Prime and irreducible elements of the ring of integers modulo n

Mohammad Hossein Jafari and Ali Reza Madadi

Department of Pure Mathematics, Faculty of Mathematical Sciences

University of Tabriz, Tabriz, Iran

Abstract

In this paper we obtain a characterization of prime and irreducible elements of the ring of integers modulo n. Also we give an explicit formula for computing the number of primes and irreducibles of this ring.

Keywords: Divisibility, Prime element, Irreducible element, Ring of integers modulo n, Euler function.

AMS subject classification: Primary 13A05; Secondary 11A25.

1 Introduction

Divisibility is an important concept in number theory and it generalizes to rings, here always assumed commutative with multiplicative identity element 1, and where concepts such as factorization of elements, prime elements, and irreducible elements can be defined. Although these concepts are most important in integral domains, nonetheless they are of some interest in more general rings also.

For elements a and b in the set of integer numbers $\mathbb{Z}$ and a natural number n, we denote by $[a]_n$ and (a, b), the congruence class of a modulo n, and the greatest common divisor of a and b, respectively. So the ring of integers modulo n, $\mathbb{Z}_n$, is the set $\{[a]_n : a \in \mathbb{Z}\}$ .This ring is one of the simplest and most important examples in ring theory. Many subsets of $\mathbb{Z}_n$ with a particular property are easy to identify explicitly. For example, $U(\mathbb{Z}_n)$, the set of units of $\mathbb{Z}_n$, is $\{[a]_n \in \mathbb{Z}_n : (a, n) = 1\}$, and the set of zero-divisors of $\mathbb{Z}_n$ is the complement of $U(\mathbb{Z}_n)$ in $\mathbb{Z}_n$.

In this paper, we give a characterization of prime and irreducible elements of $\mathbb{Z}_n$ which perhaps deserves to be more known than it seems to be.

2 Primes of $\mathbb{Z}_n$

Our notation and terminology are standard and follow [1]. Throughout R will denote a commutative ring with 1. First we recall the definition of a prime element. For $a, b \in R$, a is said to *divide* b (symbolically $a \mid b$) if for some $c \in R$, $b = ac$. So, for example, $a \mid a$, and $a \mid 0$, for every $a \in R$. Also, $a \in R$ is a unit iff $a \mid 1$. A nonzero nonunit element $p \in R$ is called *prime* if whenever $p \mid ab$ with $a, b \in R$, then either $p \mid a$ or $p \mid b$. For example, the reader might like to check that in $\mathbb{Z}_6$ the primes are $[2]_6$, $[3]_6$, $[4]_6$, and in $\mathbb{Z}_{12}$ they are $[2]_{12}$, $[3]_{12}$, $[9]_{12}$, $[10]_{12}$. For the sake of simplicity denote by π_n the set of positive prime divisors of the natural number n in $\mathbb{Z}$.

In the sequel, we write $a \mid b$ to mean divisibility is in $\mathbb{Z}$ and $[a]_n \mid [b]_n$ to mean divisibility is in $\mathbb{Z}_n$. Before giving the main theorem of this section, we state an easy lemma whose proof is omitted.

Lemma 2.1 *Let $[a]_n, [b]_n \in \mathbb{Z}_n$. Then $[a]_n \mid [b]_n$ iff $(a, n) \mid (b, n)$.*

In the following theorem the prime elements of $\mathbb{Z}_n$ will be characterized.

Theorem 2.2 *The set of prime elements of $\mathbb{Z}_n$ is*

$$\{[a]_n \in \mathbb{Z}_n : \exists\, p \in \pi_n, p < n, (a, n) = p\}.$$

Proof. Let $[a]_n \in \mathbb{Z}_n$ be a nonzero nonunit element. So $(a, n) \neq 1$ and $n \nmid a$.

We will have three distinct cases:

1) There exist two distinct primes p, q such that $pq \mid (a, n)$. In this case we show that $[a]_n$ is not a prime element.

