โครงการ

การเรียนการสอนเพื่อเสริมประสบการณ์

ชื่อโครงการ	การนับจำนวนกำลังสองในริงกาลัว Counting squares in Galois rings
ชื่อนิสิต	นายศมากร ศรีพัฒนกุล 5833541823
ภาควิชา	คณิตศาสตร์และวิทยาการคอมพิวเตอร์ สาขาวิชา คณิตศาสตร์
ปีการศึกษา	2561

คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

การนับจำนวนกำลังสองในริงกาลัว

นายศมากร ศรีพัฒนกุล

โครงงานนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2561

Counting squares in Galois rings

Mr. Samakorn Sripatthanakul

A Project Submitted in Partial Fulfillment of the Requirements
for the Degree of Bachelor of Science Program in Mathematics
Department of Mathematics and Computer Science
Faculty of Science
Chulalongkorn University
Academic Year 2018

หัวข้อโครงงาน	การนับจำนวนกำลังสองในริงกาลัว
โดย	นายศมากร ศรีพัฒนกุล เลขประจำตัว 5833541823
สาขาวิชา	คณิตศาสตร์
อาจารย์ที่ปรึกษาโครงงาน	ศาสตราจารย์ ดร.ยศนันต์ มีมาก

ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับโครงงานฉบับนี้เป็นส่วนหนึ่ง ของการศึกษาตามหลักสูตรปริญญาบัณฑิต ในรายวิชา 2301499 โครงงานวิทยาศาสตร์ (Senior Project)

. . . . หัวหน้าภาควิชาคณิตศาสตร์
และวิทยาการคอมพิวเตอร์

(ศาสตราจารย์ ดร.กฤษณะ เนียมมณี)

คณะกรรมการสอบโครงงาน

. . . . อาจารย์ที่ปรึกษาโครงงาน

(ศาสตราจารย์ ดร.ยศนันต์ มีมาก)

. . . . กรรมการ

(รองศาสตราจารย์ ดร.ศจี เพียรสกุล)

. . . . ดวงรัตน์ ไชยชนะ . . . . กรรมการ

(รองศาสตราจารย์ ดร.ดวงรัตน์ ไชยชนะ)

ศมากร ศรีพัฒนกุล: การนับจำนวนกำลังสองในริงกาลัว
(COUNTING SQUARES IN GALOIS RINGS)
อ.ที่ปรึกษาโครงงาน: ศ.ดร.ยศนันต์ มีมาก, 27 หน้า

ในโครงงานนี้ เราหาจำนวนของกำลังสองในริงกาลัว $GR(p^n, r)$ เมื่อ p เป็นจำนวนเฉพาะ และ n, r เป็นจำนวนเต็มบวก ยิ่งกว่านั้นเราประยุกต์ผลที่ได้เพื่อหาจำนวนของกำลังสองในริงผลหารของริงของจำนวนเต็มเกาส์เซียน

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์ ลายมือชื่อนิสิต . . ศมากร ศรีพัฒนกุล . .
สาขาวิชา . คณิตศาสตร์ . ลายมือชื่อ อ.ที่ปรึกษาโครงงาน . . . .
ปีการศึกษา . . . . 2561 . . . .

5833541823 : MAJOR MATHEMATICS.

KEYWORDS: SQUARE, GALOIS RING, GAUSSIAN INTEGER

SAMAKORN SRIPATTHANAKUL: COUNTING SQUARES IN GALOIS RINGS.
ADVISOR: PROF. YOTSANAN MEEMARK, PH.D., 27 PP.

In this project, we find the number of squares in the Galois ring $GR(p^n, r)$ where p is a prime number and $n, r \in \mathbb{N}$. Moreover, we apply this to obtain the number of squares in the quotient rings of the ring of Gaussian integers.

Department . Mathematics and Computer Science . Student's Signature Samakorn Sripatthanakul
Field of Study . . Mathematics . . Advisor's Signature Yotsanan Meemark
Academic Year . . . . . 2018 . . . . .

Acknowledgements

Foremost, I would like to express my sincere gratitude to my project advisor Professor Dr. Yotsanan Meemark for the continuous support of my senior project for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this project. I could not have imagined having a better advisor and mentor for my project.

Besides my advisor, I would like to thank the rest of my project committee: Associate Professor Dr. Sajee Pianskool and Assocociate Professor Dr. Tuangrat Chaichana for their encouragement, insightful comments, and hard questions.

Finally, I most gratefully acknowledge my parents and my friends for all their support throughout the period of this project.

Contents

Chapter 1

Galois Rings

A finite commutative ring is a **local ring** if it has a unique maximal ideal. It follows that if R is local ring with maximal ideal M, then the **unit group** of R, denoted by $\mathcal{U}(R)$, is the complement of M, i.e., $\mathcal{U}(R) = R \smallsetminus M$. Let n and r be positive integers and let p be a prime number. It is well known that there exists a monic polynomial $h(x)$ in $\mathbb{Z}_{p^n}[x]$ of degree r such that the reduction $\bar{h}(x)$ in $\mathbb{Z}_p[x]$ is irreducible. This such polynomial is called a **basic irreducible polynomial**. Consider the ring extension $\mathbb{Z}_{p^n}[x]/(h(x))$, called a **Galois ring**. It can be proved that up to isomophism this Galois ring is unique [1] and hence we may denote it by $GR(p^n, r)$. Observe that $GR(p^n, 1) = \mathbb{Z}_{p^n}$ and $GR(p, r) = \mathbb{F}_{p^r}$, the field of p^r elements. Some general properties of Galois rings are recorded below.

