MODULAR ARITHMETIC

MATTHEW MORGADO

Abstract. We begin with integer arithmetic, proving the division theorem, and defining greatest common divisors and relative primeness. We move onto the definitions of a ring and field, and then establish the system of modular arithmetic. Finally, we show that, under given addition and multiplication operations, $\mathbb{Z}/m\mathbb{Z}$ is a ring for any positive integer m; and that $\mathbb{Z}/p\mathbb{Z}$ is a field for any prime integer p.

Contents

1. Introduction

I begin this paper by discussing the rudiments of integer arithmetic. The Greek mathematician Euclid, working in the 300s B.C., formalized many fundamental results in this field. For instance, he developed an algorithm for finding the greatest common divisor of any two numbers [Euclid, Book VII, Propositions 1, 2]. Such fundamental results will be discussed in Section One.

I also discuss the system of modular arithmetic. The early Chinese, Indian, and Islamic cultures mainly encountered modular arithmetic in a special form - astronomical and calendrical problems. Modular arithmetic was also considered in purely mathematical contexts, such as in Sun Zi's Mathematical Manual. In the 1700s, Swiss mathematician Leonard Euler pioneered the modern conception of modular arithmetic. And in 1801, Friedrich Gauss, a German, further developed the subject, and even introduced congruence notation still used today [Berggren].

Modular arithmetic has been applied to fields ranging from number theory to computer science. Theoretically, it serves as a foundation for number theory, and its generalizations have led to developments in modern algebra [Berggren]. Practically, it is applied in many computer-based operations involving cryptography. For instance, modular arithmetic can be used to create ciphers for computer encryptions [Conrad, 8,11]. Since modular arithmetic is so crucial to both theoretical

and practical endeavors, it warrants close study, together with its roots in integer arithmetic.

2. Integer Arithmetic

In this section, we begin by proving the Division Theorem. We also define several key terms - in particular, integer division, a greatest common divisor, and relative primeness. The Division Theorem and these definitions are utilized, to prove an assortment of fundamental lemmas, propositions and theorems - all of which form the basis of modular arithmetic, which will be discussed in Section 3.

Theorem 2.1. *Consider integers a and b, with $b > 0$. Then there exist integers q and r such that $a = qb + r$, with $0 \leq r < b$. This statement is known as the Division Theorem.*

Proof. Consider the set $A = \{a - xb : x \in \mathbb{Z}\}$. This set includes nonnegative elements. For instance, if $a \geq b$, let x equal one; if $a \leq b$, let x be a sufficiently large negative number, such that $xb \leq a$. Define $r = a - qb$ to be the least nonnegative element in A. By definition, we know $r \geq 0$. We claim that $r < b$. If not, then $r = a - qb \geq b$, which implies $a - qb - b \geq 0$. This inequality means $a - qb > a - (q+1)b \geq 0$, or $r > a - (q+1)b \geq 0$. Because $(q+1)$ is an integer, $a - (q+1)b$ is in A, and is a nonnegative element less than the least nonnegative element in A. But this statement is a logical contradiction. Therefore, we know $r < b$. In sum, $a = qb + r$, with $0 \leq r < b$. □

Theorem 2.2. *Consider integers a and b, and the set $A = \{ax + by : x, y \in \mathbb{Z}\}$. Then there exists a nonnegative integer d such that the set $B = \{dz : z \in \mathbb{Z}\}$ is equal to A.*

Proof. If both a and b equal zero, then we may let d equal zero. Now assume that a and b are both not zero. Then A contains positive elements. Define d to be the least positive element in A. Hence, there exist integers x' and y' such that $d = ax' + by'$. For any element dz in B, $dz = (ax' + by')z = a(x'z) + b(y'z)$, so dz is in A. In other words, we have $B \subseteq A$.

Now, consider any $c = ax + by$ in A. Since we know $d > 0$ by our definition, we also know by Theorem 2.1, that there exist integers q and r with $c = qd + r$, and $0 \leq r < d$. This statement implies that

$$\begin{aligned} r = c - qd &= (ax + by) - q(ax' + by') \\ &= ax + by - a(qx') - b(qy') \\ &= a(x - qx') + b(y - qy'). \end{aligned}$$

Hence, r is nonnegative and in A. Since, by our definition, d is the least positive element in A, r must equal zero. Otherwise, we would have a contradiction regarding d's minimality - i.e. there exists a positive r in A, such that r is less than the least positive element in A. So, we have $c = qd + 0 = qd$ in B. Since we could have chosen any c in A, it follows that every c in A is also in B. But this statement just means $A \subseteq B$. Therefore, we know $A = B$. □

Definition 2.3. We say an integer a *divides* an integer b, if there exists an integer c such that $b = ac$. We write a *divides* b as $a|b$.

