Partition Z_n into multiplicative groups

Aline Jerman
Supervised by Prof. Ayman Badawi

A senior project presented for the degree of
Bachelor of Science in Mathematics

Department of Mathematics and Statistics
The American University of Sharjah
United Arab Emirates

1 Abstract

Let $n \geq 2$ be a positive integer. This project aims to partition the set of integers modulo n, denoted as Z_n, into multiplicative groups by considering two cases: when n is square-free and when n is not square-free. By analyzing these cases, we can better understand the structure of the multiplicative groups that form Z_n. Our primary tool in this project relies on the Chinese Remainder Theorem (CRT).

2 Introduction

Writing a number as a prime factorization means composing it into a product of prime factors. For any positive integer $n \geq 2$, it is known that n can be written uniquely as a product of a power of prime numbers. An integer n is square-free if and only if p^2 is not a factor of n for every prime factor p of n. For example, the integer $n = 10 = 2 \times 5$ is square-free; However, the integer $n = 12 = 2^2 \times 3$ is not square-free because it is divisible by 2^2.

We recall the following definitions.

Definition 1. *1. A group $(G, *)$ is a nonempty set of elements together with a binary operation $*$ such that the following axioms are satisfied:*

(a) Closure: For any two elements $a, b \in G$, we have $a * b \in G$.

(b) Associativity: The binary operation $*$ is associative, meaning that for any three elements a, b, and c in G, we have $(a * b) * c = a * (b * c)$

(c) Identity: There exists an element in G, denoted by e, such that for any element $a \in G$, we have $e * a = a * e = a$

(d) Inverse: For every element $a \in G$, there exists an element, denoted by a^{-1}, such that $a * a^{-1} = a^{-1} * a = e$

2. *A group $(G, *)$ is called an abelian group if $a * b = b * a$ for all $a, b \in G$.*

3. *We recall $(Z_n, +, .)$ is the set of integers modulo n, i.e., $Z_n = \{0, 1, ..., n-1\}$, where "$+$" is addition modulo n and "$\cdot$" is multiplication modulo n.*

4. *An element e of Z_n is called idempotent if $e \cdot e = e^2 = e$.*

5. *An element $w \in Z_n$ is called nilpotent if there exists a positive integer m such that $w^m = 0$ in Z_n.*

6. *If $k, n \geq 1$ are integers and $k \mid n$, then $D_k = \{1 \leq a < n \mid gcd(a, n) = k\}$.*

Our primary tool in this project relies on the Chinese Remainder Theorem (CRT), which provides a way to solve systems of linear congruence with pairwise relatively prime (or coprime, meaning the GCD between the two numbers is 1) moduli. The Chinese Remainder Theorem states that given a system of k linear congruencies of the form:

$$x \equiv a_1 \ (mod\, m_1)$$

$$\vdots$$

$$x \equiv a_k \ (mod\, m_k)$$

Where the moduli $m_1, m_2, ..., m_k$ are pairwise relatively prime, there exists a unique solution x, $0 \leq x < m_1 m_1 \cdots m_k$ that satisfies all the congruence's at the same time.

In this project, CRT will partition Z_n into multiplicative groups if n is square-free. On the other hand, if n is not square-free, we construct all possible multiplicative groups inside Z_n.

3 Main result

Definition 2. *Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $i = 1, 2, ..k$, where $p_1, ..., p_k$ are distinct prime numbers and $\alpha_1, ..., \alpha_k \in \mathbb{N}$. Each $p_i^{\alpha_i}$, $\forall 1 \leq i \leq k$, is called a **perfect prime factor** of n. Assume m is a factor of n such that $1 \leq m < n$ and m is a product of distinct perfect prime factors of n or $m = 1$. Then we say m is a **perfect factor** of n.*

Example 3.0.1. *Let $n = 3^5 \times 7^{11} \times 2^{13} \times 5^3$. Then*

1. *$3^5, 7^{11}, 2^{13}, 5^3$ are perfect prime factors of n*
2. *$3^5 \times 7^{11}$ is a perfect factor of n*

Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $i = 1, 2, ..k$, where $p_1, ..., p_k$ are distinct prime numbers and $\alpha_1, ..., \alpha_k \in \mathbb{N}$. Then $\phi(n) = (p_1^{\alpha_1} - p_1^{(\alpha_1 - 1)}) \cdots (p_k^{\alpha_k} - p_k^{(\alpha_k - 1)}) = |D_1|$, for the definition of D_k see the definition 2(6).

