International Journal of Pure and Applied Mathematics

Volume 59 No. 1 2010, 59-75

SOME NEW LOWER BOUNDS FOR THE NUMBER OF NEAR-RINGS ON FINITE CYCLIC GROUPS

A.K. Rahnev[1 §], A.A. Golev[2]

[1,2]Faculty of Mathematics and Informatics
University of Plovdiv
236, Bulgaria Blvd., Plovdiv, 4003, BULGARIA
[1]e-mail: assen@uni-plovdiv.bg
[2]e-mail: angelg@uni-plovdiv.bg

Abstract: New lower bounds for the number of the near-rings on finite cyclic groups are obtained. All near-rings on finite cyclic groups of order up to 23 are computed using a new heuristic algorithm. The constructions of more than 98 percents of the zero-symmetric and more than 99.5 percents of the non-zero-symmetric near-rings are described.

AMS Subject Classification: 16Y30
Key Words: near-ring, finite cyclic group, lower bound

1. Introduction

An algebraic system $(G, +, *)$ is a *(left) near-ring* on $(G, +)$, if $(G, +)$ is a group, $(G, *)$ is a semigroup and $a * (b + c) = a * b + a * c$ for $a, b, c \in G$. The left distributive law yields $x * 0 = 0$ for $x \in G$. A near-ring $(G, +, *)$ is called *zero-symmetric*, if $0 * x = 0$ holds for $x \in G$.

J.R. Clay initiated the study of near-rings, whose additive groups are finite cyclic in 1964 (see [2]). Some sufficient conditions for the construction of near-rings on any finite cyclic groups were obtained. In 1968 all near-rings on cyclic groups of order up to 7 were computed (see [3]). Later all near-rings on cyclic groups of order 8 (see [5]), of order up to 12 (see [10]), of order up to 13 (see [8]), of order up to 15 (see [1]) as well as of order up to 24 (see [7]) were computed.

Received: January 10, 2010

§Correspondence author

We will assume G coincides with the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, $2 \leq n < \infty$ since every cyclic group of order n is isomorphic to the group of the remainders of modulo n. We will denote the functions mapping $\mathbb{Z}_n$ into itself by π, and the addition and the multiplication modulo n we will denote by $+$ and $\cdot$ respectively. The equality $c = a \cdot b$ will be equivalent to the congruence $ab \equiv c \pmod{n}$.

It is known that there exists a bijective correspondence between left distributive binary operations $*$ defined on $\mathbb{Z}_n$ and the n^n functions π mapping $\mathbb{Z}_n$ into itself. If $r * 1 = b$ defines the function $\pi(r) = b$, then according to [2, Theorem II], the binary operation $*$ is a left distributive exactly when, for any $x, y \in \mathbb{Z}_n$, the equality

$$\pi(x) \cdot \pi(y) = \pi(x \cdot \pi(y)) \tag{1}$$

holds.

Denote the set of all functions π, defined above and for which the equality (1) holds, by Ω.

According to the above result, the obtaining of the near-rings on $\mathbb{Z}_n$ is equivalent to obtaining the functions π such that equation (1) holds.

2. Known Lower Bounds for Near-Rings on Finite Cyclic Groups

Now we will set up some known in the literature results.

Theorem 1. (see [2]) *For $n>2$ there are at least 2^{n-1} zero-symmetric near-rings on $\mathbb{Z}_n$.*

Theorem 2. (see [8]) *For $n>2$ there are at least:*

1) $3^{\lfloor \frac{n-1}{2} \rfloor} - 1$ zero-symmetric near-rings on $\mathbb{Z}_n$, that are different than those described in Theorem 1;

2) $\sum_s 2^{n - \frac{n}{(n,s)}}$ non-zero-symmetric near-rings on $\mathbb{Z}_n$, where s is an arbitrary idempotent modulo n.

Theorem 3. (see [9]) *Let $n = p_1 p_2 \ldots p_s$, where $p_1, p_2, \ldots, p_s$ are distinct prime numbers.*

Then the exact number of the non-zero-symmetric near-rings on $Z_n(+)$ is

$$1 + \sum_{i=1}^{s} \left\{ 1 + \sum_{j/(p_i-1)} \left[(j+1)^{\frac{n - \frac{n}{p_i}}{j}} - 1 \right] \right\} .$$

3. New Lower Bounds for Zero-Symmetric Near-Rings on Finite Cyclic Groups

The following results improve the lower bounds for the number of zero-symmetric near-rings on any finite cyclic group.

Lemma 4. *Let $n = 2p$, where p is an odd prime number or a degree of odd prime number.*

Then $(\mathbb{Z}_n, \cdot)$ has exactly four idempotents $0, 1, p, p{+}1$.

Proof. It is obvious that 0 and 1 are trivial idempotents in $(\mathbb{Z}_n, \cdot)$.

Let $p > 2$ be a prime number. Then p^k is an odd number and we have $p^k \cdot p^k = p^k \cdot (2m{+}1)$ and $p^k \cdot (2m{+}1) = (2mp^k{+}p^k) \equiv p^k \pmod{2p^k}$. Therefore $(p^k)^2 = p^k$ in $(\mathbb{Z}_n, \cdot)$, i.e. p^k is an idempotent.

Consider $(p^k{+}1) \cdot (p^k{+}1) = ((p^k)^2{+}2 \cdot p^k{+}1) = [((p^k)^2{+}p^k){+}p^k{+}1] = [p^k(p^k{+}1) + p^k{+}1]$. Since p^k is an odd number, the number $(p^k{+}1)$ is an even number and $p^k(p^k{+}1) \equiv 0 \pmod{2p^k}$. Therefore $(p^k{+}1)^2 \equiv (p^k{+}1) \pmod{2p^k}$, i.e. $p^k{+}1$ is an idempotent in $(\mathbb{Z}_n, \cdot)$.

