equiv y\,(mod\,p) & if\ x \in \mathbb{Z}\ (therefore\, y \in \mathbb{Z})\,; \\ s\,(x) \equiv s\,(y)\,(mod\,np) & if\ x \notin \mathbb{Z}\ (therefore\, y \notin \mathbb{Z})\,. \end{cases}$

Proof [14]

Definition 2.2. [10] We shall call:

1. The $m\Theta$ congruence in $(\mathbb{Z}_{n\mathbb{Z}},\ F_\alpha)$, the $m\Theta$ equivalence relation denoted ρ_p, $p \in \mathbb{N}^*$ and defined as above.
2. A $m\Theta$ integer modulo p (a residual $m\Theta$ class modulo p), the class of equivalence modulo $p\mathbb{Z}_{n\mathbb{Z}}$ of every $x \in \mathbb{Z}_{n\mathbb{Z}}$ and denoted $\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}}$.
3. The set of $m\Theta$ integers modulo p, the $m\Theta$ set $\left(\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}; \frac{F_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}}\right)$.
4. The set of integers modulo p, the set: $\mathrm{C}\left(\frac{\mathbb{Z}_{n\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}; \frac{F_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}}\right) = \frac{\mathbb{Z}}{p\mathbb{Z}}$.
5. The α-modality of $\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}}$, the integer modulo p defined as follows:
   $\forall \alpha \in I_*$, $\frac{F_\alpha}{p\mathbb{Z}_{n\mathbb{Z}}}\left(\frac{x}{p\mathbb{Z}_{n\mathbb{Z}}}\right) = \frac{F_\alpha x}{p\mathbb{Z}} \in \frac{\mathbb{Z}}{p\mathbb{Z}}$.
6. A $m\Theta$ representative of $\frac{a}{p\mathbb{Z}_{n\mathbb{Z}}}$, $(a \in \mathbb{Z}_{n\mathbb{Z}})$, every b element of $\mathbb{Z}_{n\mathbb{Z}}$, defined as follows:
   - If $a \in \mathbb{Z}$ (therefore $b \in \mathbb{Z}$) and then $b \equiv a(mod\,np)$.
   - Otherwise $a \notin \mathbb{Z}$ (then $b \notin \mathbb{Z}$) and then $[s(a) \equiv s(b)(mod\,np) \Longleftrightarrow b \equiv a(p\mathbb{Z}_{n\mathbb{Z}})]$.

Proposition 2.6. If $a \equiv b(p\mathbb{Z}_{n\mathbb{Z}})$ and $a \equiv b(p'\mathbb{Z}_{n\mathbb{Z}})$ then $a \equiv b(l.c.m.\,(p,\,p')\mathbb{Z}_{n\mathbb{Z}})$.

Proof Indeed, if $a, b \in \mathbb{Z}$ $a \equiv b(p)$ et $a \equiv b(p')$ then $a \equiv b(l.c.m.\,(p,\,p'))$.

Otherwise, $a \equiv b(p\mathbb{Z}_{n\mathbb{Z}})$ and $a \equiv b(p'\mathbb{Z}_{n\mathbb{Z}})$. However $l.c.m.(np,\,np') = nl.c.m.(p,\,p')$ therefore $s(a) \equiv s(b)(n \times l.c.m.(p,\,p'))$.

So

$$a \equiv b(l.c.m.\,(p,\,p')\mathbb{Z}_{n\mathbb{Z}}).$$

Definition 2.3. [9] Let $a,\ b \in \mathbb{Z}_{n\mathbb{Z}}$. We say that a and b are s-coprime if $g.c.d.(s(a),\ s(b)) = 1$ or $g.c.d._{n\mathbb{Z}}(a,\ b) = 1_{n\mathbb{Z}}$.

2.3. Some Intrinsic $m\Theta$ Parameters of $\mathbb{Z}_{n\mathbb{Z}}$

In $\mathbb{Z}_{2\mathbb{Z}}$,$\rceil(5 \equiv 0(mod\,2))$ whereas $5! \equiv 0(mod\,2)$. In $\mathbb{Z}_{2\mathbb{Z}}$, $5! \in 2\mathbb{Z}$ whereas $5_{2\mathbb{Z}} \in \mathbb{Z}_{2\mathbb{Z}} - \mathbb{Z}$. In $\mathbb{Z}$, the notion of factorial

loses all interest as soon as $m \in \mathbb{Z}_{n\mathbb{Z}} - \mathbb{Z}$. It is therefore quite natural to define on $\mathbb{Z}_{n\mathbb{Z}}$ a factorial law appropriate to the structure $m\Theta s$.

Definition 2.4. [9] Let $m \in \mathbb{N}^*_{n\mathbb{Z}}$. We define factorial of m without n in $\mathbb{Z}_{n\mathbb{Z}}$ as the element of $\mathbb{N}_{n\mathbb{Z}}$ noted

1. $m! > n <$ if $m \in \mathbb{N}^*$ with the definition $m! > n <= m!$ devoid of any multiple factors of n;
2. $m!_{n\mathbb{Z}} > n <$ if $m \in \mathbb{N}_{n\mathbb{Z}} - \mathbb{N}$ with the definition

$$m!_{n\mathbb{Z}} > n <= [(s(m))! > n <]_{n\mathbb{Z}}.$$

Example 2.1. [9]