The following is a well-known result of an introductory number theory course.

Fact 3.0.1. *Let $n \geq 2$ be a positive integer and $k \geq 1$ be a factor of n. Then $|D_k| = \phi(n/k)$.*

We have the following result.

Theorem 3.0.2. *Let e be a nonzero idempotent of Z_n. Then eD_1 is a multiplicative group of Z_n with identity e.*

Proof. We show closure. Let $x = eu$, y = ev$\in eD_1$ for some $u, v \in D_1$. Since D_1 is a multiplicative group of Z_n with identity 1, we have $uv =\in D_1$. Hence $xy = euev = e^2uv = euv \in eD_1$. e is the identity of eD_1. Let $x = eu \in eD_1$ for some $u \in D_1$. Since $u^{-1} \in D_1$, we have $(eu)(eu^{-1} = e^2uu^{-1} = e^2 = e$. Thus $x^{-1} = eu^{-1} \in eD_1$. Since $(Z_n, .)$ is associative, eD_1 is associative. $\square$

Theorem 3.0.3. *Let e be an idempotent of Z_n such that $e \notin \{0, 1\}$. Then the $gcd(e, n)$ is a perfect factor of n*

Proof. Suppose that $e^2 = e$ in Z_n. Then $n \mid e(e-1)$, Since $e \notin \{0, 1\}$, we conclude that neither $n \mid e$ nor $n \mid (e-1)$. Since $gcd(e, e-1) = gcd(e, 1-e) = 1$, we conclude that $n = dh$ for some perfect factors d, h of n, where $d \neq 1$, $h \neq 1$, $d \mid e$, and $h \mid (e-1)$. $\square$

Given Theorem 3.0.3, to construct multiplicative groups in Z_n with an identity different from one, we only need to consider sets of the form D_k, where k is a perfect factor of n.

Theorem 3.0.4. *Let $k, n \geq 2$ be integers and suppose that $k > 1$ is a perfect factor of n. Then $D_k = \{1 \leq a < n | gcd(a, n) = k\}$ is a multiplicative group of Z_n with identity $e_k \neq 1$ and of order $\phi(n/k)$. Furthermore, if D_k is a multiplicative group of Z_n with identity $e_k \neq 1$, then $D_k = e_k D_1$.*

Proof. First, we show that D_k has an idempotent e_k of Z_n. By the CRT, there exists a unique e_k, $1 < e_k < n$ such that $e_k \equiv 0\ (mod\ k)$ and $e_k \equiv 1\ (mod\ \frac{n}{k})$. Hence $n = k\frac{n}{k} \mid e_k(e_k - 1)$. Note that $k, \frac{n}{k}$ are perfect factors of n and $gcd(k, \frac{n}{k}) = 1$. Thus $gcd(e, n) = k$ and $e_k \in D_k$.

Let $d \in D_k$. Since $k \mid d$ and $\frac{n}{k} \mid (e_k - 1)$, we have $n = k\frac{n}{k} \mid d(e_k - 1)$. Thus $e_k d = d$ in Z_n. Thus e_k is the identity of D.

We show that $e_k D_1 = D_k$. Let $x \in e_k D_1$. Hence, $x = e_k d$, such that $d \in D_1$. Since $gcd(d, n) = 1$ and $gcd(e_k, n) = k$, we have $gcd(e_k d, n) = gcd(e_k, n) = k$. Thus $x \in D_k$. Let $y \in D_k$. Set $w = y + (e_k - 1)$. Let p be a prime factor of n. Since $y(e_k - 1) = 0$ in Z_n and $gcd(y, e_k - 1) = 1$, we have $p \mid y$ or $p \mid (e_k - 1)$, but p does not divide both. Hence $gcd(w, n) = 1$. Thus $w \in D_1$. Since $w = y + (1 - e_k)$, we have $e_k w = e_k(y + (e_k - 1)) = e_k y$. Since e_k is the identity of D_K and $y \in D_k$, we have $y = e_k y = e_k w \in e_k D_1$. Thus $e_k D_1 = D_k$. Since $e_k D_1$ is a multiplicative group of Z_n with an identity e_k by Theorem 3.0.2, we conclude that D_k is a multiplicative group of Z_n with an identity e_k. It is clear that $|D_k| = \phi(n/k)$ by Fact 3.0.1. $\square$

The following result gives the exact number of idempotents in Z_n.