Theorem 1. *[1] Let $R = GR(p^n, r)$.*

1. *R is a local ring of characteristic p^n with maximal ideal pR.*
2. *$R/pR \cong \mathbb{F}_{p^r}$ and $\mathcal{U}(R) = R \smallsetminus pR$.*
3. *There exists a non-zero element ξ in R which is a root of a monic polynomial $h(x)$ of degree r in $\mathbb{Z}_{p^n}[x]$ such that $\bar{h}(x)$ is irreducible in $\mathbb{Z}_p[x]$ and*

$$R = \{a_0 + a_1\xi + \cdots + a_{r-1}\xi^{r-1} : a_0, a_1, \ldots, a_{r-1} \in \mathbb{Z}_{p^n}\}.$$

The unit group of the Galois ring $GR(p^n, r)$ is well studied.

Theorem 2. *[1] Let $R = GR(p^n, r)$. Then $\mathfrak{U}(R) \cong \mathbb{F}_{p^r}^{\times} \times G_2$ where*

1. *$\mathbb{F}_{p^r}^{\times} = \mathbb{F}_{p^r} \smallsetminus \{0\}$ is cyclic of order $p^r - 1$.*
2. *G_2 is a group of order $p^{(n-1)r}$ such that*
   (a) *If $p = 2$ and $n \geq 3$, then G_2 is a direct product of a cyclic group of order 2, a cyclic group of order 2^{n-2} and $r - 1$ cyclic groups each of order 2^{n-1}.*
   (b) *If (p is odd) or ($p = 2$ and $n \leq 2$), then G_2 is a direct product of r cyclic groups each of order p^{n-1}.*

For an element a in a commutative ring R, a is a **square** in R if there exists a b in R such that $a = b^2$. Stangl [3] determined the number of squares in $\mathbb{Z}_{p^n}$. His results are as follows. For $n \in \mathbb{N}$ and p a prime number, we write $s(p^n)$ for the number of squares in $\mathbb{Z}_{p^n}$.

Theorem 3. *Let $n \in \mathbb{N}$. If $p = 2$, then $s(2) = 2$ and*

$$s(2^n) = \begin{cases} \dfrac{2^{n-1}+4}{3}, & n \text{ even}; \\[2ex] \dfrac{2^{n-1}+5}{3}, & n \text{ odd and } n \geq 3. \end{cases}$$

If p is an odd prime. Then

$$s(p) = \frac{p+1}{2} \quad \text{and} \quad s(p^2) = \frac{p^2-p+2}{2}.$$

If $n \geq 3$, then

$$s(p^n) = \begin{cases} \dfrac{p^{n+1}+p+2}{2(p+1)}, & n \text{ even}; \\[2ex] \dfrac{p^{n+1}+2p+1}{2(p+1)}, & n \text{ odd}. \end{cases}$$

We classify squares in the Galois ring $GR(p^n, r)$ into two types: nonunit elements and units. We obtain a 1–1 correspondence between the squares in $pGR(p^n, r)$ and the square in $GR(p^{n-2},r)$. This implies a recursion formula in Chapter 2. In Chapter 3, we find a closed form of the number of squares in $GR(p^n,r)$. Finally, we apply the results on Galois rings to obtain the number of squares in the quotient rings of the ring of Gaussian integers in Chapter 4.

Chapter 2

Recursion Formula

Let p be a prime number and n, r positive integers. Consider the Galois ring

$$R = GR(p^n, r) = \{a_0 + a_1\xi + \cdots + a_{r-1}\xi^{r-1} : a_0, a_1, \ldots, a_{r-1} \in \mathbb{Z}_{p^n}\}$$

where ξ is a root of a basic irreducible polynomial $h(x)$ of degree r in $\mathbb{Z}_{p^n}[x]$. Assume that $n \geq 3$. Then $p^2\mathbb{Z}_{p^n}$ is a subgroup of $(\mathbb{Z}_n, +)$ of order p^{n-2}. Note that if $a \in \mathbb{Z}$ consider modulo p^n and $a \geq p^{n-2}$, then $a = p^{n-2}q + r$ for some $q \in \mathbb{N}$ and $0 \leq r < p^{n-2}$, so $p^2a \equiv p^2r \ mod \ p^n$. Hence, we have shown:

Lemma 4. $p^2\mathbb{Z}_{p^n} = \{p^2a \ : \ a \in \mathbb{Z}$ *and* $0 \leq a < p^{n-2}\}$.

