ELEMENTARY NUMBER THEORY AND THE CHINESE REMAINDER THEOREM

JOHN GALLAGHER

Abstract. This paper explores basic number theory including the groups, the rings and the units of modulo classes. It concludes with the Chinese Remainder Theorem. The goal is to examine these objects, their properties and to gain insight into their relationship with other sets.

Contents

Introduction

Number theory is the study of the basic properties of numbers. In particular it looks to explore how numbers relate to each other in terms of divisibility, primality, greatest common divisors, congruences and many other distinct properties. Section one deals with basic definitions of groups, rings, units, and ideals. Section two explores the integers. In particular it proves they are both a principal ideal domain, and a Euclidean domain. It then generalizes that all Euclidean domains are also principal ideal domains. Section three defines congruence in the integers and sets up the basic notion of $\mathbb{Z}/n\mathbb{Z}$. Section four introduces the notion of the order of $\mathbb{Z}/n\mathbb{Z}$ and includes Euler's Theorem and Fermat's Little Theorem. However, there is little exploration of either's implications. Finally in Section five, the paper culminates in the proof of the Chinese Remainder Theorem and displays one application: the units of $\mathbb{Z}/p\mathbb{Z}$ (where p is a prime number) are cyclic.

1. Preliminary definitions

Definition 1.1. Group: A group G is a set with a binary operation m such that:

(1) For any two elements a, b of this group, $m(a, b) \in G$;
(2) For any three elements a, b, c of the group $m(a, m(b, c)) = m(m(a, b), c)$;
(3) The group G possesses an identity element e such that for any element $a \in G$, $m(e, a) = a$ and $m(a, e) = a$;

(4) There exists an inverse for each element. In particular, for any a, there exists a^{-1} such that $m(a, a^{-1}) = e$ and $m(a^{-1}, a) = e$.

Definition 1.2. Ring: A ring is an abelian group under addition (+) with a binary operation called multiplication ($\cdot$) such that:

(1) The product of any two elements of the ring is also contained in the ring. $a, b \in R \implies ab \in R$;
(2) Multiplication on this ring is associative. That is $a, b, c \in R, (ab)c = a(bc)$;
(3) There exists an identity $1 \in R$ such that for any $a \in R$, $a1 = 1a = 1$.
(4) Multiplication in the ring is distributive over addition, that is, for $a, b, c \in R, a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

A ring R is called commutative if any two elements commute; that is, for all $a, b \in R, ab = ba$.

Definition 1.3. Unit: A unit is any element a of a ring R such that there exists an inverse a^{-1} where $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Definition 1.4. Ideal: An ideal I of a commutative ring R is an additive subgroup $S \subset R$ such that for all $r \in R$ and $s \in S$, we have $rs \in S$.

A **principal ideal** is an ideal that can be generated by a single element of R.

A **principal ideal domain** (PID) is a integral domain in which every ideal is principal.

2. Integers, Principal Ideal Domains, and Euclidean domains

Proposition 2.1. *The integers $\mathbb{Z}$ are a principal ideal domain.*

Proof. It suffices to show that all subgroups, and therefore all ideals of the integers, are of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Let H be an arbitrary subgroup, closed under addition and subtraction, and let $h \in H$ be the smallest positive element. It is also true that $h\mathbb{Z} \subset H$.

Let us then assume that our proposition is false so that $h\mathbb{Z} \neq H$.

Because $h\mathbb{Z} \neq H$ there exists a $g \in H \setminus h\mathbb{Z}$.

Let $n = \lfloor \frac{g}{h} \rfloor$ such that n is the greatest integer $\leq \frac{g}{h}$.

Because $h\mathbb{Z} \subset H, hn \in H$, $g - hn < h$ and $\in \{0, 1, \dots, h - 1\}$. This contradicts the minimality of h.

Therefore $h\mathbb{Z} = H$. □

Definition 2.2. Euclidean domain: A ring R that has no zero divisors and where $0 \neq 1$ is called and integral domain. An integral domain is considered to be a Euclidean domain if there is a function λ from the elements of $R \setminus \{0\}$ to the set $\{1, 2, 3, \dots\}$ such that for any $a, b \in R$, where $b \neq 0$, there exists a $c, d \in R$ such that $a = cb + d$ and either $d = 0$ or $\lambda(d) < \lambda(b)$.

Proposition 2.3. *The integers $\mathbb{Z}$ are a Euclidean domain.*

Proof. Let $a, b \in \mathbb{Z}$ where $b \neq 0$. Consider the set of all integers of the form $a - xb$ with $x \in \mathbb{Z}$. This set includes positive elements. Let $r = a - qb$ be the least nonnegative element in this set. We claim that $0 \leq r < b$. If not, $r = a - qb \geq b$ and so $0 \leq a - (q + 1)b < r$ which contradicts the minimality of r. (Implicitly $\lambda(x) = |x|$). □

Proposition 2.4. *All Euclidean domains are principal ideal domains.*

Proof. Let R be a Euclidean domain with the function λ. Take an ideal $I \subset R$.