Let e be an idempotent in $(\mathbb{Z}_n, \cdot)$. Then $e^2 \equiv e \pmod{2p^k}$ and $e(e{-}1) \equiv 0 \pmod{2p^k}$. We have $(e, e{-}1) = 1$ for $0 \leq e < 2p^k$. Therefore p^k divides e or p^k divides $(e{-}1)$. This is possible when $e = 0$ or $e = p^k$ for the first case, or when $e = 1$ or $e = p^k{+}1$ for the second one.

This proves the claim of Lemma 4. □

Theorem 5. *Let $n = 2t$, t be an odd number and $\pi(0) = 0$, $\pi(t) = t$, $\pi(2k) = 0$, $k{=}1, \ldots, t{-}1$ and $\pi(2k{+}1) \in \{1, t\}$, $k{=}0, 1, \ldots, \frac{t-1}{2}, \frac{t+1}{2}, \ldots, t{-}1$.*

Then equation (1) holds and there are exactly 2^{t-1} near-rings on $\mathbb{Z}_n$.

Proof. To prove that equality (1) is true for all $x, y \in \mathbb{Z}_n$ we consider the following two cases:

Case 1. Let x be an even number. Then $\pi(x) = \pi(2k) = 0$, $\pi(x) \cdot \pi(y) = 0 \cdot \pi(y) = 0$, $\pi(x \cdot \pi(y)) = \pi(\text{even}) = 0$.

Case 2. Let x be an odd number, hence $\pi(x) = 1$ or $\pi(x) = t$.

Case 2.1. Let y be an even number. Then $\pi(y) = 0$ and equation (1) holds.

Case 2.2. Let y be an odd number. Let us consider the following two cases:

Case 2.2.1. Let $\pi(x) = 1$. Then we have $\pi(x) \cdot \pi(y) = 1 \cdot \pi(y) =$

$\pi(y) \cdot \pi(x.\pi(y)) = \pi(\pi(y)) = \pi(y)$, since $\pi(x) = 1$ for an odd number x.

Case 2.2.2. Let $\pi(x) = t, \quad t \neq 1$. Then we have

$$\pi(x) \cdot \pi(y) = t \cdot \pi(y) = t \cdot \{1, t\} = t,$$
$$\pi(x \cdot \pi(y)) = \pi(x \cdot 1) = \pi(x) = t \text{ for } \pi(y) = 1.$$

Therefore $\pi(x. \cdot \pi(y)) = \pi(x \cdot t) = t$ for $\pi(t) = t$.

According to the conditions of Theorem 5, t elements have value 0, one element is equal to t and the other $t-1$ elements have values 1 or t.

Thus there are exactly 2^{t-1} functions π such that the equation (1) holds. □

Lemma 6. *Let $p > 2$ be a prime number.*

Then for $(\mathbb{Z}_{2p}, \cdot)$ the zero is an unique nilpotent of second degree.

Proof. Consider the congruence $x \cdot x \equiv 0 \pmod{n}$, where $n{=}2p$, $x{<}n$. Then there exists $k{<}n$, such that $x \cdot x = k \cdot 2p$ and the above congruence is satisfied. Therefore, x is an even number. Thus $2x_1 \cdot 2x_1 = 2kp$ or $2x_1 \cdot x_1 = kp$, where $x = 2x_1$. Since p is a prime number $>$2, then k must be an even number. Hence $x_1 \cdot x_1 = k_1 \cdot p$, where $k = 2k_1$. Therefore p/x_1, i.e. $x_1 = t \cdot p$, $t \geq 1$. Then $x_1 \cdot x_1 = t \cdot t \cdot p \cdot p = (t \cdot t \cdot p) \cdot p$ and $k = 2 \cdot t \cdot t \cdot p \geq 2p$. This contradicts $k < n$. Hence x must be only equal to 0. □

Proposition 7. *Let $n = 2p$ and $p > 2$ be a prime number.*

Then for all functions $\pi \in \Omega$ if $\pi(0) = 0$, then $\pi(p) \in \{0, 1, p\}$.

Proof. It is obvious that for $\pi(p) = 0$ the equation (1) holds.

Consider the following cases:

Case 1. Let $\pi(p) = 1$. Then $\pi(p) \cdot \pi(p) = 1$, $\pi(p \cdot \pi(p)) = \pi(p) = 1$.

Case 2. Let $\pi(p) = p$. The left side of equation (1) is equal to $\pi(p) \cdot \pi(p) = p \cdot p$. Since p is an odd number, we obtain $p \cdot p \equiv p \pmod{2p}$ and $\pi(p) \cdot \pi(p) = p$. Then we get $\pi(p \cdot \pi(p)) = \pi(p \cdot p) = \pi(p)$. This proves the validity of (1).

Case 3. Let $\pi(p) = x$, $x \notin \{0, 1, p\}$ and x be an odd number. The right side of equation (1) is $\pi(p \cdot \pi(p)) = \pi(p \cdot x)$. Since x is an odd number, we get $p \cdot x \equiv p \pmod{2p}$ and $\pi(p) = x$. To be fulfilled equation (1) the left side must be equal to x, i.e. $\pi(p) \cdot \pi(p) = x \cdot x = x$. This is possible when x is an odd idempotent in $(\mathbb{Z}_{2p}, \cdot)$. From Lemma 4 follows that $x = p$.