Lemma 2.4. *If $a|b$ and $a|c$ hold, then $a|(b + c)$.*

Proof. By definition, $a|b$ means there exists some integer d, such that $b = ad$. Again, $a|c$ means there exists some integer e, such that $c = ae$. Combining these two facts, we have

$$b + c = ad + ae = a(d + e).$$

This equation simply means that $a|(b + c)$, since $(d + e)$ is an integer. □

Lemma 2.5. *If $a|b$ and $b|a$ hold, then either $a = -b$ or $a = b$.*

Proof. Assume $a, b = 0$. Clearly, $a = b$ and $a = -b$ are both true.

Assume $a \neq 0$ and $b = 0$ hold. Then $0|a$ cannot be the case, for any integer multiplied by zero, equals zero. Hence, we do not consider this case. Now assume $a = 0$ and $b \neq 0$ hold. By the same reasoning, $0|b$ cannot be the case; and so we do not consider this case either.

Next assume that $a, b \neq 0$. By definition, $a|b$ means there exists an integer x, such that $ax = b$. Again, $b|a$ means there exists an integer y, such that $by = a$. This last equation implies $b(yx) = ax = b$. Hence, we have the equation $yx = 1$, which occurs when $y, x = 1$ or when $y, x = -1$. If $y, x = -1$, then $by = a$ means $-b = a$. If $y, x = 1$, then $by = a$ means $b = a$. So, after reviewing both cases, we know either $a = -b$ or $a = b$. □

Definition 2.6. We say the integer d is a *greatest common divisor* of integers a and b if:
(1) $d|a$ and $d|b$ hold; and
(2) $c|a$ and $c|b$ implies $c|d$.

Lemma 2.7. *The greatest common divisor of two integers a and b, if it exists, is determined up to sign.*

Proof. Consider a greatest common divisor d of integers a and b. Now consider some other greatest common divisor c of a and b. By Property (2) of Definition 2.6, $c|d$ and $d|c$ hold. By Lemma 2.5, we thus know either $c = d$ or $c = -d$. □

Consider any two integers a and b. We denote the nonnegative greatest common divisor of a and b, if it exists, by $\gcd(a, b)$. Moreover, we call this unique number, *the* greatest common divisor of a and b. Proposition 2.9 will justify this notation, by showing that $\gcd(a, b)$ always exists.

Theorem 2.8. *Let a and b be integers, and d a nonnegative integer. Consider the sets $A = \{ax + by : x, y \in \mathbb{Z}\}$, and $B = \{dz : z \in \mathbb{Z}\}$. Then $d = \gcd(a, b)$ if and only if $A = B$.*

Proof. This proof is divided into two parts.
Proof that $A = B$ implies d is the $\gcd(a, b)$:

Assuming $A = B$, we need to show that d satisfies both conditions of Definition 2.6. Note that $a = a(1)+b(0)$ and $b = a(0)+b(1)$ are in A. Since $A = B$, there exist integers q' and q'' such that $a = q'd$ and $b = q''d$ are the case. But this statement just means that $d|a$ and $d|b$ hold, since q' and q'' are integers. Condition (1) of Definition 2.6 is thus satisfied for d.

Now consider any common divisor c of a and b. That is, there exist integers r' and r'' such that $a = cr'$ and $b = cr''$ are the case. These equations imply $ax = c(r'x)$ for any integer x, and $by = c(r''y)$ for any integer y. These statements mean that $c|ax$ and $c|by$ hold, since $r'x$ and $r''y$ are integers. By Lemma 2.4, we

know that $c|(ax+by)$, for any integers x and y. Since $A = B$, $d = ax' + by'$, for some integers x' and y'. Hence, we know $c|(ax'+by')$, which implies $c|d$. Because c is any common divisor of a and b, Condition (2) of Definition 2.6 is satisfied for d. And since d is nonnegative, we know it is the greatest common divisor of a and b.
Proof that d is the $\gcd(a,b)$ *implies* $A = B$:

Assuming d is the $\gcd(a,b)$, we need to show that $A = B$. By Theorem 2.2, we know there exists a nonnegative integer e, such that $\{ax+by : x,y \in \mathbb{Z}\}$ equals $\{ez : z \in \mathbb{Z}\}$. And by the first part of this proof, we know that e is the greatest common divisor of a and b. So, $e = \gcd(a,b) = d$; whence it follows that $\{dz : z \in \mathbb{Z}\} = \{ez : z \in \mathbb{Z}\} = \{ax+by : x,y \in \mathbb{Z}\}$. In other words, $A = B$. □

Proposition 2.9. *For any two integers a and b, the* $\gcd(a,b)$ *exists.*

Proof. By Theorem 2.2, for any two integers a and b, we can find a nonnegative integer d, such that $\{ax+by : x,y \in \mathbb{Z}\} = \{dz : z \in \mathbb{Z}\}$. Moreover, by Theorem 2.8, this d is the greatest common divisor of a and b. Therefore, for any two integers a and b, the $\gcd(a,b)$ exists. □

Proposition 2.10. *For any integer a, and for any positive integer b,* $\gcd(a,b) > 0$.

Proof. Firstly, we know that $\gcd(a,b)$ exists, by Proposition 2.9. Since the $\gcd(a,b)$ is nonnegative, we merely have to show that it is positive, and not equal to zero. Assume $\gcd(a,b) = 0$. Then by Definition 2.6, $0|b$ - i.e. there exists an integer x', such that $x'(0) = b > 0$. But we also know $x'(0) = 0$. We have a logical contradiction here. It follows that the $\gcd(a,b)$ is positive. □

Definition 2.11. Two integers a and b are *relatively prime* if their only common divisors are $+1$ and -1.

Proposition 2.12. *Suppose integers a and b are relatively prime. Then there exist integers* x' *and* y'*, such that* $ax' + by' = 1$.

Proof. By the definition of being relatively prime, the greatest common divisor of a and b is the integer one. From Theorem 2.8, it follows that $\{ax+by : x,y \in \mathbb{Z}\} = \{(1)z : z \in \mathbb{Z}\} = \{z : z \in \mathbb{Z}\}$. Hence, for $z = 1$, there exist integers x' and y', such that $ax' + by' = 1$. □

3. Rings and Fields

In this section, we define and give examples of rings, commutative rings, and fields. The work in this section allows us to understand theorems in Section 3.

Definition 3.1. Let S be a set. A *binary operation* on S is a function $*$: $S \times S \to S$. We often write $a * b$ to denote $*(a,b)$.

Definition 3.2. A *ring* is a nonempty set F equipped with two binary operations, $+$ and $*$, such that the following conditions are satisfied:
(A1) For all x,y in F, $(x+y)+z = x+(y+z)$.
(A2) There exists an element 0 in F, such that for all x in F, $x+0 = 0+x = x$.
(A3) For all x in F, there exists an element $-x$ in F such that $x+(-x) = (-x)+x = 0$.
(A4) For all x,y in F, $x+y = y+x$.
(M1) For all x,y,z in F, $(x*y)*z = x*(y*z)$.
(M2) There exists an element 1 in F, such that for all x in F, $x*1 = x$.

(LD) For all x, y, z in F, $x * (y + z) = x * y + x * z$.
(RD) For all x, y, z in F, $(x + y) * z = x * z + y * z$.

Definition 3.3. A ring F is a *commutative ring* if it additionally satisfies this axiom:
(M3) For all x, y in F, $x * y = y * x$.

An example of a commutative ring is the set of integers.

Definition 3.4. A commutative ring F is a *field* if it additionally satisfies this axiom:
(M4) For all x in $F \setminus \{0\}$, there exists an element x^{-1} in F such that $x * (x^{-1}) = 1$.

Examples of fields include the real and complex numbers.

4. Modular Arithmetic

In this section, we define congruency modulo m, a congruence class modulo m, and the set of congruence class modulo m. We also define operations on congruence classes. These definitions, together with the concepts from Sections 1 and 2, are examined to develop the system of modular arithmetic, and to show which sets of congruence classes are rings, and which fields.

Definition 4.1. For integers a, b, and m, with $m \neq 0$, we say *a is congruent to b modulo m*, written $a \equiv b(m)$, if $m|(b - a)$.

Theorem 4.2. *We have $a \equiv b(m)$ if and only if $b \equiv a(m)$.*

Proof. If $a \equiv b(m)$, $m|(b - a)$ - i.e. there exists an integer k such that $mk = b - a$. This definition implies $m(-k) = a - b$, and so $m|(a - b)$.