Let T_n denote the set of all squares in pR and let $z \in T_n$. Then $z = l^2$ for some $l \in pR$, so $z = (pL)^2$ for some $L \in R$. Thus $z = p^2L^2 \in p^2R$. It follows that z can be written as

$$z = p^2(a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{r-1}\xi^{r-1}) \quad \text{for some } a_0, a_1, \ldots, a_{r-1} \in \mathbb{Z}_{p^n}.$$

By Lemma 4, we have

$$z = p^2(b_0 + b_1\xi + b_2\xi^2 + \cdots + b_{r-1}\xi^{r-1}) \quad \text{for some } b_0, b_1, \ldots, b_{r-1} \in \mathbb{Z}_{p^{n-2}}.$$

Since z is a square, so $b_0 + b_1\xi + b_2\xi^2 + \cdots + b_{r-1}\xi^{r-1}$ must be a square. Therefore, the number of elements in T_n is the number of squares in $GR(p^{n-2}, r)$.

Let $S(p^n, r)$ be the number of squares in R and let $Q(p^n, r)$ be the number of squares in $R^\times$. Since the number of squares in pR is the number of elements in T_n and $R = R^\times \cup pR$ (a disjoint union), we have the number of squares in R is the number of squares in $R^{\times}$ and the number of squares in pR. This proves the following recursion formula.

Theorem 5. *For* $n \geq 3,\ \ S(p^n, r)\ = Q(p^n, r) + S(p^{n-2}, r).$

Chapter 3

$Q(p^n, r)$ and $S(p^n, r)$

This chapter consists of two computations which are determining $Q(p^n, r)$ and $S(p^n, r)$ of the previous chapter. We use $Q(p^n, r)$ to assist us finding $S(p^n, r)$. According to Theorem 2, we may classify p and n into three cases.

1. $p = 2$ and $n \geq 3$;
2. $p = 2$ and $n < 3$;
3. p is odd.

In the first case, by Theorem 2, we know that

$$\mathbb{F}_{2^r}^{\times} \cong \mathbb{Z}_{2^r-1} \text{ and } G_2 \ \cong\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}} \times \underbrace{\mathbb{Z}_{2^{n-1}} \times \cdots \times \mathbb{Z}_{2^{n-1}}}_{r-1 \text{ times}}$$

and the number of squares in $R^{\times}$ is $|2\mathbb{Z}_{2^r-1}| \cdot |2G_2|$. So,

$$\begin{aligned} Q(p^n, r) &= \frac{2^r - 1}{(2, 2^r - 1)} \cdot \frac{2}{(2,2)} \cdot \frac{2^{n-2}}{(2, 2^{n-2})} \cdot \left(\frac{2^{n-1}}{(2, 2^{n-1})}\right)^{r-1} \\ &= (2^r - 1) \cdot 2^{n-3} \cdot (2^{n-2})^{r-1} \\ &= (2^r - 1)(2^{nr-2r-1}) \\ &= 2^{nr-r-1} - 2^{nr-2r-1}. \end{aligned}$$

Hence, if $p = 2$ and $n \geq 3$, then $Q(p^n, r) \ = \ 2^{nr-r-1} - 2^{nr-2r-1}$.

As for the second case and the third case, by Theorem 2, we have

$$\mathbb{F}_{p^r}^{\times} \cong \mathbb{Z}_{p^r-1} \text{ and } G_2 \ \cong\ \underbrace{\mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \cdots \times \mathbb{Z}_{p^{n-1}}}_{r \text{ times}}.$$

It follows that

$$Q(p^n, r) \quad = \quad \frac{p^r - 1}{(2, p^r - 1)} \cdot \left(\frac{p^{n-1}}{(2, p^{n-1})}\right)^r.$$

If $p = 2$ and $n = 1$, then $Q(p^n, r) = (2^r - 1)(1)^r = 2^r - 1$ and if $p = 2$ and $n = 2$, then $Q(p^n, r) = (2^r - 1)(\frac{2}{2})^r = 2^r - 1$. Finally, if p is odd, then $(2, p^r - 1) = 2$, so

$$Q(p^n, r) \quad = \quad \frac{p^r - 1}{2} \cdot (p^{n-1})^r \quad = \quad \frac{p^{nr} - p^{nr-r}}{2}.$$

We conclude these results in the next theorem.

Theorem 6. *Let $n, r \in \mathbb{N}$. Then*

$$Q(p^n, r) \quad = \quad \begin{cases} 2^{nr-r-1} - 2^{nr-2r-1}, & p = 2 \text{ and } n \geq 3; \\ 2^r - 1, & p = 2 \text{ and } n < 3; \\ \dfrac{p^{nr} - p^{nr-r}}{2}, & p \text{ is odd.} \end{cases}$$

To compute the $S(p^n, r)$, we shall use the recursion formula and Theorem 6. First, we consider the cases $n = 1$ and $n = 2$.

Case $n = 1$: Recall that $S(p, r)$ is the sum of the number of squares in $GR(p, r)^\times$ and the number of squares in $pGR(p, r) = \{0\}$. Thus, $S(p, r) = Q(p, r) + 1$. It follows that

$$S(p, r) \quad = \quad \begin{cases} 2^r, & p = 2; \\ \dfrac{p^r + 1}{2}, & p \text{ is odd.} \end{cases}$$

Case $n = 2$: Again $S(p^2, r)$ is the sum of the number of squares in $GR(p^2, r)^\times$ and the number of squares in $pGR(p^2, r)$. Note that if a is a square in $pGR(p^2, r)$, then $a = (pl)^2$ for some $l \in GR(p^2, r)$, so $a = 0$ in $GR(p^2, r)$. Thus, $S(p^2, r) = Q(p^2, r) + 1$. Hence,

$$S(p^2, r) \quad = \quad \begin{cases} 2^r, & p = 2; \\ \dfrac{p^{2r} - p^r + 2}{2}, & p \text{ is odd.} \end{cases}$$

Next, we find the number of squares in $GR(p^n, r)$ for all $n \geq 3$. By using the recursive formula in Theorem 5 and $Q(p^n, r)$ in Theorem 6, we must divide p and n

into four cases.