1. In $\mathbb{Z}_{2\mathbb{Z}}$, we have:

$$5_{2\mathbb{Z}}!_{2\mathbb{Z}} > 2 <= (5! > 2 <)_{2\mathbb{Z}} = (1 \times 3 \times 5)_{2\mathbb{Z}} = 15_{2\mathbb{Z}}.$$

2. In $\mathbb{Z}_{3\mathbb{Z}}$, we have:

$$5_{3\mathbb{Z}}!_{3\mathbb{Z}} > 3 <= (5! > 3 <)_{3\mathbb{Z}} = (1 \times 2 \times 4 \times 5)_{3\mathbb{Z}}.$$

Definition 2.5. Let $n, p \in \mathbb{N}$, $2 \leq n \leq p$; $p \neq 2$. p prime. $(\mathbb{Z}_{n\mathbb{Z}}, F_\alpha)$ a $m\Theta$ set. $a \in \mathbb{Z}_{n\mathbb{Z}} - \mathbb{Z}$ and $\rceil(p|s(a))$.
If $r, r' = 0, 1, 2, \cdots, n-1$, we define:

1. $\mathbb{N}_{r\,n} = \{a \in \mathbb{Z}_{n\mathbb{Z}} : s(a) \in \mathbb{N},\ s(a) \equiv r(mod\, n)\}$; if $r \neq r',\ \mathbb{N}_{r\,n} \cap \mathbb{N}_{r'\,n} = \emptyset$.
2. $\mathbb{N}_{r\,np} = \{a \in \mathbb{N}_{r\,n} : s(a) = kn + r,\ k = 0, 1, \cdots, p-1\}$. $\mathbb{N}_{n,\,p} = \cup_{r=0}^{n-1}\mathbb{N}_{r\,np}$ and $\mathbb{N}^*_{n,\,p} = \cup_{r=1}^{n-1}\mathbb{N}_{r\,np}$.
3. $card\,\mathbb{N}_{r\,np} = p$; $card\,\mathbb{N}_{n\,p} = np$; $card\,\mathbb{N}^*_{n,\,p} = (n-1)p$.

Observation 2.1. When $\frac{(\mathbb{Z}_{n\mathbb{Z}}, F_\alpha)}{p\mathbb{Z}_{n\mathbb{Z}}}$, the $m\Theta$ quotient of $(\mathbb{Z}_{n\mathbb{Z}}, F_\alpha)$ modulo $(p\mathbb{Z}_{n\mathbb{Z}})$ is defined, $\mathbb{N}_{n,\,p}$ is a complete system of $m\Theta$ residues modulo $p\mathbb{Z}_{n\mathbb{Z}}$. In general, $s(\mathbb{N}_{n,\,p}) = \{s(x),\ x \in \mathbb{N}_{n,\,p}\}$ is not a complete system of residues modulo np, prime with np. However, $s(\mathbb{N}^*_{n,\,p})$ is a complete system of residues modulo p^2, prime with p^2. In particular if p is prime, $p \geq 3$, $s(\mathbb{N}^*_{p,\,p})$ is a complete system of residues modulo p^2, prime with p^2.

In the whole sequence $n = p$ prime $p \geq 3$, because $\rceil(p|s(a))$ and $\rceil(p^2|s(a))$. So $\exists t_a \in \mathbb{N}^*_{p,\,p} : s(t_a) \equiv s(a)(mod\, p^2)$.

$\forall x \in \mathbb{N}^*_{p,\,p},\ \exists x' \in \mathbb{N}^*_{p,\,p} : s(x)s(x') \equiv s(a)(mod\, p^2)$ means that $s(xx') \equiv s(a)\,(mod\, p^2)$. Thus

$$x \in \mathbb{N}^*_{p,\,p} \Longrightarrow \exists x' \in \mathbb{N}^*_{p,\,p}\ such\ that\ xx' \equiv a(p\mathbb{Z}_{p\mathbb{Z}}).$$

3. $m\Theta$ Quadratic Residues

Definition 3.1. For p a prime, an $m\Theta$ integer $a \in \mathbb{Z}_{n\mathbb{Z}} - \mathbb{Z}$ such that $\rceil(p|s(a))$, is called a p-valent modal quadratic residue p, $aR_p\mathbb{Z}_{p\mathbb{Z}}$, if the congruence $x^2 \equiv a(p\mathbb{Z}_{p\mathbb{Z}})$ has a solution.

Otherwise it is called a p-valent modal quadratic nonresidue p, $aN_p\mathbb{Z}_{p\mathbb{Z}}$, this means that if $x \in \mathbb{N}^*_{p,\,p}$ then $\exists x' \in \mathbb{N}^*_{p,\,p} - \{x\}$ such that $xx' \equiv a(p\mathbb{Z}_{p\mathbb{Z}})$.

Remark 3.1. In either case, if $x, x' \in \mathbb{N}^*_{p,\,p}$ and $xx' \equiv a(p\mathbb{Z}_{p\mathbb{Z}})$, we say that x' is the p-valent modal associate of x with respect to p.

Theorem 3.1. Let $x \in \mathbb{N}^*_{p,\,p}$, p prime, and $a \in \mathbb{Z}_{n\mathbb{Z}} - \mathbb{Z}$ such that $\rceil(p|s(a))$. The congruence $x^2 \equiv a(p\mathbb{Z}_{p\mathbb{Z}})$ admits two solutions x_0 and $p^2 - x_0$ in $\mathbb{N}^*_{p,\,p}$.