Case 4. Let $\pi(p) = x$, $x \notin \{0, 1, p\}$ and $x \in \mathbb{Z}_{2p}$ be an even number. The right side of (1) is equal to $\pi(p \cdot \pi(p)) = \pi(p \cdot x) = \pi(0) = 0$. The left side $\pi(p) \cdot \pi(p) = x \cdot x$ must be equal to 0. This is possible when x is an even nilpotent of second degree in $(\mathbb{Z}_{2p}, \cdot)$. From Lemma 6 follows that $x = 0$. The proposition is fulfilled. □

Theorem 8. *Let* $n = 2t$, t *be an odd number and* $\pi(0) = 0$, $\pi(t) = t$, $\pi(2k) = 0$, $k=1,\dots,t-1$, $\pi(2k+1) \in \{1, t, n-1\}$, $k=0,1,\dots,\frac{t-1}{2},\frac{t+1}{2},\dots,t-1$ *and* $\pi(n-x) = n-\pi(x)$ *for every* $x \in \mathbb{Z}_n$,

Then equation (1) holds and there are exactly $3^{\frac{t-1}{2}}$ *near-rings on* $\mathbb{Z}_n$.

Proof. Consider the following three possible cases:

Case 1. Let x be an even number. Then $\pi(x) = 0$, hence $\pi(x)\cdot\pi(y) = 0\cdot\pi(y) = 0$ and the right part of (1) is $\pi(x\cdot\pi(y)) = \pi(\text{even number}\cdot\pi(y)) = \pi(\text{even number}) = 0$. This proves the validity of (1).

Case 2. Let y be an even number. Then $\pi(x)\cdot\pi(y) = \pi(x)\cdot 0 = 0 = \pi(0) = \pi(x.0) = \pi(x\cdot\pi(y))$. This proves the validity of (1).

Case 3. Let x and y be odd numbers.

Case 3.1. Let $\pi(y) = 1$. Then $\pi(x)\cdot\pi(y) = \pi(x) = \pi(x.\pi(y))$.

Case 3.2. Let $\pi(y) = t$. Then $\pi(x)\cdot\pi(y) = \pi(x)\cdot t = t$, since $(t\cdot\text{odd number}) \equiv t \pmod{2t}$. Therefore $\pi(x\cdot\pi(y)) = \pi(x\cdot t) = \pi(t) = t$, since $\pi(t) = t$.

Case 3.3. Let $\pi(y) = n-1$. Then $\pi(x)\cdot\pi(y) = \pi(x)(n-1) = n\pi(x)-\pi(x) = n-\pi(x)$, since $n\cdot\text{odd number} \equiv n \pmod{n}$. The right side of equation (1) is $\pi(x\cdot\pi(y)) = \pi(x(n-1) = \pi(xn-x) = \pi(n-x)$. From the assumption of Theorem 8 follows $\pi(n-x) = n-\pi(x)$. This proves the validity of (1).

According to the conditions of Theorem 8 we have $\pi(n-x) = n-\pi(x)$, hence the elements less than $\frac{n}{2}$ uniquely determine the elements greater than $\frac{n}{2}$. So, there are $3^{\frac{t-1}{2}}$ functions π. This proves Theorem 8. □

For $n = 2t$, where t is an odd number, the new lower bound for the zero-symmetric near-rings on $\mathbb{Z}_n$ is given by the expression:

$$2^{n-1} + 3^{\lfloor\frac{n-1}{2}\rfloor} + 2^{t-1} + 3^{\frac{t-1}{2}} - 2\,.$$

Denote by m the number of all nilpotents of second degree on $(\mathbb{Z}_n,\cdot)$ and by d_i, $i = 1,\dots,m$ the nilpotents themselves. For every n there exists at least one nilpotent $d_1 = 0$.

Theorem 9. *Consider all* $\mathbb{Z}_n$, *such that* $(\mathbb{Z}_n,\cdot)$ *have nonzero nilpotents of second degree,* $\pi(d_i) = 0$, $i = 1,\dots,m$ *and* $\pi(x) \in \{d_1,\dots,d_m\}$ *for* $x \neq d_1,\dots,d_m$.

Then equation (1) holds and there are exactly $m^{n-m} - 1$ *near-rings on* $\mathbb{Z}_n$ *different from those described above.*

Proof. Every nilpotent of second degree satisfies $a = k \cdot i,\ i = 0, 1, \ldots, m-1$, where k is a minimal nonzero nilpotent of second degree. For every two nilpotents of second degree we have $a \cdot b = k \cdot i \cdot k \cdot j = (k \cdot k)ij \equiv 0 \cdot ij \equiv 0 \pmod{n}$. For every $p, q = 0, \ldots, n-1$, $\pi(p)$ and $\pi(q)$ are nilpotents of second degree. Therefore $\pi(p) \cdot \pi(q) \equiv 0 \pmod{n}$.

If a is a nilpotent of second degree and b is an arbitrary element from $(\mathbb{Z}_n, \cdot)$, then $a \cdot b = d$ is a nilpotent of second degree. Hence $p \cdot \pi(q) = d$ is a nilpotent of second degree. From the assumption of Theorem 9 we get $\pi(d) = 0$, i.e. $\pi(p \cdot \pi(q)) = 0$. Therefore, the equation (1) holds and the described functions π define near-rings on $\mathbb{Z}_n$.

Note that exactly m elements of π have values 0. All other $n-m$ elements have various values of the nilpotents of second degree. Thus there are m^{n-m} functions π. □

The result in Theorem 9 improves the lower bound for the number of near-rings on cyclic groups, where $(\mathbb{Z}_n, \cdot)$ have non-trivial nilpotents of second degree. These groups of order up to 23 are the following: $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}$, $\mathbb{Z}_{20}$ with 2 nilpotents, $\mathbb{Z}_9$, $\mathbb{Z}_{18}$ with 3 nilpotents and $\mathbb{Z}_{16}$ with 4 nilpotents. The numbers of these additional near-rings are: 3 for $\mathbb{Z}_4$, 63 for $\mathbb{Z}_8$, 728 for $\mathbb{Z}_9$, 1023 for $\mathbb{Z}_{12}$, 16777215 for $\mathbb{Z}_{16}$, 14348906 for $\mathbb{Z}_{18}$ and 262143 for $\mathbb{Z}_{20}$.