Let a be an element of this ideal such that $\lambda(a)$ is minimal. Assume for the sake of contradiction, that I is not principal. That is, a does not generate the entire ideal. There then exists a $b \in I \setminus \{a\}$ and b does not equal zero.

Because b exists there also exists a q, r such that $b = qa + r$ where $\lambda(r) < \lambda(a)$. This leads to a contradiction because $r = b - qa \in I$ goes against the minimality of our selection, a. □

3. Congruence in $\mathbb{Z}$

Definition 3.1. If $a, b, m \in \mathbb{Z}$ and $m \neq 0$, then a is called congruent to b modulo m if m is a divisor of $b - a$. This statement is written as $a \equiv b \pmod{m}$.

Proposition 3.2. *Congruence in $\mathbb{Z}$ is an equivalence relation.*
a) $a \equiv a \pmod{m}$;
b) $a \equiv b \pmod{m}$ implies $b \equiv a \pmod{m}$; and
c) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

Proof. a) $a - a \equiv 0$ and $m|0$.
b) If $m|b - a$ then $m|a - b$.
c) If $m|b - a$ and $m|c - b$ then $m|c - a = (c - b) + (b - a)$. □

We can now take a look at the integers and in particular look at the equivalence classes. If $a \in \mathbb{Z}$ then let $\bar{a}$ denote the set of integers congruent to a modulo m, that is $\bar{a} = \{n \in \mathbb{Z} | n \equiv a \pmod{m}\}$. This is the same as saying $\bar{a}$ is the set of integers of the form $a + km$ $(k \in \mathbb{Z})$.

Definition 3.3. A set of the form $\bar{a}$ is called a congruence class modulo m.

Definition 3.4. The set of all congruence classes modulo m is denoted by $\mathbb{Z}/m\mathbb{Z}$. It can also be denoted as $\mathbb{Z}_m$.

The set of all congruence classes modulo m is a ring. It is an abelian group under addition and subtraction and is closed under multiplication.

4. The Units of $\mathbb{Z}/p\mathbb{Z}$

Definition 4.1. The units of a ring are denoted by $R^\times$.

Definition 4.2. The order of a group element a a is the smallest positive integer m such that $a^m = 1$. This is denoted by $\text{ord}(a) = m$.

Definition 4.3. (Euler's Phi Function) Euler's phi function denoted by $\phi(n)$ is the number of positive integers less than and relatively prime to n.

Proposition 4.4. *An element of $\mathbb{Z}/m\mathbb{Z}$, is a unit if and only if the greatest common divisor of a and m is 1.*

This is a direct result of the Euclidian algorithm. The algorithm backwards yields $\gcd(a, m) = xa + my$ for integers x, y. Thus x is a's inverse

Lemma 4.5. *For a group G and any $g \in G$ ord (g) divides $|G|$*

Proof. $G/\langle g \rangle$ consists of classes of size $\langle g \rangle = \text{ord}(g)$ each. So the number of equivalence classes is $|G|/\text{ord}(g)$. □

Corollary 4.6. *(Euler's Theorem) If gcd$(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Proof. The units in $\mathbb{Z}/m\mathbb{Z}$ form a group of order $\phi(m)$. If $\gcd(a, m) = 1$ then $\bar{a}$ is a unit. Therefore because of lemma 4.5 $\bar{a}^{\phi(m)} = \bar{1}$ which is the same as $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Corollary 4.7. *(Fermat's Little Theorem) If p is a prime and $p \not| a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. If p does not divide a then $\gcd(a, p) = 1$. Now $\phi(p)$ equals $p - 1$ because p is prime. Therefore $a^{\phi(p)} \equiv 1 \pmod{p}$. □

Lemma 4.8. *For a finite abelian group $(G, +)$ let $m = max\ ord(x)$ then for all $z \in G$, $ord(z)|m$.*

Proof. Take two elements $a, b \in G$. Let $\text{ord}(a) = k$ and $\text{ord}(b) = l$. $(ab)^n = a^n b^n$. Because $\text{ord}(a) = k$, it follows that $a^k = 1$. Thus $a^n = a^{n \text{ (mod } k)}$ and $b^n = b^{n \text{ (mod } l)}$. Let us write k as $k'd$ and $l = l'd$ where $d = \gcd(k, l)$. Therefore the least common multiple of $(k, l) = k'l'd$. Note b^d has and order of l.