Proof Indeed, $x^2 \equiv a(p\mathbb{Z}_{p\mathbb{Z}})$ means that $s(x^2) \equiv s(a)(mod\, p^2)$ therefore $(s(x))^2 \equiv s(a)(mod\, p^2)$.

$(s(p^2 - x))^2 = (p^2 - s(x))^2 = p^4 - 2p^2s(x) + (s(x))^2 \equiv s(a)(mod\, p^2)$, thus $(s(p^2 - x))^2 \equiv s(a)(mod\, p^2) \Longrightarrow p^2 - x \equiv a(p\mathbb{Z}_{p\mathbb{Z}})$. If $x^2 \equiv a(p\mathbb{Z}_{p\mathbb{Z}})$ then $(p^2 - x)^2 \equiv a(p\mathbb{Z}_{p\mathbb{Z}})$. So the congruence $x^2 \equiv a(p\mathbb{Z}_{p\mathbb{Z}})$ admits two solutions in $\mathbb{N}^*_{p,\,p}$.

Conversely if x_1 and x_2 are two solutions modulo $(p\mathbb{Z}_{p\mathbb{Z}})$ of $x^2 \equiv a(p\mathbb{Z}_{p\mathbb{Z}})$ that is $x_1^2 \equiv a(p\mathbb{Z}_{p\mathbb{Z}})$ and $x_2^2 \equiv a(p\mathbb{Z}_{p\mathbb{Z}})$. $(s(x_1))^2 \equiv s(a)(mod\, p^2)$ and $(s(x_2))^2 \equiv s(a)(mod\, p^2)$.

Thus, $(s(x_2))^2 - (s(x_1))^2 = (s(x_2) + s(x_1))(s(x_2) - s(x_1)) \equiv 0(mod\, p^2)$. So, either $x_2 \equiv x_1(p\mathbb{Z}_{p\mathbb{Z}})$ or $x_2 \equiv -x_1(p\mathbb{Z}_{p\mathbb{Z}}) \equiv p^2 - x(p\mathbb{Z}_{p\mathbb{Z}})$.

Remark 3.2. In extension, we have:

$$s(\mathbb{N}^*_{p,\,p}) = \{s(x_1),\ p^2 - s(x_1)\} \cup (\bigcup_{i=1}^{\frac{p(p-1)-2}{2}} \{s(y_i),\ s(y_i')\}).$$

$\forall i \in \{1, \cdots, \frac{p(p-1)-2}{2}\},\ y_i, y_i' \in \mathbb{N}^*_{p,\,p} - \{x_1,\ p^2 - x_1\};\ y_i \neq y_i'\ such\ that\ s(y_i)s(y_i') \equiv s(a)(mod\, p^2)$.
Thus $s(x_1) \equiv s(x_1)(mod\, p^2)$, $p^2 - s(x_1) \equiv -s(x_1)(mod\, p^2)$ means that

$$s(x_1)(p^2 - s(x_1)) \equiv -(s(x_1))^2 \equiv -s(a)(mod\, p^2).$$

It follows that

$$\prod_{i=1}^{\frac{p(p-1)-2}{2}} s(y_i)s(y_i') \equiv s(a)^{\frac{p(p-1)-2}{2}}(mod\, p^2),$$

with

$$s(a)s(a)^{\frac{p(p-1)-2}{2}} = s(a)^{\frac{p(p-1)}{2}}.$$

Corollary 3.1. If there is $x \in \mathbb{N}^*_{p,\,p}$ such that $x^2 \equiv a(p\mathbb{Z}_{p\mathbb{Z}})$ then

$$\prod_{x\in\mathbb{N}^*_{p,\,p}} x \equiv -a^{\frac{p(p-1)}{2}}(p\mathbb{Z}_{p\mathbb{Z}}).$$

Proof According to the previous remark

$$\mathbb{N}^*_{p,\,p} = \{x_1,\, p^2 - x_1\} \cup \Big(\bigcup_{i=1}^{\frac{p(p-1)-2}{2}} \{y_i,\, y_i'\}\Big).$$

Thus, $\prod_{x\in\mathbb{N}^*_{p,\,p}} s(x) \equiv s(x_1)s(p^2-x_1)\prod_{i=1}^{\frac{p(p-1)-2}{2}} s(y_i)s(y_i') \equiv -s(a)^{\frac{p(p-1)}{2}}(p\mathbb{Z}_{p\mathbb{Z}})$.
So,

$$\prod_{x\in\mathbb{N}^*_{p,\,p}} x \equiv -a^{\frac{p(p-1)}{2}}(p\mathbb{Z}_{p\mathbb{Z}}).$$

3.1. p-valent Modal Quadratic Character

The data remains the same: $3 \leq p$, p prime and $a \in \mathbb{Z}_{p\mathbb{Z}} - \mathbb{Z} : \urcorner(p|s(a)) \Longrightarrow \urcorner(p^2|s(a))$. We have the following equivalence:

1. a p-valent modal quadratic residue of p;
2. $s(a)$ quadratic residue of p^2.