Case 1. $p = 2$ and n is even. Then

$$\begin{aligned}
S(p^n, r) &= Q(p^n, r) + S(p^{n-2}, r) \\
&= (2^{nr-r-1} - 2^{nr-2r-1}) + (2^{nr-3r-1} - 2^{nr-4r-1}) + \cdots \\
&\quad + (2^{3r-1} - 2^{2r-1}) + S(p^2, r) \\
&= (2^{nr-r-1} - 2^{nr-2r-1}) + (2^{nr-3r-1} - 2^{nr-4r-1}) + \cdots \\
&\quad + (2^{3r-1} - 2^{2r-1}) + 2^r \\
&= \frac{(2^{2r-1})(2^{nr-2r} - 1)}{2^r + 1} + 2^r \\
&= \frac{2^{nr-1} - 2^{2r-1} + 2^{2r} + 2^r}{2^r + 1}.
\end{aligned}$$

Case 2. $p = 2$ and n is odd. Then

$$\begin{aligned}
S(p^n, r) &= Q(p^n, r) + S(p^{n-2}, r) \\
&= (2^{nr-r-1} - 2^{nr-2r-1}) + (2^{nr-3r-1} - 2^{nr-4r-1}) + \cdots \\
&\quad + (2^{2r-1} - 2^{r-1}) + S(p, r) \\
&= (2^{nr-r-1} - 2^{nr-2r-1}) + (2^{nr-3r-1} - 2^{nr-4r-1}) + \cdots \\
&\quad + (2^{2r-1} - 2^{r-1}) + 2^r \\
&= \frac{(2^{r-1})(2^{nr-r} - 1)}{2^r + 1} + 2^r \\
&= \frac{2^{nr-1} - 2^{r-1} + 2^{2r} + 2^r}{2^r + 1}.
\end{aligned}$$

Case 3. p is odd and n is even. Then

$$\begin{aligned}
S(p^n, r) &= Q(p^n, r) + S(p^{n-2}, r) \\
&= \frac{p^{nr} - p^{nr-r}}{2} + \frac{p^{nr-2r} - p^{nr-3r}}{2} + \cdots + \frac{p^{4r} - p^{3r}}{2} + S(p^2, r) \\
&= \frac{p^{nr} - p^{nr-r} + p^{nr-2r} - p^{nr-3r} + \cdots + p^{4r} - p^{3r} + p^{2r} - p^r}{2} + 1 \\
&= \frac{p^r(p^{nr} - 1)}{2(p^r + 1)} + 1 \\
&= \frac{p^{nr+r} + p^r + 2}{2(p^r + 1)}.
\end{aligned}$$

Case 4. p is odd and n is odd. Then

$$\begin{aligned}
S(p^n,r) &= Q(p^n,r)+S(p^{n-2},r)\\
&= \frac{p^{nr}-p^{nr-r}}{2}+\frac{p^{nr-2r}-p^{nr-3r}}{2}+\cdots+\frac{p^{3r}-p^{2r}}{2}+S(p,r)\\
&= \frac{p^{nr}-p^{nr-r}+p^{nr-2r}-p^{nr-3r}+\cdots+p^{3r}-p^{2r}+p^r}{2}+\frac{1}{2}\\
&= \frac{p^r(p^{nr}+1)}{2(p^r+1)}+\frac{1}{2}\\
&= \frac{p^{nr+r}+2p^r+1}{2(p^r+1)}.
\end{aligned}$$

Finally, we have the closed form of the number of squares in $GR(p^n,r)$ for all $n\in\mathbb{N}$ and p a prime number in the following theorem.

Theorem 7. *Let p be a prime number and $n,r\in\mathbb{N}$. Then*

1. $$S(p,r) = \begin{cases} 2^r, & p=2;\\ \dfrac{p^r+1}{2}, & p \text{ is odd,}\end{cases}$$

2. $$S(p^2,r) = \begin{cases} 2^r, & p=2;\\ \dfrac{p^{2r}-p^r+2}{2}, & p \text{ is odd.}\end{cases}$$

3. *If $n\geq 3$, then*

$$S(p^n,r) = \begin{cases} \dfrac{2^{nr-1}-2^{2r-1}+2^{2r}+2^r}{2^r+1}, & p=2 \text{ and } n \text{ is even};\\[2ex] \dfrac{2^{nr-1}-2^{r-1}+2^{2r}+2^r}{2^r+1}, & p=2 \text{ and } n \text{ is odd};\\[2ex] \dfrac{p^{nr+r}+p^r+2}{2(p^r+1)}, & p \text{ is odd and } n \text{ is even};\\[2ex] \dfrac{p^{nr+r}+2p^r+1}{2(p^r+1)}, & p \text{ is odd and } n \text{ is odd.}\end{cases}$$