The existing lower bounds are obtained by the results of Theorem 1 and Theorem 2.

The new constructions are obtained by the proved in Theorems 5, 8 and 9 results.

It obvious from the Table 1 that more than 98 percents of zero-symmetric near-rings are described by above results.

4. New Lower Bounds for Non-Zero-Symmetric Near-Rings on Finite Cyclic Groups

The following results improve the lower bounds for the number of non-zero-symmetric near-rings on any finite cyclic groups.

Proposition 10. *Let $n = 2p^2$ and $p > 2$ be a prime number.*

Then for all functions $\pi \in \Omega$ if $\pi(0) = p^2$, then $\pi(x)$ is an odd number for every $x \in \mathbb{Z}_n$.

	Existing lower bound	Number of new constructions	New lower bound	Exact number	Number of not described
$\mathbb{Z}_3$	6		-	6	0
$\mathbb{Z}_4$	10	3	13	16	3
$\mathbb{Z}_5$	24		-	28	4
$\mathbb{Z}_6$	40	6	46	65	19
$\mathbb{Z}_7$	90		-	111	21
$\mathbb{Z}_8$	154	63	217	349	132
$\mathbb{Z}_9$	336	728	1064	1169	105
$\mathbb{Z}_{10}$	592	24	616	807	191
$\mathbb{Z}_{11}$	1266		-	1311	45
$\mathbb{Z}_{12}$	2290	1023	3313	4467	1154
$\mathbb{Z}_{13}$	4824		-	5263	439
$\mathbb{Z}_{14}$	8920	90	9010	10505	1495
$\mathbb{Z}_{15}$	18570		-	21783	3213
$\mathbb{Z}_{16}$	34954	16777215	16812169	16834653	22484
$\mathbb{Z}_{17}$	72096		-	72816	720
$\mathbb{Z}_{18}$	137632	14349242	14486874	15032215	545341
$\mathbb{Z}_{19}$	281826		-	286380	4554
$\mathbb{Z}_{20}$	543970	262143	806113	876919	70806
$\mathbb{Z}_{21}$	1107624		-	1164023	56399
$\mathbb{Z}_{22}$	2156200	1266	2157466	2225545	68079
$\mathbb{Z}_{23}$	4371450		-	4371615	165
$\sum$				40910046	775369

Table 1: Lower bounds for zero-symmetric near-rings

Proof. Let us consider the right side of equation (1) for 0 and for an arbitrary x: $\pi(0 \cdot \pi(x)) = \pi(0) = p^2$. The left side of (1) is equal to $\pi(0) \cdot \pi(x) = p^2 \cdot \pi(x)$. Since $n = 2p^2$, the congruence $p^2 \cdot \pi(x) \equiv p^2 \pmod{2p^2}$ is true if and only if $\pi(x)$ is an odd number. This proves the claim of Proposition 10. □

Proposition 11. *Let $n = 2p^2$ and $p > 2$ be a prime number.*
Then for all functions $\pi \in \Omega$ if $\pi(0) = p^2$, then $\pi(p^2) = p^2$.

Proof. We will consider the equation (1) for the following possible values of x and y:

Let $x = p^2$ and $y = p^2$. The right side of (1) is equal to $\pi(p^2 \cdot \pi(p^2)) = \pi(p^2) = p^2$, since from Proposition 10 $\pi(p^2)$ is an odd number.

Since p is a prime number, the equation $\pi(p^2) \cdot \pi(p^2) = p^2$ is fulfilled on $\mathbb{Z}_{2p^2}$, if $\pi(p^2)$ is equal to p or equal to p^2.

Assume $\pi(p^2) = p$. Let $x = 0$, $y = p^2$ and $\pi(p^2) = p$. Then we get

$$\pi(0) \cdot \pi(p^2) = p^2 \cdot p = p^2 \neq p = \pi(p^2) = \pi(p^2 \cdot p),$$

since p is an odd number. Therefore, the equation (1) is not satisfied.

Assume $\pi(p^2) = p^2$. Let x be an arbirary and $y = p^2$, $\pi(p^2) = p^2$. Then we obtain

$$\pi(x) \cdot \pi(p^2) = \pi(x) \cdot p^2 = p^2 = \begin{cases} \pi(0) = \pi(x \cdot p^2), \text{ for even } x \ , \\ \pi(p^2) = \pi(x \cdot p^2), \text{ for odd } x \ , \end{cases}$$

or $\pi(x) \cdot \pi(p^2) = \pi(x \cdot \pi(p^2))$. Change x by y in the above equality and we get

$$\pi(p^2) \cdot \pi(y) = p^2 \cdot \pi(y) = p^2 = \pi(p^2) = \pi(p^2 \cdot \pi(y)),$$

since $\pi(y)$ is an odd number. Therefore the equation (1) is satisfied for $\pi(p^2) = p^2$. □

Theorem 12. *Let $n = 2p^2$, $p > 2$ be a prime number and $\pi(0) = p^2$, $\pi(k) \in \{1, p^2, n-1\}$, $\pi(n-k) = n-\pi(k)$ for $k = 1, 2, \ldots, p^2-1, p^2+1, \ldots, n-1$.*

Then equation (1) holds and there are exactly 3^{p^2-1} near-rings on $\mathbb{Z}_n$.