We thus have the following definition

$$\left(\frac{s(a)}{p^2}\right) = \begin{cases} 1 & \text{if } s(a)Rp^2 \\ -1 & \text{if } s(a)Np^2 \end{cases}$$

Definition 3.2. We call p-valent modal quadratic character of a relatively to p the element of $\mathbb{Z}_{p\mathbb{Z}}$ denoted $\left(\frac{a}{p}\right)_{p\mathbb{Z}}$ and defined as follows

$$\left(\frac{a}{p}\right)_{p\mathbb{Z}} = \begin{cases} 1_{p\mathbb{Z}} & \text{if } aRp\mathbb{Z}_{p\mathbb{Z}} \\ (-1)_{p\mathbb{Z}} & \text{if } aNp\mathbb{Z}_{p\mathbb{Z}} \end{cases}$$

By definition

$$\left(\frac{s(a)}{p^2}\right) = s\left(\frac{a}{p}\right)_{p\mathbb{Z}}.$$

Remark 3.3.
1. If $a \equiv b(p\mathbb{Z}_{p\mathbb{Z}})$ then $\left(\frac{b}{p}\right)_{p\mathbb{Z}} = \left(\frac{a}{p}\right)_{p\mathbb{Z}}$.
2. if $aRp\mathbb{Z}_{p\mathbb{Z}}$ then $\prod_{x\in\mathbb{N}^*_{p,\,p}} x \equiv -\left(\frac{a}{p}\right)_{p\mathbb{Z}} a^{\frac{p(p-1)}{2}}(p\mathbb{Z}_{p\mathbb{Z}})$.
   If $a = 1_{p\mathbb{Z}}$, $1^2_{p\mathbb{Z}} = 1_{p\mathbb{Z}}$ so $1^2_{p\mathbb{Z}} \equiv 1_{p\mathbb{Z}}(p\mathbb{Z}_{p\mathbb{Z}})$, $1_{p\mathbb{Z}}Rp\mathbb{Z}_{p\mathbb{Z}}$ and thus $\left(\frac{1_{p\mathbb{Z}}}{p}\right) = 1_{p\mathbb{Z}}$.
   Therefore

$$\prod_{x\in\mathbb{N}^*_{p,\,p}} x \equiv -1_{p\mathbb{Z}}(p\mathbb{Z}_{p\mathbb{Z}}).$$

Theorem 3.2. It follows that

$$\left(\frac{1_{p\mathbb{Z}}}{p}\right)_{p\mathbb{Z}} \equiv 1_{p\mathbb{Z}}(p\mathbb{Z}_{p\mathbb{Z}}), \qquad \left(\frac{-1_{p\mathbb{Z}}}{p}\right)_{p\mathbb{Z}} \equiv (-1_{p\mathbb{Z}})^{\frac{p(p-1)}{2}}(p\mathbb{Z}_{p\mathbb{Z}}).$$

Proof We know that $\prod_{x\in\mathbb{N}^*_{p,\,p}} x \equiv -a^{\frac{p(p-1)}{2}}(p\mathbb{Z}_{p\mathbb{Z}}) \equiv -\left(\frac{a}{p}\right)_{p\mathbb{Z}} a^{\frac{p(p-1)}{2}}(p\mathbb{Z}_{p\mathbb{Z}})$ and $\prod_{x\in\mathbb{N}^*_{p,\,p}} x \equiv -1_{p\mathbb{Z}}(p\mathbb{Z}_{p\mathbb{Z}})$,. So

$$\left(\frac{a}{p}\right)_{p\mathbb{Z}} a^{\frac{p(p-1)}{2}} \equiv -1_{p\mathbb{Z}}(p\mathbb{Z}_{p\mathbb{Z}}).$$

If $a = 1_{p\mathbb{Z}}$, we have $\left(\frac{1_{p\mathbb{Z}}}{p}\right)_{p\mathbb{Z}} \equiv 1_{p\mathbb{Z}}(p\mathbb{Z}_{p\mathbb{Z}})$ and $\left(\frac{1}{p^2}\right) \equiv 1(mod\, p^2)$.
If $a = -1_{p\mathbb{Z}}$, we have $\left(\frac{-1_{p\mathbb{Z}}}{p}\right)_{p\mathbb{Z}} \equiv (-1_{p\mathbb{Z}})^{\frac{p(p-1)}{2}}(p\mathbb{Z}_{p\mathbb{Z}})$ and $\left(\frac{-1}{p^2}\right) \equiv (-1)^{\frac{p(p-1)}{2}}(mod\, p^2)$.

Observation 3.1.

$$\max s(\mathbb{N}^*_{p,\,p}) = p(p-1)+p-1 = p^2-1.$$

Example 3.1. $\prod_{x\in\mathbb{N}^*_{p,\,p}} x = (p^2-1)_{p\mathbb{Z}}!_{p\mathbb{Z}} > p <= ((p^2-1)! > p <)_{p\mathbb{Z}}$ and $\prod_{x\in\mathbb{N}^*_{p,\,p}} s(x) = (p^2-1)! > p <$. For $p=3$,

$$\begin{aligned}\mathbb{N}^*_{3,\,3} &= \{x_{3\mathbb{Z}} > 3 <\}\\ &= \{1_{3\mathbb{Z}},\, 2_{3\mathbb{Z}},\, 4_{3\mathbb{Z}},\, 5_{3\mathbb{Z}},\, 7_{3\mathbb{Z}},\, 8_{3\mathbb{Z}}\}\end{aligned}$$

$$\begin{aligned}\prod_{x\in\mathbb{N}^*_{3,\,3}} x &= (3^2-1)_{3\mathbb{Z}}!_{3\mathbb{Z}} > p <= ((3^2-1)! > 3 <)_{3\mathbb{Z}}\\ &= (1\times 2\times 4\times 5\times 7\times 8)_{3\mathbb{Z}} \equiv -1_{3\mathbb{Z}}(3\mathbb{Z}_{3\mathbb{Z}})\end{aligned}$$