Chapter 4

Applications to the Quotient Rings of the Ring of Gaussian Integers

The ring of **Gaussian integers**, denoted by $\mathbb{Z}[i]$, consists of complex numbers that have the form $a+bi$, where $a,b \in \mathbb{Z}$ and $i=\sqrt{-1}$. The units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$. For $a,b \in \mathbb{Z}$ not both zeros, we have the order of the ring $\mathbb{Z}[i]/(a+bi)$ is $N(a+bi)=a^2+b^2$. It is well known that every prime in $\mathbb{Z}[i]$ is a unit multiple of the following primes:

1. π or $\bar{\pi}$, where $N(\pi)=q$ is a prime number in $\mathbb{Z}$ which is $q \equiv 1 \; mod \; 4$,

2. p, where p is a prime number in $\mathbb{Z}$ with $p \equiv 3 \; mod \; 4$ and

3. $\alpha = 1+i$.

Cross [2] worked on representatives for the equivalence classes of the quotient rings of ideals of $\mathbb{Z}[i]$ generated by prime powers in the next theorem.

Theorem 8. *[2] The equivalence classes of $\mathbb{Z}[i]$ modulo a power of a prime are given as follows. For all $m,n \in \mathbb{N}$, we have*

1. $\mathbb{Z}[i]/(\pi^n) = \{[a] : 0 \leq a \leq q^n - 1\}$,

2. $\mathbb{Z}[i]/(p^n) = \{[a+bi] : 0 \leq a,b \leq p^n - 1\}$,

3. $\mathbb{Z}[i]/(\alpha^{2m}) = \{[a+bi] : 0 \leq a,b \leq 2^m - 1\}$,

4. $\mathbb{Z}[i]/(\alpha^{2m+1}) = \{[a+bi] : 0 \leq a \leq 2^{m+1} - 1$ *and* $0 \leq b \leq 2^m - 1\}$.

Now, we count the number of squares in the quotient rings of the ring of Gaussian integers by counting the squares in the ring which is isomorphic to these extension rings. We distinguish the proof into three cases depending on types of primes.

Let n be a positive integer.

Case 1. $\mathbb{Z}[i]/(\pi^n)$ where $N(\pi) = q$ is a prime number in $\mathbb{Z}$ with $q \equiv 1 \bmod 4$. Assume that $r, s \in \mathbb{Z}$ are such that $r \equiv s \bmod \pi^n$. Then π^n divides $r - s$, so $\bar{\pi}^n$ divides $\overline{r-s} = r - s$. Since π and $\bar{\pi}$ are not associates, π and $\bar{\pi}$ are relatively prime in $\mathbb{Z}[i]$, so $\pi^n\bar{\pi}^n = q^n$ divides $r - s$. Thus, $r \equiv s \bmod q^n$. Since $|\mathbb{Z}[i]/(\pi^n)| = N(\pi^n) = \pi^n\bar{\pi}^n = q^n$, the above argument shows that

$$\mathbb{Z}[i]/(\pi^n) = \{a + (\pi^n) : a \in \mathbb{Z} \text{ and } 0 \leq a \leq q^n - 1\}.$$

The natural map $\varphi : a + (\pi^n) \longmapsto [a]$ gives an isomorphism of $\mathbb{Z}[i]/(\pi^n)$ onto $\mathbb{Z}_{q^n}$. Since $\mathbb{Z}_{q^n}$ is a Galois ring over $\mathbb{Z}_{q^n}$ with $r = 1$, Theorem 7 implies the following theorem.

Theorem 9. *Let $S(\pi^n)$ denote the number of squares in $\mathbb{Z}[i]/(\pi^n)$ where $n \in \mathbb{N}$. Then*

1. $S(\pi) = \dfrac{q+1}{2}$
2. $S(\pi^2) = \dfrac{q^2 - q + 2}{2}$
3. *If $n \geq 3$, then*

$$S(\pi^n) = \begin{cases} \dfrac{q^{n+1} + q + 2}{2(q+1)}, & n \text{ is even}; \\ \\ \dfrac{q^{n+1} + 2q + 1}{2(q+1)}, & n \text{ is odd}. \end{cases}$$

Case 2. $\mathbb{Z}[i]/(p^n)$ where p is a prime number in $\mathbb{Z}$ with $p \equiv 3 \bmod 4$. We will show that $\mathbb{Z}[x]/(p^n, x^2 + 1) \cong \mathbb{Z}[i]/(p^n)$.