Suppose that $a = bc$ where $p \nmid c$ and $q \nmid b$. Thus $p \mid b$ and $q \mid c$ and also $[a]_n \mid [b]_n[c]_n$. If $[a]_n \mid [b]_n$, then by the above Lemma $(a, n) \mid (b, n)$, a contradiction. By a similar argument we have $[a]_n \nmid [c]_n$. Therefore, $[a]_n$ is not prime.

2) There exist a prime p and natural number $k \geq 2$, such that $(a, n) = p^k$. Again we show that $[a]_n$ is not a prime element.

Let $a = p^m b$, where $m \geq k$ and $p \nmid b$. By division algorithm there exist two integers r and s such that $m = r(k-1) + s$, $1 \leq r$ and $0 \leq s < k-1$. Thus $a = (p^{k-1})^r (p^s b)$ and so $[a]_n \mid ([p^{k-1}]_n)^r [p^s b]_n$. If $[a]_n \mid [p^{k-1}]_n$, then by the above Lemma $p^k = (a, n) \mid (p^{k-1}, n) = p^{k-1}$, a contradiction. If $[a]_n \mid [p^s b]_n$, then by the same Lemma $p^k = (a, n) \mid (p^s b, n) = p^s$, which is again a contradiction. Therefore, $[a]_n$ is not prime.

3) There exists a prime p such that $(a, n) = p$. We show that $[a]_n$ is prime.

First note that $p < n$ because $n \nmid a$. Also, we have $(a, n) = p = (p, n)$. So by the above Lemma $[a]_n \mid [p]_n$ and $[p]_n \mid [a]_n$. Suppose that $[a]_n \mid [b]_n [c]_n$, where $[b]_n, [c]_n \in \mathbb{Z}_n$. Thus there exist integers r, s such that $bc = ar + ns$. So p must divide either b or c. Let, say, $p \mid b$. Then $[p]_n \mid [b]_n$ and since $[a]_n \mid [p]_n$, we get $[a]_n \mid [b]_n$.

As an easy corollary, we have:

Corollary 2.3 *The ring $\mathbb{Z}_n$ has no prime elements iff either $n = 1$ or n is a prime.*

3 Irreducibles of $\mathbb{Z}_n$

Recall that a nonzero nonunit element p of R is said to be *irreducible* if whenever $p = ab$ with $a, b \in R$, then either a or b is a unit of R. For example, again the reader might like to check that $\mathbb{Z}_6$ has no irreducible elements, whereas $[2]_{12}$ and $[10]_{12}$ are the only irreducible elements in $\mathbb{Z}_{12}$.

The characterization of the irreducible elements of $\mathbb{Z}_n$ is given in the following theorem.

Theorem 3.1 *The set of irreducible elements of $\mathbb{Z}_n$ is*

$$\{[a]_n \in \mathbb{Z}_n : \exists\, p \in \pi_n, p^2 \mid n, (a, n) = p\}.$$

Proof. Let $[a]_n$ be a nonzero nonunit of $\mathbb{Z}_n$. So $(a, n) \neq 1$ and $n \nmid a$.

Three distinct cases will occur:

1) There exist two primes p, q (not necessarily distinct) such that $pq \mid (a, n)$. In this case we show that $[a]_n$ is not irreducible.

Let $a = bc$ where $p \mid b$ and $q \mid c$. Then we have $[a]_n = [b]_n[c]_n$. It is obvious that $[b]_n$ and $[c]_n$ are nonzero nonunit elements. So $[a]_n$ is not irreducible.

2) There exists a prime p such that $(a, n) = p$ and $p^2 \nmid n$. Again we show that $[a]_n$ is not irreducible.

In this case we have $(n, p^2) = p$ and $p \mid a$, so there exists $r, s \in \mathbb{Z}$ with $a = nr + p^2 s$. So we obtain $[a]_n = [p]_n[ps]_n$. Again it is obvious that $[p]_n$ and $[ps]_n$ are nonzero nonunit elements. So $[a]_n$ is not irreducible.

3) There exists a prime p such that $(a, n) = p$ and $p^2 \mid n$. In this case we show that $[a]_n$ is irreducible.