3.2. p-valent Modal Quadratic Residue of p^k

Definition 3.3. More generally, if $3 \le p$, p prime, $\forall k \in \mathbb{N}^*$ we note respectively:

1. $\mathbb{N}_{0pp^k} = \mathbb{N}_{p^k-1} = \{0,\, 1,\, \cdots,\, p^k-1\}$.
2. $\mathbb{N}_{rpp^k} = \{a \in \mathbb{N}_{r\,p} :\ s(a) = k'p + r;\, k' = 0,\, 1,\, \cdots,\, p-1,\, \cdots,\, p^k-1\}$. If $r \in \{1,\, \cdots,\, p-1\}$, $\mathbb{N}_{r\,p} = \{a \in \mathbb{Z}_{p\mathbb{Z}} - \mathbb{Z};\ s(a) \in \mathbb{N},\ s(a) \equiv r(mod\, p)\}$.
3. $\mathbb{N}_{pp^k} = \bigcup_{r=0}^{p-1} \mathbb{N}_{rpp^k}$; $\mathbb{N}^*_{p,\,p^k} = \bigcup_{r=1}^{p-1} \mathbb{N}_{rpp^k}$.

We have $card\,\mathbb{N}_{rpp^k} = p^k$, $card\,\mathbb{N}_{pp^k} = p^{k+1}$, $card\,\mathbb{N}^*_{p,\,p^k} = (p-1)p^k$.

$\mathbb{N}^*_{p,\,p^k}$ is a complete system of p-valent modal residues modulo $p^k\mathbb{Z}_{p\mathbb{Z}}$. $s(\mathbb{N}^*_{p,\,p^k})$ is a complete system of residues modulo p^{k+1} prime with p^{k+1}. Thus if $x \in s(\mathbb{N}^*_{p,\,p^k})$, $s(x\mathbb{N}^*_{p,\,p^k})$ also is a complete system of residues modulo p^{k+1} prime with p^{k+1}. So, if $a \in \mathbb{Z}_{p\mathbb{Z}} - \mathbb{Z}$ and $\rceil(p|s(a))$, $\rceil(p^k|s(a))$: $\forall x \in \mathbb{N}^*_{p,\,p^k}$, $\exists x' \in \mathbb{N}^*_{p,\,p^k}$ such that $s(xx') \equiv s(a)(mod\, p^{k+1})$. Therefore,

$$xx' \equiv a(mod\, p^k\mathbb{Z}_{p\mathbb{Z}}).$$

Definition 3.4. We say that a is:

1. p-valent modal quadratic residue of p^k if and only if $\exists x \in \mathbb{N}^*_{p,\,p^k} :\ x^2 \equiv a(mod\, p^k\mathbb{Z}_{p\mathbb{Z}})$.
2. non p-valent modal quadratic residue of p^k if and only if $\forall x \in \mathbb{N}^*_{p,\,p^k}$, $\exists x' \in \mathbb{N}^*_{p,\,p^k} - \{x\}$ such that $xx' \equiv a(mod\, p^k\mathbb{Z}_{p\mathbb{Z}})$.

Observation 3.2. We observe that the congruence $x^2 \equiv a(mod\, p^k\mathbb{Z}_{p\mathbb{Z}})$ admits two solutions in $\mathbb{N}^*_{p,\,p^k}$ if we can find x_1 in $\mathbb{N}^*_{p,\,p^k}$ such that $x_1^2 \equiv a(mod\, p^k\mathbb{Z}_{p\mathbb{Z}})$. Then we get two cases: either $\exists x \in \mathbb{N}^*_{p,\,p^k}$, $x^2 \equiv a(mod\, p^k\mathbb{Z}_{p\mathbb{Z}})$ and $\prod_{x\in\mathbb{N}^*_{p,\,p^k}} s(x) \equiv -s(a)^{\frac{(p-1)p^k}{2}}(mod\, p^{k+1})$ so $\prod_{x\in\mathbb{N}^*_{p,\,p^k}} x \equiv -a^{\frac{(p-1)p^k}{2}}(mod\, p^k\mathbb{Z}_{p\mathbb{Z}})$; or $\forall x \in \mathbb{N}^*_{p,\,p^k}$, $\exists x \in \mathbb{N}^*_{p,\,p^k} - \{x\}$ such that $xx' \equiv a(mod\, p^k\mathbb{Z}_{p\mathbb{Z}})$.

In either case, x' ($x' = x\ or\ x' \ne x$) is said to be the p-valent modal associate of x with respect to p^k.

But in this second case ($x' \ne x$)

$\prod_{x\in\mathbb{N}^*_{p,\,p^k}} s(x) \equiv s(a)^{\frac{(p-1)p^k}{2}}(mod\, p^{k+1})$;

$\prod_{x\in\mathbb{N}^*_{p,\,p^k}} x \equiv a^{\frac{(p-1)p^k}{2}}(mod\, p^k\mathbb{Z}_{p\mathbb{Z}})$.