Proof. Consider equation (1) for the following possible cases:

Case 1. Let $\pi(x) = 1$ and $\pi(y) \in \{1, p^2, n-1\}$. We obtain

$$\pi(x) \cdot \pi(y) = \pi(y) = \begin{cases} 1 = \pi(x) = \pi(x \cdot 1), \\ p^2 = \pi(0) = \pi(x \cdot p^2), \ x \text{ even} \ , \\ p^2 = \pi(p^2) = \pi(x \cdot p^2), \ x \text{ odd} \ , \\ n-1 = n-\pi(x) = \pi(n-x) = \pi(x \cdot (n-1)), \end{cases} ,$$

or $\pi(x) \cdot \pi(y) = \pi(x \cdot \pi(y))$, and

$$\pi(y) \cdot \pi(x) = \pi(y) \cdot 1 = \pi(y) = \pi(y \cdot 1) = \pi(y \cdot \pi(x)).$$

Case 2. Let $\pi(x) = p^2$ and $\pi(y) \in \{1, p^2, n-1\}$. We have

$$\pi(y) \cdot \pi(x) = \pi(y) \cdot p^2 = p^2 = \begin{cases} \pi(0) = \pi(y \cdot p^2), \text{ for even } y \ , \\ \pi(p^2) = \pi(y \cdot p^2), \text{ for odd } y \ , \end{cases}$$

or $\pi(y) \cdot \pi(x) = \pi(y \cdot \pi(x))$, and

$$\pi(x) \cdot \pi(y) = p^2 = \begin{cases} \pi(x) = \pi(x \cdot 1), \\ \pi(0) = \pi(x \cdot p^2), \ x \text{ even} \ , \\ \pi(p^2) = \pi(x \cdot p^2), \ x \text{ odd} \ , \\ n-p^2 = n-\pi(x) = \pi(n-x) = \pi(x \cdot (n-1)), \end{cases}$$

or $\pi(x)\cdot\pi(y)=\pi(x\cdot\pi(y))$.

Case 3. Let $\pi(x)=n-1$ and $\pi(y)\in\{1,\,p^2,\,n-1\}$. We get

$$\begin{aligned}\pi(y)\cdot\pi(x) &= \pi(y)\cdot(n-1)=n\cdot\pi(y)-\pi(y)\\ &= n-\pi(y)=\pi(n-y)=\pi(y\cdot(n-1))=\pi(y\cdot\pi(x)),\end{aligned}$$

and

$$\pi(x)\cdot\pi(y)=(n-1)\cdot\pi(y)=n-\pi(y)$$
$$=\begin{cases} n-1=\pi(x)=\pi(x\cdot 1),\\ n-p^2=p^2=\pi(x\cdot p^2),\\ n-(n-1)=n-\pi(x)=\pi(n-x)=\pi(x\cdot(n-1)),\end{cases}$$

or $\pi(x)\cdot\pi(y)=\pi(x\cdot\pi(y))$.

Therefore, the equation (1) holds for all possible cases.

Note that $\pi(n-x)=n-\pi(x)$. Hence, to each element less than $\frac{n}{2}$ it could be assigned an unique element greater than $\frac{n}{2}$. So, there are 3^{p^2-1} functions π that satisfy the conditions of Theorem 12. □

Theorem 13. *Let $n=2p^2$, $p>2$ be a prime number, and $\pi(kp)=p^2$, $k{=}0,1,\ldots,2p-1$ and $\pi(x)\in\{p,p^2,n-p\}$, $x\neq kp$.*

Then equation (1) holds and there are exactly $3^{2p(p-1)}$ near-rings on $\mathbb{Z}_n$.

Proof. According to the assumptions of Theorem 13 $\pi(x)\in\{p,p^2,n-p\}$ and $(n-p)=2p^2-p=p(2p-1)$. Therefore, $\pi(x)=kp$, where k is an odd number. Consider the left side of (1) for arbitrary x and y. We have

$$\pi(x)\cdot\pi(y)=k_1p\cdot k_2p=k_1k_2\cdot p^2=p^2,$$

since k_1k_2 is an odd number.

At the same time, according to the conditions of Theorem 13 the right side of (1) could be written in the form

$$\pi(x\cdot k_2p)=\pi((xk_2)p)=\pi(kp)=p^2.$$

Therefore, the equation (1) holds.

There are $2p$ fixed values of π. The other elements can have three distinct values. Therefore, there are exactly $3^{2p(p-1)}$ function π for which the conditions of Theorem 13 are fulfilled. □

For $n=2p^2$, where $p>2$ is a prime number, the new lower bound for the non-zero-symmetric near-rings on $\mathbb{Z}_n$ is given by the expression:

$$\sum_s 2^{n-\frac{n}{(n,s)}}+3^{p^2-1}+3^{2p(p-1)}-1\,,$$

where s is an arbitrary idempotent modulo n.

Lemma 14. *Let $n = 4p$ and $p>2$ be a prime number. Then for $(\mathbb{Z}_n, \cdot)$:*

1) If $p \equiv 1 \pmod 4$, then the non-trivial idempotents are only p and $3p+1$.

2) If $p \equiv 3 \pmod 4$, then the non-trivial idempotents are only $p+1$ and $3p$.

Proof. 1) Let $p = (4k + 1)$.

a) Then $p^2 = (4k + 1)^2 = 4k(4k + 1) + 4k + 1 \equiv 0 + 4k + 1 = p \pmod{4p}$. It follows that p is an idempotent.

b) $q = n+1-p = 3p+1$ is an idempotent, since $q \equiv 1-p \pmod n$ and $q^2 \equiv (1-p)^2 \equiv 1 - 2p + p^2 \equiv 1 - 2p + p = 1 - p \pmod{4p}$.