Let $[b]_n, [c]_n \in \mathbb{Z}_n$ and $[a]_n = [b]_n[c]_n$. Then there is an integer k such that $a = bc + kn$. By hypothesis, $p \mid bc$ and so p must divide at least one of b, c. It cannot divide both, else, since $p^2 \mid n$, we would have $p^2 \mid a$, a contradiction. Let, say, $p \mid b$ and $p \nmid c$. Now if there exists $q \in \pi_n - \{p\}$, then $q \nmid c$, for $(a, n) = p$. Thus $(c, n) = 1$ and so $[c]_n$ is a unit. This completes the proof.

One of the consequences of the above theorem is the following:

Corollary 3.2 *The ring $\mathbb{Z}_n$ has no irreducible elements iff either $n = 1$ or n is squarefree.*

As seen in the previous examples $\mathbb{Z}_6$ and $\mathbb{Z}_{12}$, in general the primes of $\mathbb{Z}_n$ are not necessarily irreducible. The converse, however, is true.

Corollary 3.3 *Every irreducible element of $\mathbb{Z}_n$ is a prime element.*

4 The number of primes and irreducibles of $\mathbb{Z}_n$

In this last section we give an explicit formula for computing the number of prime and irreducible elements of $\mathbb{Z}_n$. First we prove a general theorem from which our formula will be derived.

Theorem 4.1 *Let n be a natural number, $p \in \pi_n$ and $m = \frac{n}{p}$. Let also $A_p = \{[a]_n \in \mathbb{Z}_n : (a, n) = p\}$. Then the map $f : A_p \to U(\mathbb{Z}_m)$ defined by $f([a]_n) = [\frac{a}{p}]_m$ is well-defined, one-to-one and onto.*

Proof. Suppose that $[a]_n, [b]_n \in A_p$. Then $(a, n) = p = (b, n)$ and so $(\frac{a}{p}, m) = 1 = (\frac{b}{p}, m)$. Therefore, $[\frac{a}{p}]_m, [\frac{b}{p}]_m \in U(\mathbb{Z}_m)$. Since

$$\begin{aligned} [a]_n = [b]_n &\Leftrightarrow n \mid a - b \\ &\Leftrightarrow m \mid \frac{a}{p} - \frac{b}{p} \\ &\Leftrightarrow [\frac{a}{p}]_m = [\frac{b}{p}]_m \end{aligned}$$

thus f is a well-defined and one-to-one function.

Now let $[c]_m \in U(\mathbb{Z}_m)$ be arbitrary. So $(c, m) = 1$. We define a as follows:

$$a = \begin{cases} pc & (p, c) = 1 \\ p(c + m) & (p, c) = p \end{cases}$$

It is easy to check that $(a, n) = p$ and $f([a]_n) = [c]_m$. Therefore, f is also onto.

The number of prime and irreducible elements of $\mathbb{Z}_n$ is given in the following corollary.

Corollary 4.2 *i) The number of prime elements of $\mathbb{Z}_n$ is*

$$\sum_{p \in \pi_n,\, p < n} \varphi(\frac{n}{p}),$$

ii) The number of irreducible elements of $\mathbb{Z}_n$ is

$$\sum_{p \in \pi_n,\, p^2 | n} \varphi(\frac{n}{p}),$$

where φ is the Euler function.

Proof. By using the previous theorem, theorem 2.2 and theorem 3.1, we have

$$\{[a]_n \in \mathbb{Z}_n : \exists\, p \in \pi_n, p < n, (a, n) = p\} = \overset{\circ}{\bigcup_{p \in \pi_n,\, p < n}} A_p,$$

$$\{[a]_n \in \mathbb{Z}_n : \exists\, p \in \pi_n, p^2 \mid n, (a,n) = p\} = \overset{\circ}{\bigcup_{p\in\pi_n,\, p^2|n}} A_p,$$

and the result immediately follows.

References

[1] D. S. Malik, J. M. Mordeson and M. K. Sen, *Fundamentals of Abstract Algebra*, The McGraw-Hill Companies, Inc., 1997.

E-mail:jafari@tabrizu.ac.ir

E-mail:a-madadi@tabrizu.ac.ir