Proof. Define $\rho : \mathbb{Z}[x] \to \mathbb{Z}[i]/(p^n)$, by $\rho : f(x) \longmapsto f(i) + (p^n)$. Then ρ is an onto homomorphism. To compute the kernel of ρ, let $f(x) \in \mathbb{Z}[x]$ be such that $f(i) + (p^n) = 0 + (p^n)$. Then p^n divides $f(i)$ in $\mathbb{Z}[i]$, so $f(i) = p^n(b + ci)$ for some

$b, c \in \mathbb{Z}$. Thus, $f(i) - p^n(b + ci) = 0$, so i is a root of $f(x) - p^n(b + cx)$ in $\mathbb{Z}[x]$. It follows that $f(x) - p^n(b + cx) = (x^2 + 1)g(x)$ for some $g(x) \in \mathbb{Z}[x]$. Then $f(x) = p^n(b + cx) + (x^2 + 1)g(x)$ is in $(p^n, x^2 + 1)$. Hence, ker $\rho = (p^n, x^2 + 1)$. □

Next, we prove that $\mathbb{Z}[x]/(p^n, x^2 + 1) \cong \mathbb{Z}_{p^n}[x]/(x^2 + \bar{1})$.

Proof. Define $\eta : \mathbb{Z}[x] \to \mathbb{Z}_{p^n}[x]/(x^2 + \bar{1})$, by $\eta(a_0 + a_1x + \cdots + a_kx^k) = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_kx^k + (x^2 + \bar{1})$ for all $a_0, a_1, \ldots, a_k \in \mathbb{Z}$ and $k \in \mathbb{N} \cup \{0\}$. Then η is an onto homomorphism. Its kernel is $\{a_0 + a_1x + \cdots + a_kx^k : k \in \mathbb{N} \cup \{0\},\ a_0, a_1, \ldots, a_k \in \mathbb{Z}$ and $x^2 + \bar{1}$ divides $\bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_kx^k$ in $\mathbb{Z}_{p^n}[x]\}$. If $a_0, a_1, \ldots, a_k \in \mathbb{Z}$ and $\bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_kx^k = (x^2 + \bar{1})(\bar{b}_0 + \bar{b}_1x + \cdots + \bar{b}_mx^m)$ for some $m \in \mathbb{N} \cup \{0\}$ and $b_0, b_1, \ldots, b_m \in \mathbb{Z}$, then p^n divides $(a_0 + a_1x + \cdots + a_kx^k) - (x^2 + 1)(b_0 + b_1x + \cdots + b_mx^m)$ in $\mathbb{Z}[x]$, so $a_0 + a_1x + \cdots + a_kx^k = (x^2 + 1)(b_0 + b_1x + \cdots + b_mx^m) + p^nh(x)$ for some $h(x) \in \mathbb{Z}[x]$. □

Since $p \equiv 3 \bmod 4$, -1 is not a square modulo p, so $x^2 + \bar{1}$ is irreducible in $\mathbb{Z}_p[x]$. Hence, $\mathbb{Z}_{p^n}[x]/(x^2 + \bar{1})$ is a Galois ring with $r = 2$. By Theorem 7, we have the following theorem.

Theorem 10. *Let $S(p^n)$ denote the number of squares in $\mathbb{Z}[i]/(p^n)$ where $n \in \mathbb{N}$. Then*

1. $S(p) = \dfrac{p^2 + 1}{2}$
2. $S(p^2) = \dfrac{p^4 - p^2 + 2}{2}$
3. *If $n \geq 3$, then*

$$S(p^n) = \begin{cases} \dfrac{p^{2n+2} + p^2 + 2}{2(p^2 + 1)}, & n \text{ is even}; \\ \\ \dfrac{p^{2n+2} + 2p^2 + 1}{2(p^2 + 1)}, & n \text{ is odd}. \end{cases}$$

Case 3. $\mathbb{Z}[i]/(\alpha^n)$ where $\alpha = 1 + i$. For $n \in \mathbb{N}$, let $S(\alpha^n)$ be the number of squares in $\mathbb{Z}[i]/(\alpha^n)$ and let $Q(\alpha^n)$ be the number of squares in $\mathbb{Z}[i]/(\alpha^n)$ that are units. By Theorem 8, we know that $\mathbb{Z}[i]/(\alpha) = \{[0], [1]\}$ and $\mathbb{Z}[i]/(\alpha^2) = \{[0], [1], [i], [1 + i]\}$.

Since ($0^2 \equiv 0 \bmod \alpha$ and $1^2 \equiv 1 \bmod \alpha$) and ($0^2 \equiv 0 \bmod \alpha^2$, $1^2 \equiv 1 \bmod \alpha^2$, $i^2 \equiv 1 \bmod \alpha^2$ and $(1+i)^2 \equiv 0 \bmod \alpha^2$), we have $S(\alpha) = 2$ and $S(\alpha^2) = 2$. For $n \geq 3$, we begin with a lemma.

Lemma 11. *Let $n \in \mathbb{N}$ with $n \geq 3$. For $b \in \mathbb{Z}[i]$, $b + (\alpha^{n-2})$ is a square in $\mathbb{Z}[i]/(\alpha^{n-2})$ if and only if $b\alpha^2 + (\alpha^n)$ is a square in $\mathbb{Z}[i]/(\alpha^n)$.*

Proof. Let $b \in \mathbb{Z}[i]$. Suppose $b + (\alpha^{n-2})$ is a square in $\mathbb{Z}[i]/(\alpha^{n-2})$. Then there exists a $c \in \mathbb{Z}[i]$ such that $c^2 \equiv b \bmod \alpha^{n-2}$, so $c^2 - b = \alpha^{n-2}z$ for some $z \in \mathbb{Z}[i]$. It follows that $(c\alpha)^2 - b\alpha^2 = \alpha^n z$ or $b\alpha^2 \equiv (c\alpha)^2 \bmod \alpha^n$. Hence, $b\alpha^2$ is a square in $\mathbb{Z}[i]/(\alpha^n)$.

