Abstract Algebra, 4th edition by Beachy and Blair
Abstract Algebra YouTube playlist by Socratica

1 Integers

1.1 Divisors

$a\mathbb{Z}$ denotes all the integer (±) multiples of a.

Every set of integers that is bounded below contains a least element. (Corollary of the Well-Ordering Principle of $\mathbb{N}$.)

The division algorithm states that for any integers a and b with $b > 0$, there exist unique integers q (the *quotient*) and r (the remainder) such that $a = bq + r$ with $0 \leq r < b$. (Where the remainder $r = 0$, we say $b|a$ meaning b *divides* a or b *is a divisor of* a.)

Let I be a nonempty set of integers closed under addition and subtraction. The $I = 0$ or I contains some smallest positive element, in which case I consists of all multiples of that smallest positive element.

Definition: greatest common divisor: let a and b both be integers where at least one of a and b is not zero. A positive integer d is called the greatest common divisor of a and b if 1. $d|a$ and $d|b$ (d divides both a and b), and 2. $c|a$ and $c|b$ implies $c|d$ (any divisor of a and b is also a divisor of d).

The greatest common divisor of a and b is written $gcd(a, b)$ or simply (a, b).

$\gcd(0, 0)$ is undefined, but $\gcd(a, 0) = |a|$.

Theorem: the gcd is unique. (Suppose there are two gcds, then apply part 2 of the definition).

Theorem: $\gcd(a, b) = ma + nb$ for $m, n \in \mathbb{Z}$. (The greatest common divisor of a and b can be written as a linear combination of a and b. Remember that m and n can be negative!)

Corollary: the set of all linear combinations of a and b is equal to $d\mathbb{Z}$.

$\gcd(a, b) = \gcd(|a|, |b|)$.

If $b > 0$ and $b|a$, then $\gcd(a, b) = b$.

$a = bq + r$ implies $\gcd(a, b) = \gcd(b, r)$ for $b \neq 0$.

The Euclidean Algorithm

$\gcd(a, b) = \gcd(b, r_1)$

if $r_{n+1} = 0$, then $r_n = \gcd(a, b)$.

1.2 Primes

Two numbers a and b are called *relatively prime* if $\gcd(a, b) = 1$.

Proposition. Let a, b be nonzero integers. Then $(a, b) = 1$ if and only if there exist integers m, n such that $ma + nb = 1$.

Proposition. Let a, b, c be integers where $a \neq 0$ or $b \neq 0$.

a) if $b|ac$, then $b|(a, c) \cdot c$

b) if $b|ac$, and $(a, b) = 1$, then $b|c$

c) if $b|a$, $c|a$ and $(b, c) = 1$ then $bc|a$

d) $(a, bc) = 1$ if and only if $(a, b) = 1$ and $(a, c) = 1$

Lemma (Euclid) An integer $p > 1$ is prime if and only if for all integers a and b, if $p|ab$, then either $p|a$ or $p|b$. (This is true only if p prime; consider the case $6|2 \cdot 3$)

1.3 Congruences

Definition. Let n be a positive integer. Integers a and b are said to be *congruent modulo* n **if they have the same remainder when divided by** n**,** denoted $a \equiv b(\text{mod } n)$. In other words, $a \equiv b(\text{mod } n) \Leftrightarrow a\%n = b\%n$

Let a, b, and $n \neq 0$ be integers. Then $a \equiv b(\text{mod } n)$ if and only if $n|(a-b)$. In other words, if both a and b have the same remainder mod n, then they must differ by a multiple of n.

Proposition Let $n > 0$ be an integer. Then the following conditions hold for integers a, b, c, d:

a) if $a \equiv c(\text{mod } n)$ and $b \equiv d(\text{mod } n)$, then $a \pm b \equiv b \pm d(\text{mod } n)$ and $ab \equiv cd(\text{mod } n)$

b) if $a + c \equiv a + d(\text{mod } n)$ then $c \equiv d(\text{mod } n)$. If $ac \equiv ad(\text{mod } n)$ and $(a, n) = 1$, then $c \equiv d(\text{mod } n)$.