Theorem 3.0.5. *Let $n \geq 2$, $ID(Z_n) = \{e \in Z_n \mid e^2 = e \in\ Z_n\}$, and $M = |\{d \ \mid\ d$ is a perfect prime factor of $n\ \}|$. Then $|Id(Z_n)| = 2^M$*

Proof. Let $e \in Id(Z_n)$. Then by Theorem 3.0.2, e is 1 or e is a perfect prime factor of n or a product of 2 perfect prime factors of n or $\cdots$ or a product of $M - 1$ perfect prime factors of n or 0 = the product of all M perfect prime factors of n. Hence $|Id(Z_n)| = \binom{M}{0} + \binom{M}{1} + \binom{M}{2} + \cdots + \binom{M}{M-1} + \binom{M}{M} = 2^M$ $\square$

Example 3.0.2. *Let $n = 3^2 \times 5 \times 7^5$, the number of idempotents of Z_n is $2^3 = 8$ by Theorem 3.0.5*

In the following example, we illustrate how to use the CRT to find all idempotents in Z_n

Example 3.0.3. *Consider Z_{63}. We have $n = 3^2 \cdot 7 = 63$. Since n divides $e^2 - e = e(e - 1)$, it follows that $3^2 = 9$ and 7 will divide either e or $e - 1$ by Theorem 3.0.2. Therefore, we have:*

$3^2 \mid e(e - 1)$*, so either* $3^2 \mid e$ *or* $3^2 \mid (e - 1)$*, and*
$7 \mid e(e - 1)$*, so either* $7 \mid e$ *or* $7 \mid (e - 1)$.
This leads to 4 possible combinations.
1) $e \equiv 0 \pmod{3^2}$ *and* $e \equiv 0 \pmod 7$*, or*
2) $e \equiv 0 \pmod{3^2}$ *and* $e \equiv 1 \pmod 7$*, or*
3) $e \equiv 1 \pmod{3^2}$ *and* $e \equiv 0 \pmod 7$*, or*
4) $e \equiv 1 \pmod{3^2}$ *and* $e \equiv 1 \pmod 7$

Recall that an element $x \in Z_n$ is called a nilpotent element of Z_n if $x^m = 0$ in Z_n for some positive integer $m \geq 1$. We have the following result.

Theorem 3.0.6. *Let $x \in Z_n$. Then x is a nilpotent of Z_n if and only if $p \mid n$ for every prime factor p of n. In particular, if n is square-free, 0 is the only nilpotent element of Z_n.*

Proof. Let p be a prime factor of n. Assume x is a nilpotent element of Z_n. Thus $x^m = 0$ in Z_n. Hence $n \mid x^m$. Thus $p \mid x$. Conversely, suppose that $p \mid n$ for every prime factor p of n. Then clearly, $n \mid x^m$ for some integer $m \geq 1$. Hence, if n is square-free, then it is clear that 0 is the only nilpotent element of Z_n. $\square$

3.1 Partition Z_n when n is square-free

Recall that $n \in Z^+$ is called *square-free* if $n = q_1q_2...q_k$, where $q_1q_2...q_k$ are distinct prime integers, $e \in Z_n$ is an idempotent Z_n iff $e^2 = e$ in Z_n iff $e^2 \equiv e \pmod{n}$, and w is called nilpotent in Z_n iff $w^m = 0$ in Z_n iff $w^m \equiv 0 \pmod{n}$. Also; recall that if $k \mid n$, then $D_k = \{1 \le a < n \mid gcd(a, n) = k\}$.

Theorem 3.1.1. *If e is idempotent in Z_n, then $1 - e$ is also idempotent in Z_n.*

Proof. Suppose e is an idempotent in Z_n. Then $e^2 = e$ in Z_n. It follows that $(1-e)^2 = 1 - 2e + e^2 = 1 - e$. Therefore, $(1 - e)$ is also idempotent in Z_n. □

Note that if n is a square-free integer, then every proper factor of n is a perfect factor of n.