Conversely, suppose that there is a $y \in \mathbb{Z}[i]$ such that $b\alpha^2 \equiv y^2 \bmod \alpha^n$. Then $b\alpha^2 - y^2 = \alpha^n w$ for some $w \in \mathbb{Z}[i]$, so $\alpha^2 \mid y^2$. Thus, $\alpha \mid y$, so we have $y = x\alpha^2$ for some $x \in \mathbb{Z}[i]$. Hence, $b\alpha^2 - x\alpha^2 = \alpha^n w$, so $b - x = \alpha^{n-2}w$, i.e., $b \equiv x \bmod \alpha^{n-2}$ as desired. □

Let $n \in \mathbb{N}$ and $n \geq 3$. Suppose $k \in \mathbb{Z}[i]$ and $k\alpha$ is a square in $\mathbb{Z}[i]/(\alpha^n)$. Then $k\alpha - c^2 = \alpha^n z$ for some $c, z \in \mathbb{Z}[i]$, so $\alpha \mid c^2$. Since α is a prime in $\mathbb{Z}[i]$, $\alpha \mid c$. It follows that $\alpha \mid k$, so $k = b\alpha$ for some $b \in \mathbb{Z}[i]$ and $b\alpha^2 + (\alpha^n)$ is a square in $\mathbb{Z}[i]/(\alpha^n)$. The above lemma implies that $b + (\alpha^{n-2})$ is a square in $\mathbb{Z}[i]/(\alpha^{n-2})$. Thus, we have a 1–1 correspondence between nonunit squares in $\mathbb{Z}[i]/(\alpha^n)$ and squares in $\mathbb{Z}[i]/(\alpha^{n-2})$. This proves $S(\alpha^n) - Q(\alpha^n) = S(\alpha^{n-2})$. We record this recursion formula in the next theorem.

Theorem 12. *For $n \geq 3$, $S(\alpha^n) = Q(\alpha^n) + S(\alpha^{n-2})$.*

Cross [2] computed the following unit groups.

Theorem 13. *[2] $\mathcal{U}(\mathbb{Z}[i]/(\alpha)) \cong \{0\}$, $\mathcal{U}(\mathbb{Z}[i]/(\alpha^2)) \cong \mathbb{Z}_2$, $\mathcal{U}(\mathbb{Z}[i]/(\alpha^3)) \cong \mathbb{Z}_4$ and $\mathcal{U}(\mathbb{Z}[i]/(\alpha^4)) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$. For $n \geq 5$,*

$$\mathcal{U}(\mathbb{Z}[i]/(\alpha^n)) \cong \begin{cases} \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_4, & \text{if } n = 2m; \\ \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_4, & \text{if } n = 2m+1. \end{cases}$$

Then we have $Q(\alpha) = 1$, $Q(\alpha^2) = 2$, $Q(\alpha^3) = 2$ and $Q(\alpha^4) = 2$. For $n \geq 5$, we have two cases.

Case 1. $n = 2m$ is even. Then

$$Q(\alpha^{2m}) = |2\mathbb{Z}_{2^{m-1}}| \cdot |2\mathbb{Z}_{2^{m-2}}| \cdot |2\mathbb{Z}_4| = \frac{2^{m-1}}{2} \cdot \frac{2^{m-2}}{2} \cdot \frac{4}{2} = 2^{2m-4} = 2^{n-4}.$$

Case 2. $n = 2m+1$ is odd. Then

$$Q(\alpha^{2m+1}) = |2\mathbb{Z}_{2^{m-1}}| \cdot |2\mathbb{Z}_{2^{m-1}}| \cdot |2\mathbb{Z}_4| = \frac{2^{m-1}}{2} \cdot \frac{2^{m-1}}{2} \cdot \frac{4}{2} = 2^{2m-3} = 2^{n-4}.$$

Hence, $Q(\alpha^n) = 2^{n-4}$ for all $n \geq 5$.

Now, for $n \geq 3$, by repeated applications of Theorem 12, we obtain:
If n is even, then

$$\begin{aligned} S(\alpha^n) &= Q(\alpha^n) + S(\alpha^{n-2}) \\ &= 2^{n-4} + 2^{n-6} + \cdots + 2^2 + S(\alpha^4) \\ &= \frac{2^2(2^{n-4}-1)}{3} + Q(\alpha^4) + S(\alpha^2) \\ &= \frac{2^{n-2}+8}{3}, \end{aligned}$$

and if n is odd, then

$$\begin{aligned} S(\alpha^n) &= Q(\alpha^n) + S(\alpha^{n-2}) \\ &= 2^{n-4} + 2^{n-6} + \cdots + 2^1 + S(\alpha^3) \\ &= \frac{2(2^{n-3}-1)}{3} + Q(\alpha^3) + S(\alpha) \\ &= \frac{2^{n-2}+10}{3}. \end{aligned}$$

We conclude the number of squares in $\mathbb{Z}[i]/(\alpha^n))$ in the following theorem.

