A short note on generation of class of rings with subrings having different multiplicative identity than the ring

Manasi Athale
Rahul Athale
Research Institute for Symbolic Computation,
Johannes Kepler university, Linz, Austria
E-mail: `manasi,athale@risc.uni-linz.ac.at`

Abstract

The short note demonstrates how one can use the theorem of existence of solution for linear congruence to generate a class of rings which has subrings with different multiplicative identity than the ring itself. The note also describes the method to generate the subrings with this property and gives some examples.

1 Introduction

In the basic books on Algebra, like [3, 1], there are many exercises on the topic subrings. One of such exercise is at the heart of this paper. We wanted to generate a class of rings which will generate lots of examples for subrings with different identity than the ring. We need some prerequisites from number theory which we note in the next section and then prove the main theorem of the paper. In the last section we generate some examples.

2 Main Theorem

The goal of the note is to describe a method to generate the subrings of $\mathbb{Z}_n$ which have different multiplicative identity than 1. We will need the following theorems to prove our result, see [2, 4].

Theorem 1. *The congruence*

$$ax \equiv b \mod c$$

has a solution if and only if $\gcd(a, c) \mid b$*. Additionally, if solutions exist then there are* $\gcd(a, c)$ *unique solutions.*

Theorem 2. *$ax \equiv ay \mod m$ if and only if $x \equiv y \mod \frac{m}{\gcd(a,m)}$*

Now using theorem 1 let us prove the main theorem. This theorem will give us an algorithm to find for which values of n we can have subrings R with different multiplicative identity than 1.

Theorem 3. *For every $n \in \mathbb{N}, n$ is divisible by two or more primes if and only if $\mathbb{Z}_n$ has a proper subring whose multiplicative identity is not equal to 1.*

Proof:
Let us suppose that n is divisible by only one prime, say p, i.e. let $n = p^m$, for some $m \in \mathbb{N}$ and $m > 1$. We have to prove that every proper subring of $\mathbb{Z}_n$ either has 1 as identity or it has no identity. Suppose that i is the identity of the proper subring $R \subsetneq \mathbb{Z}_n$. Then i should satisfy following congruence relation

$$i^2 \equiv i \mod n. \tag{1}$$

Now let us look at the structure of the subrings R.

$$R = \{0, p^k, 2p^k \ldots, jp^k, \ldots, (p^{m-k} - 1)p^k \mid 0 \leq j \leq p^{m-k} - 1, 0 < k \leq m - 1\}.$$

Now by substituting $i = jp^k$ and $n = p^m$ in congruence (1), we get

$$(jp^k)^2 \equiv jp^k \mod p^m.$$

Using theorem 2, we get,

$$(jp^k) \equiv 1 \mod \frac{p^m}{\gcd(jp^k, p^m)}.$$

Let us find the value of j. Here, we are not interested in the case $j = 0$. The $\gcd(jp^k, p^m) < p^m$ for all possible values of j, so after simplification the congruence will be

$$(jp^k) \equiv 1 \mod p^r \quad \text{where } r \geq 1. \tag{2}$$

The $\gcd(p^k, p^r) \geq p$ and $p \nmid 1$, so by theorem 1 the congruence (2) will have no solution. So congruence in (1) does not hold for any value of i. This is a contradiction. So our assumption of existence of identity was wrong.

Let us now prove that if n is divisible by two or more primes then we can find a proper subring R of $\mathbb{Z}_n$ which has multiplicative identity different than 1. We will prove it when $n = pq$, where $\gcd(p, q) = 1$.

Let $R = \{0, p, 2p, \ldots, (q-1)p\} \subset \mathbb{Z}_n$. Let us assume that i is the identity of R and as R does not contain 1, it will prove the result. The identity i should satisfy the congruence (1). As every element of the ring R is of the form jp, where $0 \leq j \leq (q-1)$, we can write the congruence (1) as

$$(jp)^2 \equiv jp \mod pq.$$

Using theorem 2, we get,

$$jp \equiv 1 \mod \frac{pq}{\gcd(jp, pq)}. \tag{3}$$

The $\gcd(jp, pq) = p$ as $0 \le j \le q-1$ and we are not interested in the case where $j = 0$, so the congruence (3) becomes

$$jp \equiv 1 \mod q. \tag{4}$$

The $\gcd(jp, q) = 1$, which divides 1 on the right hand side of the congruence (4), so by theorem 1, we get the unique value for j and then $i = jp$ is a good candidate for the identity of the subring R. Now we will prove that indeed i is the identity of the subring. Let us consider an element $r = sp \in R$. Consider the congruence $jp \equiv 1 \mod q$. By theorem 2, we get $jp * kp \equiv kp \mod pq$, as the $\gcd(kp, pq) = p$ for all $0 < k < q-1$. For $k = 0$, the two sides of the congruence are equal to 0. So $i = jp$ is the identity of the subring which is distinct from 1.

We can prove this result in the same manner as above in the case where $gcd(p, q) = 1$ with minor changes in the proof. This proves the claim for any n with more than two distinct prime divisors.

3 Examples

In this section, we will see the theorem in action which we proved in the last section.

Example 1. Let $n = 6 = 2 * 3, p = 2, q = 3$.
Consider $R = \{0, 2, 4\} \subset \mathbb{Z}_6$. Applying theorem 3, to get the identity of R, we have to solve the congruence $2j \equiv 1 \mod 3$. The answer is $j = 2$ and the identity is $i = 2 * 2 = 4$.

Now, we will see how we can use the theorem 3 for n, which is divisible by more than two primes.

Example 2. Let $n = 30 = 2 * 3 * 5, p = 5, q = 6$.
Consider $R = \{0, 5, 10, 15, 20, 25\} \subset \mathbb{Z}_{30}$. Applying theorem 3, to get the identity of R, we have to solve the congruence $5j \equiv 1 \mod 6$. We can compute the answer by hand or by using any computer algebra system, for example, Maple or Mathematica. The answer is $j = 5$ and the identity is $i = 5 * 5 = 25$.

Now, we will see how we can use the theorem 3 for n, which is divisible by square of product of two primes.

Example 3. Let $n = 36 = 2 * 2 * 3 * 3, p = 9, q = 4$.
Consider $R = \{0, 9, 18, 27\} \subset \mathbb{Z}_{36}$. Applying theorem 3, to get the identity of R, we have to solve the congruence $9j \equiv 1 \mod 4$. We can compute the answer by hand and the answer is $j = 1$ and the identity is $i = 9 * 1 = 9$.

Finally, let us see how we can find the subring when n is a larger number, with more than two prime divisors.

Example 4. Let $n = 450 = 2 * 3 * 3 * 5 * 5, p = 225, q = 2$.
Consider $R = \{0, 225\} \subset \mathbb{Z}_{450}$. Applying theorem 3, to get the identity of R, we have to solve the congruence $225j \equiv 1 \mod 2$. We can compute the answer by hand and the answer is $j = 1$ and the identity is $i = 225 * 1 = 225$.

References

[1] P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. **Basic Abstract Algebra.** First Indian Edition, Cambridge University Press, 1995.

[2] M. Herkommer. **Number Theory, A Programmer's Guide.** McGraw-hill, 1999.

[3] I. N. Herstein. **Topics in Algebra.** Second Edition, Wiley Eastern Limited, June 1992.

[4] I. Niven, H. Zuckerman. **An Introduction to The Theory of Numbers.** Third Edition, John Wiley and Sons Inc., 1972.