Reversing a and b, we can apply this reasoning, to prove $b \equiv a(m)$ implies $a \equiv b(m)$. □

Definition 4.3. A *congruence class modulo m* for some integer a, written $\bar{a}$, is the set $\{n \in \mathbb{Z} : n \equiv a(m)\}$.

Proposition 4.4. *We have $n \in \bar{a}$ if and only if $n = a + km$, for some integer k.*

Proof. If $n = a + km$, for some integer k, then $km = n - a$, and so $m|(n - a)$. Thus, $a \equiv n(m)$. This fact implies $n \equiv a(m)$ by Theorem 4.2. Hence, $n \in \bar{a}$.

If $n \in \bar{a}$, $n \equiv a(m)$. This fact implies $a \equiv n(m)$ by Theorem 4.2. Hence, $m|(n - a)$ - i.e. there exists an integer k such that $km = n - a$, or $n = a + km$. □

Lemma 4.5. *If $a \equiv b(m)$ and $b \equiv c(m)$ hold, then $a \equiv c(m)$.*

Proof. By definition, $a \equiv b(m)$ means $m|(b - a)$. Again, $b \equiv c(m)$ means $m|(c - b)$. Since $(c - a) = (b - a) + (c - b)$, we know by Lemma 2.4 that $m|(c - a)$. Hence, $c \equiv a(m)$; and by Theorem 4.2, this congruence means $a \equiv c(m)$ is also the case. □

Theorem 4.6. *We have $a \equiv b(m)$ if and only if $\bar{a} = \bar{b}$.*

Proof. Firstly, since $a = a + m(0)$, a is in $\bar{a}$. If $\bar{a} = \bar{b}$, then a is in $\bar{b}$ as well. Hence, $a \equiv b(m)$.

If $a \equiv b(m)$, then a is in $\bar{b}$. Now, consider any integer c such that $c \equiv a(m)$. Since $a \equiv b(m)$ by assumption, we know by Lemma 4.5 that $c \equiv b(m)$ is also true. Therefore, every c in $\bar{a}$ is in $\bar{b}$, and $\bar{a} \subseteq \bar{b}$. Since $a \equiv b(m)$, we know $b \equiv a(m)$ by

Theorem 4.2. Applying the same reasoning from above, we have $\bar{b} \subseteq \bar{a}$. In sum, $\bar{a} = \bar{b}$. □

For any integer k, $km = (a + km) - a$. Since $m|km$, we have $m|[(a + km) - a]$, and so $a \equiv (a + km)\ (m)$. By Theorem 4.6, this congruence means $\bar{a} = \overline{a + km}$.

Theorem 4.7. *For any positive integer m, there are exactly m distinct congruence classes modulo m. In particular, these classes are exactly $\bar{0}$, $\bar{1}$, ..., $\overline{m-1}$.*

Proof. We will show $\bar{0}$, $\bar{1}$,...,$\overline{m-1}$ are distinct congruence classes modulo m, for $m > 0$. Let $0 \leq k < l < m$ hold. Assume $\bar{k} = \bar{l}$. Then by Theorem 4.6, $k \equiv l(m)$, which implies $m|(l-k)$. Since $l-k > 0$ and $m > 0$ hold, we have a positive integer x such that $mx = l-k$. Yet this statement contradicts the fact that $mx > m > l-k$, for any positive integer x. Therefore $\bar{k} \neq \bar{l}$ must be true.

Now let a be any integer. By Theorem 2.1, there exist integers q and r such that $a = qm + r$, with $0 \leq r < m$. Hence, $qm = a - r$. This equation implies we have $m|(a - r)$ - i.e. $r \equiv a(m)$. By Theorem 4.6, we know $\bar{r} = \bar{a}$. □

Definition 4.8. The *set of congruence classes modulo m* is denoted by $\mathbb{Z}/m\mathbb{Z}$.

Theorem 4.9. *The set $\mathbb{Z}/m\mathbb{Z}$, for any positive integer m, is a commutative ring under the addition operation $\bar{a}+\bar{b} = \overline{a+b}$, and the multiplication operation $\bar{a}\bar{b} = \overline{ab}$.*

Proof. We must do two things:
(1) ensure that these operations are well-defined for $\mathbb{Z}/m\mathbb{Z}$; and
(2) check that $\mathbb{Z}/m\mathbb{Z}$ satisfies the Commutative Ring Axioms.
By Theorem 4.7, $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$.