Definition 3.5. We call:

1. quadratic character of $s(a)$ relatively to p^{k+1}

$$\left(\frac{s(a)}{p^{k+1}}\right) = \begin{cases} 1 & \text{if } s(a)Rp^{k+1}\\ -1 & \text{if } s(a)Np^{k+1}\end{cases}$$

2. p-valent modal quadratic character of a with to p^k. It is the element of $\mathbb{Z}_{p\mathbb{Z}}$ denoted $\left(\frac{a}{p^k}\right)_{p\mathbb{Z}}$ and defined as follows:

$$\left(\frac{a}{p^k}\right)_{p\mathbb{Z}} = \begin{cases} 1_{p\mathbb{Z}} & \text{if } aRp^k\mathbb{Z}_{p\mathbb{Z}}\\ -1_{p\mathbb{Z}} & \text{if } aNp^k\mathbb{Z}_{p\mathbb{Z}}\end{cases}$$

Remark 3.4. We have

$$s\left(\frac{a}{p^k}\right)_{p\mathbb{Z}} = \left(\frac{s(a)}{p^{k+1}}\right).$$

If $a \equiv b((mod\, p^k\mathbb{Z}_{p\mathbb{Z}})$, then $\left(\frac{a}{p^k}\right)_{p\mathbb{Z}} = \left(\frac{b}{p^k}\right)_{p\mathbb{Z}}$.

Theorem 3.3. It follows that

$$\left(\frac{1_{p\mathbb{Z}}}{p^k}\right)_{p\mathbb{Z}} \equiv 1_{p\mathbb{Z}}(p^k\mathbb{Z}_{p\mathbb{Z}}),\ \ \left(\frac{-1_{p\mathbb{Z}}}{p^k}\right)_{p\mathbb{Z}} \equiv (-1_{p\mathbb{Z}})^{\frac{p^k(p-1)}{2}}(p^k\mathbb{Z}_{p\mathbb{Z}}).$$

Proof We know that $\prod_{x\in\mathbb{N}^*_{p,\,p^k}} x \equiv -a^{\frac{p^k(p-1)}{2}}(p^k\mathbb{Z}_{p\mathbb{Z}}) \equiv -\left(\frac{a}{p^k}\right)_{p\mathbb{Z}} a^{\frac{p^k(p-1)}{2}}(p^k\mathbb{Z}_{p\mathbb{Z}})$ and $\prod_{x\in\mathbb{N}^*_{p,\,p^k}} x \equiv -1_{p\mathbb{Z}}(p^k\mathbb{Z}_{p\mathbb{Z}})$. So

$$\left(\frac{a}{p^k}\right)_{p\mathbb{Z}} a^{\frac{p^k(p-1)}{2}} \equiv -1_{p\mathbb{Z}}(p^k\mathbb{Z}_{p\mathbb{Z}}).$$

If $a = 1_{p\mathbb{Z}}$, we have $\left(\frac{1_{p\mathbb{Z}}}{p^k}\right)_{p\mathbb{Z}} \equiv 1_{p\mathbb{Z}}(p^k\mathbb{Z}_{p\mathbb{Z}})$ and $\left(\frac{1}{p^k}\right) \equiv 1(mod\, p^{k+1})$.

If $a = -1_{p\mathbb{Z}}$, we have $\left(\frac{-1_{p\mathbb{Z}}}{p^k}\right)_{p\mathbb{Z}} \equiv (-1_{p\mathbb{Z}})^{\frac{p^k(p-1)}{2}}(p^k\mathbb{Z}_{p\mathbb{Z}})$ and $\left(\frac{-1}{p^k}\right) \equiv (-1)^{\frac{p^k(p-1)}{2}}(mod\, p^{k+1})$.

Observation 3.3. $\max \mathbb{N}^*_{p,\, p^k} = p^k(p-1) + p^k - 1 = p^{k+1} - 1$,

$$\prod_{x \in \mathbb{N}^*_{p,\, p^k}} x \equiv \left[(p^{k+1}-1)! > p < \right]_{p\mathbb{Z}}.$$

Remark 3.5. $\left((p^{k+1}-1)! > p < \right)_{p\mathbb{Z}} \equiv -1_{p\mathbb{Z}}(p^k\mathbb{Z}_{p\mathbb{Z}})$ and $(p^{k+1}-1)! > p < \equiv -1(mod\, p^{k+1})$.

None of these results is remotely Wilson's theorem.

4. Theorem for Determining the $m\Theta$ Quadratic Character

The data is the same $p \in \mathbb{N}^*$ $p \geq 3$, p prime; $k \in \mathbb{N}^*$; $a \in \mathbb{Z}_{p\mathbb{Z}} - \mathbb{Z}$ and $\rceil(p|s(a))$.

Definition 4.1. $s(a)$ admits a unique residue modulo p^{k+1} comprised between $-\frac{1}{2}p^{k+1}$ and $\frac{1}{2}p^{k+1}$, because $-\frac{1}{2}p^{k+1} + p^{k+1} = \frac{1}{2}p^{k+1}$, called minimal residue of $s(a)$ modulo p^{k+1}.

Observation 4.1.
1. It is positive if the smallest positive residue of $s(a)$ modulo p^{k+1} is between 0 and $\frac{1}{2}p^{k+1}$ and it is the smallest positive residue.
2. It is negative if the smallest positive residue of $s(a)$ modulo p^{k+1} is between $\frac{1}{2}p^{k+1}$ and p^{k+1} and it is then the opposite of this smallest residue.

The following theorem is a non-classical version of Gauss's lemma, it is the theorem for determining the p-valent modal quadratic character of $a \in \mathbb{Z}_{p\mathbb{Z}} - \mathbb{Z}$ with respect to p^k.