2) Let $p = (4k + 3)$.

a) For $q = (p+1) = 4(k+1)$ we have $q^2 = 4.4(k+1)^2 = 4[(k+1)(4k+4)] = 4[(k+1)(4k+3) + (k+1)] \equiv 4(k+1) \pmod{4p}$. Hence $p+1$ is an idempotent.

b) Let $q = n-p = 3p$. Then $(3p)^2 = 9p^2 \equiv 9(4k+3)^2 = 9.4k(4k+3) + 9.3(4k+3) \equiv 27(4k+3) = 24(4k+3) + 3(4k+3) \equiv 3(4k+3) = 3p \pmod{4p}$. It follows that $3p$ is an idempotent.

It is easy to prove that there are exactly 4 idempotents in $(\mathbb{Z}_n, \cdot)$. This proves Lemma 14. □

Theorem 15. *Let $n = 4p$, $p > 2$ be a prime number, $e > 1$ be the even idempotent, and $\pi(2k) = e$, $\pi(2k+1) \in \{e, n-e+2\}$, $k=0, 1, ..., 2p-1$.*

Then equation (1) holds and there are exactly 2^{2p} near-rings on $\mathbb{Z}_n$.

Proof. Consider the expression $(n-e+2).(n-e+2)$. For $p \equiv 1 \pmod 4$ the even idempotent is $e = 3p + 1$:

$$(n - e + 2)(n - e + 2) = (n - e + 2)n - en + e^2 - 2e + 2n - 2e + 4 \equiv e^2 + 4 - 4e$$
$$\equiv e+3n+4-4e = e+12p+4-4e = e+4(3p+1)-4e = e+4e-4e = e \pmod n.$$

For $p \equiv 3 \pmod 4$ we have $e = p + 1$:

$$(n - e + 2)(n - e + 2) = (n - e + 2)n - en + e^2 - 2e + 2n - 2e + 4 \equiv e^2 + 4 - 4e$$
$$\equiv +n+4-4e = e+4p+4-4e = e+4(p+1)-4e = e+4e-4e = e \pmod n.$$

The left side of equation (1) for arbitrary x and y is equal to:

$$\pi(x) \cdot \pi(y) = \begin{cases} e \cdot e = e, \\ e \cdot (n-e+2) = en + 2e - e^2 = 2e - e = e, \\ (n-e+2) \cdot (n-e+2) = e. \end{cases} .$$

Consider the right side of equation (1). Since e and $n-e+2$ are even number, we get

$$\pi(x\cdot\pi(y)) = \begin{cases} \pi(x\cdot e), \\ \pi(x\cdot(n{-}e{+}2)), \end{cases} = \pi(2x) = e.$$

Therefore, the equation (1) holds for all possible functions π.

Note there are $2p$ fixed elements of π. The other elements can have two distinct values. There are exactly 2^{2p} functions π satisfying the condition of Theorem 15. □

As a partial case of Theorem 15 for $n = 12$ it follows Proposition 6 (see [8]).

Theorem 16. *Let $n = 4p$, $p > 2$ be a prime number, $e > 1$ be the even idempotent, $\pi(2k) = e$, $\pi(2k{+}1) \in \{1, e, 2p{+}1\}$, $k{=}0, 1, ..., 2p{-}1$, and $\pi(2j{+}1) = \pi(2j{+}1 + 2p) + 2p$ for $\pi(2j{+}1) \in \{1, 2p{+}1\}$, $j{=}0, 1, ..., 2p{-}1$.*

Then equation (1) holds and there are exactly 3^p near-rings on $\mathbb{Z}_n$.

Proof. From the conditions of Theorem 16 follows that $\pi(2j{+}1) = \pi(2j{+}1{+}2p){+}2p$ for $\pi(2j{+}1) \in \{1, 2p{+}1\}$. Thus, if $\pi(2j{+}1) = e$, then $\pi(2j{+}1{+}2p) = e$.

Consider the equation (1) for the following possible functions π:

Case 1. Let $\pi(x) = \pi(y) = e$. Then

$$\pi(x)\cdot\pi(y) = e\cdot e = e = \pi(2k) = \pi(x\cdot e) = \pi(x\cdot\pi(y)),$$

since e is an even number.

Case 2. Let $\pi(x) = e$ and $\pi(y)$ be an arbitrary. Then the left-hand side of (1) is

$$\pi(x)\cdot\pi(y) = e\cdot\pi(y) = \begin{cases} e\cdot 1 = e, \\ e\cdot e = e, \\ e\cdot(2p+1) = 2pe + e = 4pk + e = e. \end{cases}$$

Consider the expression $\pi(x\cdot(2p{+}1))$, where $\pi(x) = e$ and x is an odd number. Then $\pi(x(2p+1)) = \pi(2px + x) = \pi(2px + x - 2p + 2p) = \pi(2p(x + 1) + x + 2p) = \pi(x + 2p) = \pi(x) = e$, since x is an odd number. If $\pi(2j+1) = e$, then $\pi((2j+1) + 2p) = e$.

The right-hand side of (1) is

$$\pi(x\cdot\pi(y)) = \begin{cases} \pi(x\cdot 1) = \pi(x) = e, \\ \pi(x\cdot e) = \pi(2k) = e, \\ \pi(x\cdot(2p{+}1)) = \pi(2k) = e, \text{ for even } x, \\ \pi(x\cdot(2p{+}1)) = \pi(x + 2p) = e, \text{ for odd } x. \end{cases}$$

Case 3. Let $\pi(x)$ be an abitrary and $\pi(y) = e$. From the above equality it follows that $\pi(x)\cdot\pi(y) = e$. The right-hand side is equal to $\pi(x\cdot e) = \pi(2k) = e$, since e is an even number.