Theorem 3.1.2. *Let $n \ge 2$ be a square-free integer and $G = \{D_k \mid 1 \le k < n$ and $k \mid n\}$. Then D_k is a multiplicative group of Z_n with identity e_k for every proper factor k of n, $H \cap L = \emptyset$ for every $H, L \in G$, and $Z_n^* = \cup_{F \in G} F$, i.e., Z_n^* is the union of disjoint multiplicative groups of Z_n.*

Proof. Since n is square free, every proper factor $k \ge 1$ of n is a perfect factor of n. Hence D_k is a multiplicative group of Z_n with identity e_k for every proper factor $k \ge 1$ of n by Theorem 3.0.4. Let $H, L \in G$. Then $H = D_a$ and $L = D_b$ for some distinct perfect factors a, b of n. Hence, it is clear that $H \cap L = \emptyset$. Let $c \in Z_n^*$ and $k = gcd(c, n)$. Since k is a perfect factor of n, D_k is a multiplicative group of Z_n and $c \in D_k$. Thus $Z_n^* = \cup_{F \in G} F$, i.e., Z_n^* is the union of disjoint multiplicative groups of Z_n. □

In the following example, we illustrate using the CRT and Theorem 3.0.4 to construct all multiplicative groups of Z_{30}.

Example 3.1.1. *Let $n = 30 = 3 \cdot 5 \cdot 2$ is square-free. The goal is to obtain all the D_k multiplicative groups for each proper factor k of 30. The proper factors of 30 are $k = 1, 2, 3, 5, 6, 10, 15$. Each group will have an identity that is equal to one of the idempotents of Z_{30}.*

The number of idempotents for Z_{30} is $2^3 = 8$ by Theorem 3.0.6.

***Step 1: Find the multiplicative group** D_1*

$$D_1 = \{a \in \mathbb{Z} \mid 1 \le a < 30, \gcd(a, 30) = 1\} = \{1, 7, 11, 13, 17, 19, 23, 29\}$$

.

Note that $\phi(30) = (2-1)2^0 \cdot (3-1)3^0 \cdot (5-1)5^0 = 8 = |D_1|$

Step 2: Find identities of** D_k **using the CRT

Identity of D_6 *:*

$$e \equiv 0 \pmod{2}$$

$$e \equiv 0 \pmod{3}$$

$$e \equiv 1 \pmod 5$$

Since we have linear congruences, we will begin with the steps of CRT:
I) For $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$*,* $i = 1, 2, ..k$*, let each* $n_i = p_i^{\alpha_i}$ *and each* $m_i = n/n_i$
In our case,
$n_1 = 2$*,* $n_2 = 3$*,* $n_3 = 5$*,*$m_1 = 30/2 = 15$*,* $m_2 = 30/3 = 10$*, and* $m_3 = 30/5 = 6$
II) Find the multiplicative inverse of each m_i *in* Z_{n_i} *(meaning* $m_i y_i = 1$ *in* Z_{n_i}*)*
In our case,
a) $15y_1 = 1$ *in* Z_2
$y_1 = 1$ *in* Z_2
b) $10y_2 = 1$ *in* Z_3
$y_2 = 1$ *in* Z_3
c) $6y_3 = 1$ *in* Z_5
$y_3 = 1$ *in* Z_5
III) Calculate $e = r_1 m_1 y_1 + ... r_i m_i y_i$ $(mod\ n)$*, where each* r_i *is the remainder of* $e\ (mod\ (n_i))$ *(either 0 or 1 in our case). Hence since* $r_1, r_2 = 0$*,* $e_6 = r_3 m_3 y_3\ (mod\ 30) = 6$

Since $6 \cdot 5 = 0$*, the identity of* $D_5 = 1 - e_6 = 1 - 6 = -5\ (mod\ 30) = 25$

Identity of D_{10}*:*

$$e \equiv 0 \pmod 2$$
$$e \equiv 1 \pmod 3$$
$$e \equiv 0 \pmod 5$$

Note that $r_1 = r_3 = 0$*,* $m_2 = 10$*,* $r_2 = 1$ *and* $y_2 = 1$*. Hence* $e_{10} = r_2 m_2 y_2\ (mod\ 30) = 10$

Since $10 \cdot 3 = 0$*, the identity of* D_3 *is* $1 - e_{10} = -9\ (mod\ 30) = 21$