Theorem 14. *We have $S(\alpha) = 2$ and $S(\alpha^2) = 2$. For $n \geq 3$, then*

$$S(\alpha^n) = \begin{cases} \dfrac{2^{n-2}+8}{3}, & n \textit{ is even}; \\[2ex] \dfrac{2^{n-2}+10}{3}, & n \textit{ is odd}. \end{cases}$$

Since $\mathbb{Z}[i]$ is a UFD, if w is a nonzero nonunit element in $\mathbb{Z}[i]$, then it is a product of powers of a prime in $\mathbb{Z}[i]$. Using the Chinese remainder theorem and Theorems 9, 10 and 14, we can determine the number of squares in $\mathbb{Z}[i]/(w)$ where w is a nonzero nonunit element in $\mathbb{Z}[i]$.

References

[1] Gilberto Bini and Flamini Flaminio. *Finite Commutative Rings and Their Applications*. Springer Science+Business Media, LLC. New York. 2002.

[2] James T. Cross. The Euler ϕ-Function in the Gaussian Integers. *The American Mathematical Monthly.* Vol.90, No.8 (Oct.,1983): Page 518–528.

[3] Walter D. Stangl. Counting squares in $\mathbb{Z}_n$. *Mathematics Magazine.* Vol.69, No.4 (Oct.,1996): Page 285–289.

The Project Proposal of Course 2301399 Project Proposal Academic Year 2018

Project Title (Thai)	การนับจำนวนกำลังสองในริงผลหารของริงของจำนวนเต็มเกาส์เซียน
Project Title (English)	Counting squares in quotient rings of the ring of Gaussian integer
Project Advisor	Professor Yotsanan Meemark, Ph.D.
By	Mr. Samakorn Sripatthanakul ID 5833541823
	Mathematics Program
	Department of Mathematics and Computer Science
	Faculty of Science, Chulalongkorn University

Background and Rationale

In 1996, Stangl [1] determined the number of squares in $\mathbb{Z}_{p^n}$ where p is a prime number. He showed that $\forall n \geq 3, s(p^n) = q(p^n) + s(p^{n-2})$ where $s(p^n)$ is the number of all squares in $\mathbb{Z}_{p^n}$ and $q(p^n)$ the number of squares in $\mathbb{Z}_{p^n}$ that are units. A square in $\mathbb{Z}_{p^n}$ that is a unit is called a quadratic residue modulo p^n and their number is well known.

Let $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$ be the ring of Gaussian integers. Cross [2] completely determined the group of units of the quotient ring $\mathbb{Z}[i]/(\alpha)$ for all $\alpha \in \mathbb{Z}[i]$. It allows us to count the number of squares in this quotient ring which are units.

In this project, we will find the number of squares in quotient rings of the ring of Gaussian integers. We will prove a recursion formula for the number of squares in $D/(p^n)$ where D is a unique factorization domain and $p \in D$ is a prime element. Then, we use Cross's result to obtain the number of squares.

Objectives

To count the number of squares in quotient rings of the ring of Gaussian integers.

Project Activities

1. Study the work of Stangl [1] and Cross [2].
2. Review basic knowledge on Abstract Algebra and Number Theory which relates to our project.

3. Prove a recursion formula for the number of squares in $D/(p^n)$ where D is a unique factorization domain and $p \in D$ is a prime element.

4. Compute the number of quadratic residues by using result of Cross [2] and then compute the number of squares that are non-unit.

5. Use recursion formula to determine form of number of squares in $\mathbb{Z}[i]/(\pi^n)$ where π is s prime in $\mathbb{Z}[i]$.

6. Write a report.

Activities Table

Project Activities	August 2018 - April 2019								
	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr
1.Study the work of Stangl [1] and Cross [2].	■								
2.Review basic knowledge on Abstract Algebra and Number Theory which relates to our project.		■	■						
3.Prove a recursion formula for the number of squares in $D/(p^n)$ where D is a unique factorization domain and $p \in D$ is a prime element.				■					
4.Compute the number of quadratic residues by using result of Cross [2] and then compute the number of squares that are non-unit.				■	■	■			
5.Use recursion formula to determine form of number of squares in $\mathbb{Z}[i]/(\pi^n)$ where π is s prime in $\mathbb{Z}[i]$.						■	■		
6.Write a report.								■	■

Benefits

To obtain the number of squares in quotient rings of the ring of Gaussian integers.

Equipment

1. Computer
2. Paper
3. Printer
4. Stationery
5. Word processing program

References

[1] Gilberto Bini and Flamini Flaminio. *Finite Commutative Rings and Their Applications.* Springer Science+Business Media, LLC. New York. 2002.

[2] James T. Cross. The Euler ϕ-Function in the Gaussian Integers. *The American Mathematical Monthly.* Vol.90, No.8 (Oct.,1983): Page 518–528.

[3] Walter D. Stangl. Counting squares in $\mathbb{Z}_n$. *Mathematics Magazine.* Vol.69, No.4 (Oct.,1996): Page 285–289.

Author's profile

Mr. Samakorn Sripatthanakul
ID 5833541823
Department of Mathematics and Computer Science
Faculty of Science, Chulalongkorn University