Case 4. Let $\pi(x) = 1$ and $\pi(y) = 2p + 1$. The left-hand side of (1) is

$$\pi(x) \cdot \pi(y) = 2p + 1.$$

Since $\pi(x) = 1$, then $\pi(x + 2p) = \pi(x) + 2p$. The right-hand side is

$\pi(x \cdot 2p+1) = \pi(2px+x) = \pi(2px-2p+x+2p) = \pi(x+2p) = \pi(x)+2p = 2p+1.$

Therefore, equation (1) holds.

Case 5. Let $\pi(x) = 2p + 1$. The left-hand side of (1) is

$$(2p + 1)(2p + 1) = 2p^2 + 4p + 1 \equiv 1 \pmod{4p}.$$

Since $\pi(x) = 2p + 1$, then $\pi(x + 2p) = \pi(x) + 2p$. The right-hand side is

$$\pi(x \cdot 2p + 1) = ... = \pi(x) + 2p = 2p + 1 + 2p = 4p + 1 = 1;$$

Therefore, equation (1) holds.

Case 6. Let $\pi(y) = 1$. Then

$$\pi(x) \cdot \pi(y) = \pi(x) = \pi(x \cdot 1) = \pi(x \cdot \pi(y)).$$

Equation (1) holds for all possible functions π.

From the conditions of Theorem 2 p elements have fixed value of π. Each odd element $2j+1$, $j=0, 1, ..., 2p-1$ uniquely determines the element $2j+1+2p$. So, there are 3^p functions π. □

Theorem 17. *Let $n = 4p$, $p > 2$ be a prime number, $e > 1$ be the odd idempotent, and $\pi(pk) = e$, $k=0, 1, 2, 3$, $\pi(x) \in \{1, e, 2p-1\}$ and $\pi(x) + \pi((2p-1)x) = 2p$, $x \neq kp$.*

Then equation (1) holds and there are exactly 3^{2p-2} near-rings on $\mathbb{Z}_n$.

Proof. From Lemma 14 if $p \equiv 1 \pmod 4$, then $e = p$, and if $p \equiv 3 \pmod 4$, then $e = 3p$, since e is an odd idempotent.

Consider equation (1) for the following possible functions π:

Case 1. Let $\pi(y) = e$. Then

$$\pi(x) \cdot \pi(y) = \pi(x) \cdot e = \begin{cases} 1 \cdot e = e, \\ e \cdot e = e, \\ (2p-1) \cdot e = 2ep - e = 2p - e = e. \end{cases}$$

The right-hand side of (1) is

$$\pi(x \cdot \pi(y)) = \pi(x \cdot e) = \begin{cases} \pi(x \cdot p) = \pi(k_1 p) = e, \\ \pi(x \cdot 3p) = \pi(k3p) = \pi(k_2 p) = e. \end{cases}$$

Therefore, equation (1) holds.

Case 2. Let $\pi(x) = e$. Then

$$\pi(x) \cdot \pi(y) = e \cdot \pi(y) = \begin{cases} e \cdot e = e, \\ e \cdot (2p{-}1) = 2p - e. \end{cases}$$

The right-hand side of (1) is

$$\pi(x \cdot \pi(y)) = \begin{cases} \pi(x \cdot e) = \pi(kp) = e, \\ \pi(x \cdot (2p{-}1)) = 2p - \pi(x) = 2p - e. \end{cases}$$

Therefore, equation (1) holds.

Case 3. Let $\pi(x) = 1$.

Case 3.1. Let $\pi(y) = 1$. Then

$$\pi(x) \cdot \pi(y) = \pi(y) = \left\{ \begin{array}{l} 1 = \pi(x) = \pi(x \cdot 1), \\ e = \pi(kp) = \pi(x \cdot e), \\ 2p{-}1 = 2p - \pi(x) = \pi(x \cdot (2p{-}1)). \end{array} \right\} = \pi(x \cdot \pi(y)).$$

Therefore, equation (1) holds.

Case 3.2. Let $\pi(y) = 2p{-}1$. Then

$$\pi(x) \cdot \pi(y) = \pi(x) \cdot (2p{-}1) = \begin{cases} e \cdot (2p{-}1) = 2ep - e = 2p - e, \ e \text{ is odd}, \\ (2p{-}1) \cdot (2p{-}1) = 4p^2 - 4p + 1 = 1. \end{cases}$$

The right-hand side is equal to

$$\pi(x \cdot (2p{-}1)) = 2p - \pi(x) = \begin{cases} 2p - e, \\ 2p - (2p{-}1) = 1. \end{cases}$$

Therefore, equation (1) holds.

Case 4. Let $\pi(x) = 2p{-}1$. Then

$$\pi(x) \cdot \pi(y) = (2p{-}1) \cdot \pi(x) = \begin{cases} (2p{-}1) \cdot e = 2ep - e = 2p - e = e, \\ (2p{-}1) \cdot (2p{-}1) = 4p^2 - 4p + 1 = 1. \end{cases}$$

The right-hand side is

$$\pi(x \cdot \pi(y)) = \begin{cases} \pi(x \cdot e) = \pi(kp) = e, \\ \pi(x \cdot (2p{-}1)) = 2p - \pi(x) = 2p - (2p{-}1) = 1. \end{cases}$$

Therefore, equation (1) holds for all possible cases.

