THE MULTIPLICATIVE GROUP \((\mathbb{Z}/n\mathbb{Z})^*\)

Contents

1. Introduction 1
2. Preliminary results 1
3. Main result 2
4. Some number theoretic consequences : 3

1. INTRODUCTION

Let \(n\) be a positive integer, and consider \(\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}\). If \(\bar{a}\) and \(\bar{b}\) are elements of \(\mathbb{Z}/n\mathbb{Z}\), we defined

\[\bar{a} \cdot \bar{b} = \overline{ab} .\]

By Lemma 2.9.6 in Artin, this product is well-defined, i.e., it does not depend on the choice of integers \(a, b\). We let \((\mathbb{Z}/n\mathbb{Z})^*\) = \(\{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}\). The purpose of these notes is to show that \((\mathbb{Z}/n\mathbb{Z})^*\) is a group under multiplication.

2. PRELIMINARY RESULTS

First, we prove some preliminary results.

Lemma 2.1. Let \(a, b \in \mathbb{Z}\). Then \(\bar{a} = \bar{b}\) if and only if \(b = a + kn\) for some \(k \in \mathbb{Z}\).

The previous lemma follows easily from the definition of \(\mathbb{Z}/n\mathbb{Z}\), and we omit its proof.

Lemma 2.2. Let \(a, b \in \mathbb{Z}\). Suppose \(\bar{a} = \bar{b}\) in \(\mathbb{Z}/n\mathbb{Z}\).

(1) Then \(\gcd(a, n) = \gcd(b, n)\).

(2) In particular, \(\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*\) if and only if \(\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*\).

Proof: By Lemma 2.1, \(b = a + kn\) for some \(k \in \mathbb{Z}\). By Problem 1 from problem set 3, \(\gcd(b, n) = \gcd(a, n)\). This proves (1). For (2), note that by definition of \((\mathbb{Z}/n\mathbb{Z})^*\), \(\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*\) if and only if \(\gcd(a, n) = 1\). By Part (1), \(\gcd(a, n) = 1\) if and only if \(\gcd(b, n) = 1\), which is equivalent to \(\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*\).

Q.E.D.
Note that assertion (2) in the Lemma shows that \((\mathbb{Z}/n\mathbb{Z})^*\) is a well-defined set, i.e., whether \(\overline{a}\) is in \((\mathbb{Z}/n\mathbb{Z})^*\) depends only on \(\overline{a}\) and not on \(a\).

**Lemma 2.3.** Let \(a, b \in \mathbb{Z}\). Then \(\gcd(a, b) = 1\) if and only if there exist \(m, n \in \mathbb{Z}\) such that \(am + bn = 1\).

This was proved in class, as a consequence of Proposition 2.2.6 in Artin.

**Lemma 2.4.** Let \(a, b \in \mathbb{Z}\) and suppose \(\gcd(a, n) = \gcd(b, n) = 1\). Then \(\gcd(ab, n) = 1\).

**Proof:** By Lemma 2.3, there are \(r, s, x, y \in \mathbb{Z}\) such that \(ar + ns = 1\) and \(bx + ny = 1\). Thus,

\[
1 = (ar + sn)(bx + ny) = abrx + n(ary + bsx + xny).
\]

Thus, again by Lemma 2.3, \(\gcd(ab, n) = 1\).

Q.E.D.

### 3. Main result

We now show that \((\mathbb{Z}/n\mathbb{Z})^*\) is a group under multiplication.

**Proposition 3.1.** Let \(G = (\mathbb{Z}/n\mathbb{Z})^*\). The \(G\) is an abelian group under multiplication.

**Proof:** We first show that multiplication is a law of composition on \(G\). For \(\overline{a}, \overline{b} \in G\), then \(\gcd(a, n) = 1 = \gcd(b, n)\). Thus, \(\gcd(ab, n) = 1\) by Lemma 2.4. Thus, \(\overline{ab} \in G\).

Q.E.D.