Proof

If $a \equiv c(\text{mod } n)$ and $b \equiv d(\text{mod } n)$, then $n|(a-c)$ and $n|(b-d)$. Adding shows that $n|((a+b)-(c+d))$, and subtracting shows that $n|((a-b)-(c-d))$. So, $a \pm b \equiv c \pm d(\text{mod } n)$. □

Since $n|(a-c)$, we have $n|(ab-cb)$, and then since $n|(b-d)$, we must have $n|(cb-cd)$. Adding shows that $n|(ab-cd)$ and thus $ab \equiv cd(\text{mod } n)$. □

If $ac \equiv ad(\text{mod } n)$, then $n|(ac-ad)$, and since $(n, a) = 1$, it follows from the previous proposition (the four-part one) that $n|(c-d)$. Thus $c \equiv d(\text{mod } n)$. □

Consequences

1) For any number in the congruence, you can substitute any congruent integer.

2) You can add or subtract the same integer on both sides of a congruence.

3) You can multiply both sides of a congruence by the same integer.

4) You can divide both sides of a congruence by an integer a only if $(a, n) = 1$.

Let a and $n > 1$ be integers. There exists an integer b such that $ab \equiv 1(\text{mod } n)$ if and only if $(a, n) = 1$.

Theorem. Let a, b, and $n > 1$ be integers. The congruence $ax \equiv b(\text{mod } n)$ has a solution if and only if b is divisible by d, where $d = (a, n)$. If $d|b$, then there are d distinct solutions modulo n, and these solutions are congruent modulo n/d.

Algorithm

First compute $d = (a, n)$. If $d|b$, we write $ax \equiv b(\text{mod } n)$ as $ax = b + qn$. Since d is a common divisor of a, b, and n, we can write $a = da_1$, $b = db_1$, and $n = dm$. Thus we get $a_1x = b_1 + qm$, which yields the congruence $a_1x \equiv b_1(\text{mod } m)$, where $a_1 = a/d$, $b_1 = b/d$, and $m = n/d$. Since $d = (a, n)$, the numbers a_1 and m must be relatively prime. Thus... (p. 31)

Chinese Remainder Theorem Let n and m be positive integers, with $(n, m) = 1$. Then the system of congruences

$$x \equiv a(\text{mod } n)$$
$$x \equiv b(\text{mod } m)$$

has a solution. Moreover, any two solutions are congruent modulo mn.

If $ma + nb = c$, then $ma \equiv c(\text{mod } n)$ and $nb \equiv c(\text{mod } m)$.

1.4 Integers Modulo N

Definition. The congruence class of *a* modulo *n* (denoted $[a]_n$) is the set of all integers which have the same remainder as a when divided by n (for $a, n \in \mathbb{Z}$ and $n > 0$). $[a]_n = \{x \in \mathbb{Z} \mid x \equiv a(\text{mod } n)\}$.

Note: the product of two nonzero congruence classes can equal zero.

Definition. The set of integers modulo *n* (denoted $\mathbb{Z}_n$) is the collection of all congruence classes modulo n and is equal to $\{[0]_n, [1]_n, \ldots, [n-1]_n\}$. For example, where $n = 2$, the set $\mathbb{Z}_2$ consists of the sets $[0]_2$ (the even integers) and $[1]_2$ (the odd integers).

We can use this notation to express the following rules:

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$\times$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

More broadly, we can express addition and multiplication in $\mathbb{Z}_n$ as:

$$[a]_n + [b]_n = [a + b]_n$$
$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

For example $[8]_{12} = [20]_{12}$ and $[10]_{12} = [34]_{12}$, so $[8]_{12} + [10]_{12} = [18]_{12} = [20]_{12} + [34]_{12} = [54]_{12} = [6]_{12}$.

$\mathbb{Z}_n$ forms a commutative ring.

Definition If $[a]_n \in \mathbb{Z}_n$ and $[a]_n[b]_n = [0]_n$ for some nonzero congruence class $[b]_n$, then $[a]_n$ is called a *divisor of zero*.

If $[a]_n$ is not a divisor of zero, we can cancel $[a]_n$ in $[a]_n[b]_n = [a]_n[c]_n$ to see $[b]_n = [c]_n$

Definition If $[a]_n \in \mathbb{Z}_n$ and $[a]_n[b]_n = [1]_n$, then $[b]_n$ is the *multiplicative inverse* of $[a]_n$. We also say that $[a]_n$ is an *invertible element* of $\mathbb{Z}_n$, or a *unit* of $\mathbb{Z}_n$.