According to Theorem 17, four elements have fixed value e. Every other element x uniquely determines the element $2p{-}x$. So, there are 3^{2p-2} functions π. □

For $n = 4p$, where $p > 2$ is a prime number, the new lower bound for the non-zero-symmetric near-rings on $\mathbb{Z}_n$ is given by the expression:

$$\sum_s 2^{n - \frac{n}{(n,s)}} + 2^{2p} + 3^p + 3^{2p-2} - 3\,,$$

	Existing lower bound	Number of new constructions	New lower bound	Exact number	Number of not described
$\mathbb{Z}_3$	1		-	1	0
$\mathbb{Z}_4$	1		-	1	0
$\mathbb{Z}_5$	1		-	1	0
$\mathbb{Z}_6$	33		-	33	0
$\mathbb{Z}_7$	1		-	1	0
$\mathbb{Z}_8$	1		-	1	0
$\mathbb{Z}_9$	1		-	1	0
$\mathbb{Z}_{10}$	393		-	393	0
$\mathbb{Z}_{11}$	1		-	1	0
$\mathbb{Z}_{12}$	769	169	938	1055	117
$\mathbb{Z}_{13}$	1		-	1	0
$\mathbb{Z}_{14}$	5256		-	5256	0
$\mathbb{Z}_{15}$	6215		-	6215	0
$\mathbb{Z}_{16}$	1		-	1	0
$\mathbb{Z}_{17}$	1		-	1	0
$\mathbb{Z}_{18}$	66049	538001	604050	610684	6634
$\mathbb{Z}_{19}$	1		-	1	0
$\mathbb{Z}_{20}$	98305	7825	106130	109847	3717
$\mathbb{Z}_{21}$	304834		-	304834	0
$\mathbb{Z}_{22}$	1111088		-	1111088	0
$\mathbb{Z}_{23}$	1		-	1	0
$\sum$				2149417	10468

Table 2: Lower bounds for non-zero-symmetric near-rings

where s is an arbitrary idempotent modulo n.

The existing lower bounds are obtained by the results of Theorem 2 and Theorem 3.

The new constructions are obtained by the proved in Theorems 12, 13, 15, 16 and 17 results.

It obvious from the Table 2 that more than 99.5 percents of non-zero-symmetric near-rings are described by above results.

	Zero-symmetric	Non-zero-symmetric	Total number
$\mathbb{Z}_3$	6	1	7
$\mathbb{Z}_4$	16	1	17
$\mathbb{Z}_5$	28	1	29
$\mathbb{Z}_6$	65	33	98
$\mathbb{Z}_7$	111	1	112
$\mathbb{Z}_8$	349	1	350
$\mathbb{Z}_9$	1169	1	1170
$\mathbb{Z}_{10}$	807	393	1200
$\mathbb{Z}_{11}$	1311	1	1312
$\mathbb{Z}_{12}$	4467	1055	5522
$\mathbb{Z}_{13}$	5263	1	5264
$\mathbb{Z}_{14}$	10505	5256	15761
$\mathbb{Z}_{15}$	21783	6215	27998
$\mathbb{Z}_{16}$	16834653	1	16834654
$\mathbb{Z}_{17}$	72816	1	72817
$\mathbb{Z}_{18}$	15032215	610684	15642899
$\mathbb{Z}_{19}$	286380	1	286381
$\mathbb{Z}_{20}$	876919	109847	986766
$\mathbb{Z}_{21}$	1164023	304834	1468857
$\mathbb{Z}_{22}$	2225545	1111088	3336633
$\mathbb{Z}_{23}$	4371615	1	4371616

Table 3: Number of near-rings on $\mathbb{Z}_n$, $n \leq 23$

5. Generating of Near-Rings on Finite Cyclic Groups

We computed all near-rings on finite cyclic groups of order up to 23, using a new heuristic algorithm.

The obtained results are identical with the exact values from [4] and Theorem 3.

6. Conclusion

We computed all near-rings on $\mathbb{Z}_n$, $n \leq 23$ and improved the lower bounds for the number of near-rings on finite cycling groups. The accumulated empiric data allows us to set up hypotheses and to improve the lower bounds even for values $n > 23$.

Two technical mistakes in [6, p. 425] are found. The number of near-rings on $\mathbb{Z}_9$ is 1170 instead of 1190, and the number of non-isomorphic near-rings on $\mathbb{Z}_4 \times \mathbb{Z}_2$ is 1159 instead of 115.

The application of a new heuristics significantly improves the used algorithm and it gives us possibilities to generate and obtain the exact number of near-rings on $\mathbb{Z}_n$, $n \leq 31$.

Acknowledgments

This research has been partially supported by the project No IS-M-4/2008 of Department for Scientific Research, Plovdiv University "Paisii Hilendarski".

References

[1] E. Aichinger, F. Binder, J. Ecker, R. Eggetsberger, P. Mayr, C. Nöbauer, *SONATA: Systems of Nearrings and their Applications*, Package for the group theory system GAP4, Johanes Kepler University Linz, Austria (2008), http://www.algebra.uni-linz.ac.at/sonata/

[2] J.R. Clay, The near-rings on a finite cycle group, *Amer. Math. Monthly*, **71** (1964), 47-50.

[3] J.R. Clay, The near-rings on groups of low order, *Math. Zeitschr.*, **104** (1968), 364-371.

[4] R.A. Jacobson, The structure of near-rings on a group of prime order, *Amer. Math. Monthly*, **73** (1966), 59-61.

[5] G. Pilz, *Near-Rings*, North-Holland, Amst., **23** (1977).

[6] G. Pilz, *Near-Rings*, North-Holland, Amst., Revised Edition, **23** (1983).

[7] A.K. Rahnev, A.A. Golev, Computing near-rings on finite cyclic groups, *Compt. Rend. Acad. Bulg. Sci.* (2010), To Appear.

[8] A.K. Rakhnev, G.A. Daskalov, Construction of near-rings on finite cyclic groups, In: *Math. and Math. Education*, Sunny Beach, Bulgaria (1985), 280-288.

[9] A.K. Rakhnev, On near-rings, whose additive groups are finite cyclics, *Compt. Rend. Acad. Bulg. Sci.*, **39**, No. 5 (1986), 13-14.

[10] R. Yerby, H. Heatherly, *Near-Ring Newsletter*, **7** (1984), 14-22.