We now check the group axioms. For \(\overline{a}, \overline{b}, \overline{c} \in G\), then

\[
(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{abc} = \overline{a} \cdot (\overline{b} \cdot \overline{c})
\]

(this was checked in class; see also the comment after Lemma 2.9.6 in Artin). Thus, multiplication is associative on \(G\). Similarly, multiplication is commutative. We take as the identity \(\overline{1}\). Certainly, \(\gcd(1, n) = 1\), so \(\overline{1} \in G\). Further, if \(\overline{a} \in G\), then

\[
\overline{a} \cdot \overline{1} = \overline{a} = \overline{a} \cdot \overline{1},
\]

so \(\overline{1}\) satisfies the property of the identity. Finally, let \(\overline{a} \in G\), so \(\gcd(a, n) = 1\). By Lemma 2.3, there exist \(x, y \in \mathbb{Z}\) such that \(ax + ny = 1\). Hence, by definition on \(\mathbb{Z}/n\mathbb{Z}\),

\[
\overline{a}x + \overline{ny} = \overline{1}.
\]

Since \(\overline{ny} = \overline{0}\),

\[
\overline{a} \cdot \overline{x} = \overline{1},
\]

and by commutativity, \(\overline{x} \cdot \overline{a} = \overline{1} \in G\). But certainly, \(ax + ny = 1\) implies that \(xa + ny = 1\), so \(\gcd(x, n) = 1\) by Lemma 2.3, and \(\overline{x} \in G\).

Q.E.D.
4. Some number theoretic consequences:

We continue to let $G = (\mathbb{Z}/n\mathbb{Z})^*$, and we define
\[ \phi(n) = |G|, \] the cardinality of the set $G$. By 2.6.12 on p. 58 of Artin, since $\mathbb{1}$ is the identity of $G$, for each $\overline{a} \in G$, then $\overline{a}^{\phi(n)} = \mathbb{1}$. The following theorem of Euler is an easy consequence (groups did not exist yet when Euler was around).

**Theorem 4.1.** $a^{\phi(n)} \equiv 1 \pmod{n}$.

For this statement to be useful, we need to be able to compute $\phi(n)$.

**Lemma 4.2.** Let $p$ be prime and let $k$ be a positive integer. Then $\phi(p^k) = p^k - p^{k-1}$. In particular, $\phi(p) = p - 1$.

**Proof:** Let $S = \mathbb{Z}/p^k\mathbb{Z} - G$, so $S = \{ \overline{a} \in \mathbb{Z}/p^k\mathbb{Z} : \gcd(a, p^k) > 1 \}$. Using properties of prime numbers, it is easy to check that $\overline{a} \in S$ if and only if $p$ divides $a$. Thus, $S = \{ sp : 0 \leq sp \leq p^k - 1, s \in \mathbb{Z} \}$, so $S = \{ 0, p, 2p, \ldots, (p^{k-1} - 1)p \}$, and in particular, $|S| = p^{k-1}$. But by the definition of $S$, $|S| = |\mathbb{Z}/p^k\mathbb{Z}| - |G|$, so $|G| = p^k - p^{k-1}$.

**Q.E.D.**

**Theorem 4.3.** Let $m, n$ be positive integers. If $\gcd(m, n) = 1$, then $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.

We will prove this when we discuss chapter 10 of Artin, which should happen late this semester.

The previous theorem implies that we can compute $\phi(n)$ by knowing the prime factorization of $n$. Indeed, if we write $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ as a product of distinct primes of $\mathbb{Z}$, then by Theorem 4.3, Lemma 4.2, and an easy calculation,

\[ \phi(n) = \prod_{i=1}^{k} \phi(p_i^{r_i}) = \prod_{i=1}^{k} (p_i^{r_i} - p_i^{r_i-1}) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}). \]

We note one additional consequence, which is called Fermat’s Little Theorem.

**Theorem 4.4.** If $a \in \mathbb{Z}$ and $p$ is prime, then $a^{p-1} \equiv 1 \pmod{p}$.

**Proof:** Since $\phi(p) = p - 1$ by Lemma 4.2, it follows from Euler’s Theorem 4.1 that $a^{p-1} \equiv 1 \pmod{p}$ if $\gcd(a, p) = 1$. By multiplying each side by $a$, we obtain $a^p \equiv a \pmod{p}$, so this proves the result when $\gcd(a, p) = 1$. If $\gcd(a, p) > 1$, then $p$ divides $a$ by properties of primes, so $a \equiv 0 \pmod{p}$, and hence $a^p \equiv 0^p \equiv 0 \pmod{p}$.

**Q.E.D.**

**Remark 4.5.** It is easy to check that $\phi(2) = 1$. If you compute values of $\phi(n)$ for $n > 2$, you see experimentally that $\phi(n)$ is always even. It is interesting to try to prove that $\phi(n)$ is even just using group theory. A hint for this is that if there exists any $a \in (\mathbb{Z}/n\mathbb{Z})^*$ of even order $m$, then $m$ divides $\phi(n)$ by Lagrange’s theorem, so $2$ also divides $\phi(n)$. I learned this argument from a student in this course circa 2002.