It suffices to show that $\text{ord}(ab^d) = k'l'd$. Indeed $a^{k'l'd'} b^{k'l'd^2} = 1$. Moreover, if $(ab^d)^x = 1$ then $a^x = (b^d)^{-x} = y$.

However, $\text{ord}(z)|\text{ord}(a) = k'd$ and $\text{ord}(z)|\text{ord}(b^d) = l'$.

Furthermore, $\gcd(k'l'd) = 1$ so ord $(z) = 1$ and $z = 1$. Backtracking for a moment to $a^x = (b^d)^{-x} = z$, we can apply the previous statement so $a^x = 1$ and $(b^d)^x = 1$. It then follows that $k'd'|x$ and $l'|x$ so $k'l'd|x$.

Therefore if G has elements of ordk, l then it has one of order lcm (k, l).

To finish the lemma, let $z \in G$ have ord$k$ then there exist elements of order $\text{lcm}(k, m) = m$ which implies $k|m$. □

Proposition 4.9. *$\mathbb{Z}_p^\times$ is cyclic.*

Proof. Let $m = \max \text{ord}(a)$ where $a \in \mathbb{Z}_p^\times$.

By the lemma, for all $a \in \mathbb{Z}_p^\times$, $\text{ord}(a)|m$ implies that $a^m = a^{m \text{ (mod } ord(a))} = a^0 = 1$.

Therefore for all $a \in \mathbb{Z}_p^\times$, a because $|\mathbb{Z}_p^\times| = p - 1$is a root of $x^m - 1 \in \mathbb{Z}_p[x]$.

There are $p - 1$ units. All are roots of $x^m - 1$ and $x^m - 1$ has at most m roots. Therefore $m \geq p - 1$, so $m = p - 1$ Finally, there exists a $g \in \mathbb{Z}_p^\times$ of order $p - 1$. □

5. The Chinese Remainder Theorem

Lemma 5.1. *If $a_1, \ldots, a_l$ are all relatively prime to m, then so is $a_1 a_2 \ldots a_l$.*

Proof. Because $\bar{a}_i \in \mathbb{Z}/m\mathbb{Z}$ is a unit, $\bar{a}_1 \bar{a}_2 \ldots \bar{a}_t = \overline{a_1 a_2 \ldots a_t}$. Therefore by proposition 4.4, $a_1 a_2 \ldots a_t$ is relatively prime to m. □

Lemma 5.2. *Suppose that $a_1, a_2, \ldots, a_t$ all divide n and that $(a_i, a_j) = 1$ for $i \neq j$. Then $a_1 a_2 \ldots a_t$ divides n.*

Proof. The proof is by induction on t. If $t = 1$ then there is nothing to do. Suppose that $t > 1$ and that the lemma is true for $t - 1$. Then $a_1, a_2, \ldots, a_{t-1}$ divides n. Using Lemma 5.1 a_t is prime to $a_1, a_2, \ldots, a_{t-1}$. So there are integers r and s such that $ra_t + sa_1 a_2 \ldots a_{t-1} = 1$. Multiply both sides by n and it quickly follows that the left hand is divisible by $a_1 a_2 \ldots a_t$. □

Proposition 5.3. *(The Chinese Remainder Theorem)*

Suppose that $m = m_1 m_2 \dots m_t$ and that $gcd(m_i, m_j) = 1$ for any $i \neq j$. Let $b_1, b_2, \dots, b_t$ be integers and consider the system of congruences:

$$x \equiv b_1(m_1), x \equiv b_2(m_2), \dots, x \equiv b_t(m_t)$$

Then this system always has solutions and any two solutions differ by a multiple of m.

Proof. Let $n_i = m/m_i$. By lemma 5.1, m_i and n_i are relatively prime. Therefore there exists integers r_i and s_i such that $r_i m_i + s_i n_i = 1$. Let $e_i = s_i n_i$. $e_i \equiv 1(m_i)$ and $e_i \equiv 0(m_j)$ for $i \neq j$.

If $x_0 = \sum_i^t b_i e_i$ then we have $x_0 t \equiv b_i e_i(m_i)$ and consequently $x_0 = b_i(m_i)$. x_0 is a solution.

Suppose that there were another solution. Then $x_1 - x_0 \equiv 0(m_i)$ for $i = 1, 2, \dots, t$. In other words $m_1, m_2, \dots, m_t$ divide $x_1 - x_0$ by lemma 5.2. □

Acknowledgements. I would like to take this section to thank Laurence Field and Benjamin Fehrman. Without the hours of instruction and dedication from Laurie, I would not have been able to learn or present this material. Additionally without the help of Ben, these proofs would have been unreachable.

References

[1] Kenneth Ireland. Michael Rosen. A Classical Introduction to Modern Number Theory. Springer-Verlag 1982.