Identity of D_{15}*:*

$$e \equiv 1 \pmod 2$$
$$e \equiv 0 \pmod 3$$
$$e \equiv 0 \pmod 5$$

Note that $r_2 = r_3 = 0$*,* $m_1 = 15$*,* $r_1 = 1$ *and* $y_1 = 1$*. Hence* $e_{15} = r_1 m_1 y_1\ (mod\ 30) = 15$

Since $2 \cdot 15 = 0$*, the identity of* D_2 *is* $1 - e_{15} = -14\ (mod\ 30) = 16$

Step 3: Find the groups D_k

This is done by calculating $D_k = e_k D_1 = \{e_k \cdot a \mid a \in D_1\}$*, see Theorem 3.0.4. In other words, multiply the identity of* D_k *with every element in* D_1*.*

We get the following multiplicative groups of Z_n*:*
$D_1 = \{1, 7, 11, 13, 17, 19, 23, 29\}$*,* $e_1 = 1$ *and* $|D_1| = \phi(30) = 8$*.*

$D_2 = \{16, 22, 26, 28, 2, 4, 8, 14\}$*,* $e_2 = 16$ *and* $|D_2| = \phi(30/2) = \phi(15) = 8$*.*

$D_3 = \{21, 27, 3, 9\}$, $e_3 = 21$ and $|D_3| = \phi(30/3) = \phi(10) = 4$.

$D_5 = \{25, 5\}$, $e_5 = 25$ and $|D_5| = \phi(30/5) = \phi(6) = 2$.

$D_6 = \{6, 12, 18, 24\}$, $e_6 = 6$ and $|D_6| = \phi(30/6) = \phi(5) = 4$.

$D_{10} = \{10, 20\}$, $e_{10} = 10$ and $|D_{10}| = \phi(30/10) = \phi(3) = 2$.

$D_{15} = \{15\}$, $e_{15} = 15$ and $|D_{15}| = \phi(30/15) = \phi(2) = 1$.

Thus we have, $Z_{30}^* = D_1 \cup D_2 \cup D_3 \cup D_6 \cup D_{10}$.

3.2 Z_n When n is not square-free

We start with the following example.

Example 3.2.1. *Let $n = 18 = 3^2 \cdot 2$. Then n is not square-free. By Theorem 3.0.4, D_1, D_2, and D_9 are the only multiplicative groups of Z_{18}. Now $15 \notin D_i$ for every $i \in \{1, 2, 9\}$, but $15 = 9 + 6$. Note that $9 \in D_9$ and 6 is a nilpotent element of Z_{18} by Theorem 3.0.6.*

The set of all nilpotent elements of Z_n is denoted by $Nil(Z_n)$. We have the following result.

Theorem 3.2.1. *Let $n > 2$ be an integer and assume that n is not square-free. Let $a \in Z_n$ such that $a \notin Nil(Z_n)$. Suppose that a is not an element of every multiplicative group of Z_n. Then there is a multiplicative group D_d for some perfect factor d of n such that $a = f + w$ for some $f \in D_d$ and $w \in Nil(Z_n)$,*

Proof. Let $a \in Z_n$ such that a is not an element of every multiplicative group of Z_n. Assume that $a \notin Nil(R)$. Let e be the smallest nonzero idempotent of Z_n such that $k \mid e$. Hence every prime factor p of e is a prime factor of a. Since $e_k(1 - e_k) = 0$ in Z_n and $gcd(e_k, 1 - e_k) = 1$, we conclude that $w = a(1 - e) \in Nil(Z_n)$ by Theorem 3.0.6. Since $1 = (1 - e) + e$, we have $a = a(1 - e) + ae = w + ef$. Let $f = ae$ and $d = gcd(e, n)$. Then d is a perfect factor of n by Theorem 3.0.2. Hence $gcd(e, n) = gcd(ae, n) = d$ and $f = ae$ is an element of the multiplicative group D_d of Z_n. Thus $a = f + w$, for some $f \in D_d$ and $w \in Nil(Z_n)$, where D_d is a multiplicative group of Z_n for some perfect factor d of n. □

Example 3.2.2. *Consider Z_{18}. By Theorem 3.0.6, $Nil(Z_{18}) = \{0, 6, 12\} = D_6 \cup \{0\}$. By Theorems 3.0.3, 3.0.4, we conclude that D_1, D_2, D_9 are the only multiplicative groups of Z_{18}. By using the CRT as in the previous section, we get the following groups of Z_{18}:*