If $[a]_n$ has a multiplicative inverse, it cannot be a divisor of zero because $[a]_n[b]_n = [0]_n$ implies $[b]_n = [a]_n^{-1}([a]_n[b]_n) = [a]_n^{-1}[0]_n = [0]_n$

$[a]_n$ can be written as $[a]$.

Proposition. Let n be a positive integer. Then a) the congruence $[a]_n$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if $gcd(a, n) = 1$. b) A nonzero element of $\mathbb{Z}$ either has a multiplicative inverse or is a divisor of zero.

Corollary The following conditions on the modulus $n > 0$ are equivalent,

1) n is prime.

2) $\mathbb{Z}_n$ has no divisors of zero except $[0]_n$.

3) Every nonzero element of $\mathbb{Z}_n$ has a multiplicative inverse.

Definition Let n be a positive integer. The number of positive integers less than and relatively prime to n will be denoted by *Euler's totient function* $\varphi(n)$.

Proposition If the prime factorization of n is $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, where $\alpha_i > 0$ for $1 \leq i \leq k$, then

$$\varphi(n) = n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdots \Big(1 - \frac{1}{p_k}\Big)$$

Theorem (Euler) If $gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1(\text{mod } n)$

Corollary (Fermat) If p is a prime number, then for any integer a we have $a^p = a(\text{mod } p)$.

2 Functions

2.1 Functions

Definition The Cartesian product of two sets A and B is the set of ordered pairs $A \times B = \{(a, b) | a \in A \text{ and } b \in B\}$.

Definition Let S and T be sets. A **function** from S into T is a subset F of $S \times T$ such that for each element $x \in S$ there is exactly one element $y \in T$ such that $(x, y) \in F$. S is called the **domain** of the function, and T is called the codomain of the function. The subset $\{y \in T | (x, y) \in F \text{ for some } x \in S\}$ of the codomain is called the **image** of the function.

Definition Let $f : S \to T$ and $f : T \to U$ be functions. The *composite* $g \circ f$ of f and g is the function from S to U defined by the formula $(g \circ f)(x) = g(f(x))$ for all $x \in S$. The composite is defined only when the codomain of the first function is equal to the domain of the second function. Some authors allow the composite of two functions to be defined if the codomain of the first function is a subset of the domain of the second function.

Composition of functions is associative.

Definition Let $f : S \to T$ be a function. f is said to *map* S *map* onto T if for each element $y \in T$ there exists an element $x \in S$ with $f(x) = y$. If f maps S onto T, we say f is a *surjective (onto)* function.

If $f(x_1) = f(x_2) \to x_1 = x_2$ for all $x_1, x_2 \in S$ then f is said to be *injective* or *one-to-one*.

If f is both one-to-one and onto (both surjective and injective), then f is said to be a *one-to-one correspondence* or *bijection* from S to T.

Note: saying f maps S **into** T is different from saying f maps S **onto** T

Proposition Let $f : S \to T$ and $f : T \to U$ be functions.

a) If f and g are one-to-one, then $g \circ f$ is one-to-one.

b) If f and g are onto, then $g \circ f$ is onto.

Definition Let S, T be sets. The *identity* function $1_S : S \to S$ is defined by the formula $1_S(x) = x$ for all $x \in S$. If $f : S \to T$ is a function, then a function $g : T \to S$ is called an inverse for f if $g \circ f = 1_S$ and $f \circ g = 1_T$.

$f(1_S(x)) = 1_T(f(x)) = f(x)$.

Proposition Let $f : S \to T$ be a function. If f has an inverse, then f must be one-to-one and onto. Conversely, if f is one-to-one and onto, it has a unique inverse.

Proposition Let $f : S \to T$ be a function and assume that S and T are finite sets with the same number of elements. The f is a one-to-one correspondence if it is either one-to-one or onto.

2.2 Equivalence Relations

An equivalence relationship is an operation that satisfies the following:

Reflexivity: $\forall x,\, x = x$
Symmetry: $x = y \to y = x$
Transitivity: $x = y \land y = z \to x = z$

2.3 Permutations

3 Groups