Well-Defined Check:
We must first show that these operations are well-defined. That is, no matter which congruence class equivalent to $\bar{a}$ (of the form $\overline{a + km}$) and to $\bar{b}$ (of the form $\overline{b + qm}$) we choose, $\overline{a + km} + \overline{b + qm} = \bar{a} + \bar{b}$. We have:
(Addition): $\overline{a + km} + \bar{b} = \overline{(a + km) + b} = \overline{(a + b) + km} = \overline{(a + b)} = \bar{a} + \bar{b}$.
(Multiplication): $\overline{a + km}\ \bar{b} = \overline{(a + km)b} = \overline{(a + b) + (bk)m} = \overline{ab} = \bar{a}\bar{b}$.
Considering congruence classes of the form $\overline{b + km}$, for any integer k, we can apply this reasoning to show that our choice of any congruence class equivalent to $\bar{b}$, does not matter.

Ring Axioms Check:

The satisfaction of these axioms looks very much like that for the integers. So, this part of the proof is left to the reader.

We now know that the operations are well-defined, and that all the Commutative Ring Axioms hold for $\mathbb{Z}/m\mathbb{Z}$. Therefore, $\mathbb{Z}/m\mathbb{Z}$ is a commutative ring. □

Lemma 4.10. *Consider any prime integer p. For any integer a such that $0 < a < p$, we have $\gcd(a, p) = 1$.*

Proof. Firstly, by Proposition 2.9, we know the number $\gcd(a, p)$ exists. The $\gcd(a, p)$ is a positive divisor of p. Since p is prime, this fact implies the $\gcd(a, p)$ is

1 or p. But the $\gcd(a, p)$ is also a positive divisor of a, and so it must be less than or equal to a. But $a < p$, so we have $\gcd(a, p) \leq a < p$. This inequality implies that $\gcd(a, p) = 1$. □

Theorem 4.11. *The set $\mathbb{Z}/p\mathbb{Z}$, for any prime integer p, is a field under the addition operation $\bar{a} + \bar{b} = \overline{a+b}$, and the multiplication operation $\bar{a}\bar{b} = \overline{ab}$.*

Proof. Using Definition 4.9, we know that $\mathbb{Z}/p\mathbb{Z}$ is a commutative ring. Now, we must show that $\mathbb{Z}/p\mathbb{Z}$ satisfies (M4).
(M4): Let X be a non-zero element of $\mathbb{Z}/p\mathbb{Z}$. As in the proof of Theorem 4.7, we have $X = \bar{a}$ for some integer a, such that $0 < a < p$. So, we know by Lemma 4.10 that $\gcd(a, p) = 1$. By Proposition 2.12, we can find integers r and s, such that $1 = ra + sp$. This equation implies $sp = 1 - ra$ - i.e. $p|(1 - ra)$, and so $ra \equiv 1(p)$ hold. Define $\bar{a}^{-1}$ to be r.
In sum, $(a^{-1})a \equiv 1(p)$. By Theorem 4.6, we know $\bar{a}^{-1}\bar{a} = \bar{1}$.

□

Acknowledgments. It is a pleasure to thank my mentors, Preston Wake and Yun Cheng, for providing my topic idea and corresponding research materials. Moreover, they guided my learning and writing processes in our mentor meetings and email correspondence. Their aid and amiable attitude were instrumental in the crafting of this paper.

References

[Conrad] Conrad, Keith. Modular Arithmetic. University of Connecticut. Web. ¡http://www.math.uconn.edu/ kconrad/blurbs/ugradnumthy/modarith.pdf¿.

[Berggren] Berggren, John L. "Modular Arithmetic." Encyclopaedia Britannica. N.d. Web. http://www.britannica.com/EBchecked/topic/920687/modular-arithmetic.

[Euclid] Euclid. "Euclid's Elements." Euclid's Elements. Ed. D. E. Joyce. Dept. Math. and Comp. Sci., Clark University, 1996-8. Web. ¡http://aleph0.clarku.edu/ djoyce/java/elements/elements.html¿. This citation refers to an online-published copy of Euclid's Elements.

[1] Ireland, Kenneth, and Michael Rosen. A Classical Introduction to Modern Number Theory. New York, NY: Springer, 1993. Print.

[2] Tobias Oekiter, Hubert Partl, Irene Hyna and Elisabeth Schlegl. The Not So Short Introduction to LaTeX 2_ε. http://tobi.oetiker.ch/lshort/lshort.pdf.