Theorem 4.1. Let $p \geq 3$, p prime; $k \in \mathbb{N}^*$; $a \in \mathbb{Z}_{p\mathbb{Z}} - \mathbb{Z}$ such that $\rceil(p|s(a))$;

$$\left(\frac{a}{p^k}\right)_{p\mathbb{Z}} = (-1)^{\mu_{pk}}_{p\mathbb{Z}}$$

μ_{pk} is the number of $qs(a)$, $1 \leq q \leq \frac{1}{2}(p-1)p^k$, whose smallest residue modulo p^{k+1} is greater than $\frac{1}{2}p^{k+1}$.

Proof Through observation 4.1, we can consider the $\frac{1}{2}(p-1)p^k$ elements of $\mathbb{Z}_{p\mathbb{Z}} - \mathbb{Z}$ as follows

$$\{aq : q = 1, 2, \cdots, \frac{1}{2}(p-1)p^k\}.$$

We have two cases:
1. $r_1, r_2, \cdots, r_{\lambda_{pk}}$ the minimum residues modulo p^{k+1} of the $qs(a)$ of smallest positive residue modulo p^{k+1} less than $\frac{1}{2}p^{k+1}$.
2. $-r'_1, -r'_2, \cdots, -r'_{\mu_{pk}}$ the minimum residues modulo p^{k+1} of the $qs(a)$ of smallest positive residue modulo p^{k+1} greater than $\frac{1}{2}p^{k+1}$.

We thus have $\lambda_{pk} + \mu_{pk} = \frac{1}{2}(p-1)p^k$.

$$\begin{aligned} \forall i, j;\ if\, i \neq j \qquad & \rceil\left(r_i \equiv r'_j\, (mod\, p^{k+1})\right) \\ & \rceil\left(r_i \equiv r_j\, (mod\, p^{k+1})\right) \\ & \rceil\left(r'_i \equiv r'_j\, (mod\, p^{k+1})\right) \end{aligned}$$

Consequently, $r_1, r_2, \cdots, r_{\lambda_{pk}}, -r'_1, -r'_2, \cdots, -r'_{\mu_{pk}}$ is a rearrangement of the integers q: $q = 1, 2, \cdots, \frac{1}{2}(p-1)p^k$. Since

$$\begin{aligned} \prod_{q=1}^{\frac{1}{2}(p-1)p^k} (qs(a)) &= (s(a))^{\frac{1}{2}(p-1)p^k} \cdot \left(\frac{1}{2}(p-1)p^k\right)! \\ &\equiv \prod_{i=1}^{\lambda_{pk}} r_i \prod_{j=1}^{\mu_{pk}} (-r'_j)(mod\, p^{k+1}) \\ &\equiv (-1)^{\mu_{pk}}\left(\frac{1}{2}(p-1)p^k\right)! \end{aligned}$$

so $(s(a))^{\frac{1}{2}(p-1)p^k} \equiv (-1)^{\mu_{pk}}\, (mod\, p^{k+1})$ and $a^{\frac{1}{2}(p-1)p^k} \equiv (-1)^{\mu_{pk}}\, (mod\, p^k\mathbb{Z}_{p\mathbb{Z}})$. Or, $a^{\frac{1}{2}(p-1)p^k} \equiv \left(\frac{a}{p^k}\right)_{p\mathbb{Z}} (mod\, p^k\mathbb{Z}_{p\mathbb{Z}})$, therefore $\left(\frac{a}{p^k}\right)_{p\mathbb{Z}} \equiv (-1)^{\mu_{pk}}_{p\mathbb{Z}}\, (mod\, p^k\mathbb{Z}_{p\mathbb{Z}})$.

By definition, $\left(\frac{a}{p^k}\right)_{p\mathbb{Z}} \in \{1_{p\mathbb{Z}}, -1_{p\mathbb{Z}}\}$ then

$$\left(\frac{a}{p^k}\right)_{p\mathbb{Z}} = (-1)^{\mu_{pk}}_{p\mathbb{Z}}.$$

Example 4.1. If $a = 2_{p\mathbb{Z}}$, $p \geq 3$ then

$$\begin{aligned}\{qs(a) : q = 1, 2, \cdots, \frac{1}{2}(p-1)p^k\} &= \\ \{2q : q = 1, 2, \cdots, \frac{1}{2}(p-1)p^k\} &= \{2, 4, \cdots, (p-1)p^k\}.\end{aligned}$$

Obviously, $\lambda_{pk} = \frac{1}{2}\left[\frac{1}{2}p^{k+1}\right]$, where $[x]$ denotes the integer value of x. So, $\lambda_{pk} = \left[\frac{1}{4}p^{k+1}\right]$ and $\lambda_{pk} = \frac{1}{2}(p-1)p^k - \left[\frac{1}{4}p^{k+1}\right]$. Since $p \geq 3$:

1. Either $p \equiv 1(mod\,4)$, so $p = 4m+1$, $p^k \equiv p^{k+1} \equiv 1(mod\,4)$.
   $p^{k+1} = 4n+1$ thus $\frac{1}{4}p^{k+1} = n + \frac{1}{4}$ and $\left[\frac{1}{4}p^{k+1}\right] = n = \frac{p^{k+1}-1}{4}$.
   Thus if $p \equiv 1(mod\,4)$ then $\mu_{pk} = (p^{k+1} - 2p^k + 1)$.
2. Or $p \equiv 3(mod\,4)$, $p^k \equiv 1(mod\,4)$; $p^{k+1} \equiv 3(mod\,4)$ respectively if $k \equiv 0(mod\,2)$, $k \equiv 1(mod\,2)$.
   - if $k \equiv 0(mod\,2)$,
     $p^{k+1} \equiv 1(mod\,4)$ $p^k = 4n+1$; $p^{k+1} \equiv 3(mod\,4)$, $p^{k+1} = 4m+3$; $\left[\frac{1}{4}p^{k+1}\right] = m = \frac{p^{k+1}-3}{4}$. So $\mu_{pk} = \frac{1}{4}(p^{k+1} - 2p^k + 3)$, $p \equiv 3(mod\,4)$,
     $k \equiv 0(mod\,2)$.
   - If $k \equiv 1(mod\,2)$, $p^k \equiv 3(mod\,4)$, $p^{k+1} \equiv 1(mod\,4)$
     $p^{k+1} = 4m'+1$, $\left[\frac{1}{4}p^{k+1}\right] = m' = \frac{p^{k+1}-3}{4}$. Then $\mu_{pk} = \frac{1}{4}(p^{k+1} - 2p^k + 3)$, $p \equiv 3(mod\,4)$,
     $k \equiv 1(mod\,2)$.

   Since $\left(\frac{2}{p^{k+1}}\right) = (-1)^{\mu_{pk}}$, $\left(\frac{2}{p^{k+1}}\right) = 1 \Longleftrightarrow (-1)^{\mu_{pk}} = 1 \Longleftrightarrow \mu_{pk} \equiv 0(mod\,2)$.
3. If $p \equiv 1(mod\,4)$ then $\frac{1}{4}(p^{k+1} - 2p^k + 3) \equiv 0(mod\,2)$, $p^{k+1} - 2p^k + 3 \equiv 0(mod\,8)$.
   Thus, $\left(\frac{2}{p^{k+1}}\right) = 1$ and $p \equiv 1(mod\,4) \Longrightarrow p^{k+1} - 2p^k + 1 \equiv 0(mod\,8)$, $p \equiv 1(mod\,4)$.

5. Conclusion

This note shows that the study of the notion of quadratic residues [4, 6] on the $m\Theta$ set $\mathbb{Z}_{p\mathbb{Z}} - \mathbb{Z}$, p prime, leads to the notion of p-valent modal quadratic character. The p-valent modal quadratic character is a Θ-valent modal version of Legendre's symbol [8]. The results contained in this article have no place in classical arithmetic [5], however constitute an extension in $\mathbb{Z}_{p\mathbb{Z}}$. These results are also widely used in the intrinsic arithmetic of $\mathbb{Z}_{n\mathbb{Z}}$ namely the Fermat-Euler theorem in $\mathbb{Z}_{p\mathbb{Z}}$, in quotient p-valent modal rings.
At the end of this study, some interesting problems remain to be solved:

1. We would like to establish the $m\Theta$ quadratic reciprocity law and give it a proof by the Gauss's Lemma.
2. We should give a suggestive description of $m\Theta$ Euler's function and $m\Theta$ Möbius function.

Acknowledgements

The authors address their thanks to the reviewers for their valuable suggestions and comments.

References

[1] P. Mooree, P. Stevenhagen, Prime divisors of Lucas sequences, Acta Arith. 82, (1997), 403-410.

[2] T. Ono, An introduction to algebraic number theory, New York, 1990.

[3] F. Nemenzo, H. Wada, An elementary proof of Gauss' genus theorem, Proc. Japan Acad. Sci. 68 (1992), 94-95.

[4] F. Lemmermeyer, Reciprocity Laws: From Euler to Eisenstein, Springer, Berlin, 2000.

[5] C. F. Gauss, Untersuchungen $\ddot{U}$ber hohere Arithmetik (trans. H. Maser) , American Mathematical Society, 2006.

[6] Steve Wright, Quadratic Residues and Non-Residues, Lecture Notes in Mathematics, LNM, Volume 2171, 2016.

[7] FL Tiplea, S. Iftene, G Teseleanu, On the distribution of quadratic residues and non-residues modulo composite integers and applications to cryptography, Applied Mathematics and Computation 372, 124993, 2020-Elsevier.

[8] C. Monico, M. Elia, Note on an additive characterization of quadratic residues modulo p, Journal of Combinatorics, Information and System Sciences 31, 209-215, 2006.

[9] F. Ayissi Eteme, Logique et Algèbre de structures mathématiques modales Θ-valentes chrysippiennes, Edition Hermann, Paris, 2009.

[10] F. Ayissi Eteme, Anneau chrysippien Θ-valent, CRAS, Paris 298, série 1, 1984, pp. 1-4.

[11] FL Tiplea, A brief introduction of quadratic residuosity based cryptography, Math. Pures Appl, 2021.

[12] F. L. Tiplea, Efficient Generation of Roots of Power Residues modulo Powers of Two , 10 (6), 908, March 2022.

[13] J. A. Tsimi and G. Pemha, A mΘ spectrum of Reed-Muller codes, Journal of Discrete Mathematical Sciences and Cryptography (JDMSC), 2021.

[14] J. A. Tsimi and G. Pemha, An algorithm of Decoding of $m\Theta$ Reed-Muller codes, Journal of Discrete Mathematical Sciences and Cryptography (JDMSC), 2021.

[15] J. A. Tsimi and G. Pemha, On the Generalized modal Θ-valent Reed-Muller codes, Journal of Information and Optimization Sciences (JIOS), 2021.

[16] F. Lemmermeyer, Hermite's identity and the quadratic reciprocity law, Elem. Math. July 2022.