$D_1 = \{1, 5, 7, 11, 13, 17\}, e_1 = 1, |D_1| = \phi(18) = 6$

$D_2 = \{2, 4, 8, 10, 14, 16\}, e_2 = 10, |D_2| = \phi(18/2) = \phi(9) = 6$

$D_9 = \{9\}, e_9 = 9, |D_9| = \phi(18/9) = \phi(2) = 1$

Let $a \in Z_{18}$ such that $a \notin (Nil(Z_{18}) \cup D_1 \cup D_2 \cup D_3 \cup D_9)$. Then $a \in D_3 = \{3, 15\}$. Hence by Theorem 3.2.1, we have $3 = 9 + 12, 9 \in D_9, 12 \in Nil(Z_{18})$ and $15 = 9 + 6, 9 \in D_9, 6 \in Nil(Z_{18})$.

Hence we have, $Z_{18} = Nil(Z_{18}) \cup D_1 \cup D_2 \cup D_3 \cup D_9$.

4 Example of Caley's tables of multiplicative groups of Z_n

$(D_2, \bullet_{\text{mod}10})$	**2**	**4**	**6**	**8**
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

$(D_3, \bullet_{\text{mod}21})$	**3**	**6**	**9**	**12**	**15**	**18**
3	9	18	6	15	3	12
6	18	15	12	9	6	3
9	6	12	18	3	9	15
12	15	9	3	18	12	6
15	3	6	9	12	15	18
18	12	3	15	6	18	9

$(D_7, \bullet_{\text{mod}21})$	7	14
7	7	14
14	14	7

$(D_2, \bullet_{\text{mod}30})$	**2**	**4**	**8**	**14**	**16**	**22**	**26**	**28**
2	4	8	16	28	2	14	22	26
4	8	16	2	26	4	28	14	22
8	16	2	6	22	8	26	28	14
14	28	26	22	16	14	8	4	2
16	2	4	8	14	16	22	26	28
22	14	28	26	8	22	4	2	16
26	22	14	28	4	26	2	16	8
28	26	22	14	2	28	16	8	4

$(D_3, \bullet_{\text{mod}30})$	**3**	**9**	**21**	**27**
3	9	27	3	21
9	27	21	9	3
21	3	9	21	27
27	21	4	27	9

$(D_5, \bullet_{\text{mod}30})$	5	25
5	25	5
25	5	25

$(D_6, \bullet_{\text{mod}30})$	**6**	**12**	**18**	**24**
6	6	12	18	24
12	12	24	6	18
18	18	6	24	12
24	24	18	12	6

$(D_9, \bullet_{\text{mod}36})$	**9**	**27**
9	9	27
27	27	9

$(D_4, \bullet_{\text{mod}36})$	**4**	**8**	**16**	**20**	**28**	**32**
4	16	32	28	8	4	20
8	32	28	20	16	8	4
16	28	20	4	32	16	8
20	8	16	32	4	20	28
28	4	8	16	20	28	32
32	20	4	8	28	32	16

D2, ._18	2	4	8	10	14	16
2	4	8	16	2	10	14
4	8	16	14	4	2	10
8	16	14	10	8	4	2
10	2	4	8	10	14	16
14	10	2	4	14	16	8
16	14	10	2	16	8	4

5 Conclusion

. In this project, we used the Chinese Remainder Theorem (CRT) to construct multiplicative groups of Z_n with an identity different from one. If n is square-free, we showed that Z_n^* is the union of disjoint multiplicative groups of Z_n. If n is not square-free, we constructed all multiplicative groups of Z_n and showed that if an element $a \in Z_n \setminus Nil(Z_n)$ such that a is not an element of every multiplicative group of Z_n, then there is a multiplicative group D_d for some perfect factor d of n such that $x = f + w$ for some $f \in D_d$ and $w \in Nil(Z_n)$, In the future, we will look at other problems where the CRT applies.

References

[1] Ayman Badawi, Abstract Algebra Manual: Problems and Solutions, Nova Science Publications, USA, 2004.

[2] Joseph A. Gallian, Contemporary Abstract Algebra, Brooks/Cole, USA, 2022.