INTRO TO ABSTRACT ALGEBRA

Jacob Shiohira, FALL 2017
MATH 310 | University of Nebraska-Lincoln

Chapter 1

Section 1.1: The Division Algorithm

WELL-ORDERING AXIOM Every nonempty subset of the set of non-negative integers contains a smallest element.

THEOREM 1.1 Let a, b be integers with $b > 0$. Then there exist unique integers q an r such that

$$a = bq + r \text{ and } 0 \leq r < b.$$

Notice that the restrictions on b and r. If these did not exist, we could find multiple $q, r \in \mathbb{Z}$ that would satisfy the Division Algorithm.

Section 1.2: Divisibility

DEFINITION: Let a and b be integers with $b \neq 0$. We say that b **divides** a (or that b is a divisor of a, or that b is a factor of a) if $a = bc$ for some integer c. In symbols, "b divides a" is written $b|a$ and "b does not divide a" is written $b \not| a$.

Remarks:

1. Every nonzero integer b divides 0 because $0 = 0b$. For every integer a, we have 1 divides a because $a = 1 \cdot a$.
2. If b divides a, then $a = bc$ for some c. Hence, $-a = b(-c)$, so that $b|(-a)$. An analogous argument shows that every divisor of $-a$ is also a divisor of a. Therefore,

   $$a \text{ and } -a \text{ have the same divisors.}$$

3. Suppose $a \neq 0$ and $b|a$. Then, $a = bc$, so that $|a| = |b||c|$. Consequently, $0 \leq |b| \leq |a|$. This last inequality is equivalent to $-|a| \leq b \leq |a|$. Therefore,
   (a) every divisor of the nonzero integer a is less than or equal to $|a|$;
   (b) a nonzero integer has only finitely many divisors.
4. If a and b are integers, then $\text{lcm}(a, b)\gcd(a, b) = |ab|$.

DEFINITION: Let a and b be integers, $ab \neq 0$. The **greatest common denominator** (gcd) of a and b is the largest integer d that divides both a and b. In other words, d is the gcd of a and b provided that

1. $d|a$ and $d|b$;

2. if $c|a$ and $c|b$, then $c \leq d$.

The greatest common divisor of a and b is usually denoted (a, b).

THEOREM 1.2 Let a and b be integers, $ab \neq 0$, and let d be their greatest common divisor. Then there exist (not necessarily unique) integers u and v such that $d = au + bv$.
Remarks:

1. Every integer that can be written in the form $au + bv$ for some $u, v \in \mathbb{Z}$, is a multiple of the $\gcd(a, b)$.

2. Every common divisor of a and b also divides $\gcd(a, b)$.

COROLLARY 1.3 Let a and b be integers, both not 0, and let d be a positive integer. Then d is the greatest common divisor of a and b if and only if d satisfies these conditions:

1. $d|a$ and $d|b$;

2. if $c|d$ and $c|b$, then $c|d$.

Note that the 'if and only if' part of the statement requires two steps.

THEOREM 1.4 If $a|bc$ and $(a, b) = 1$, then $a|c$.

Section 1.3: Primes and Unique Factorization

Every nonzero integer n has except ± 1 has at least four distinct divisors, namely, $1, -1, n, -n$. Integers that have *only* these divisors play a crucial role.

DEFINITION: An integer p is said to be **prime** if $p \neq 0, \pm 1$ and the only divisors of p are ± 1 and $\pm p$.

Remarks:

(a) p is prime if and only if $-p$ is prime.

(b) If p and q are prime and $p|q$, then $p = \pm q$.

(c) If $p = rt$, then either $r = \pm 1$ or $t = \pm 1$.

(d) Integers a and b are *relatively prime* if $\gcd(a, b) = 1$.

THEOREM 1.5 Let p be an integer with $p \neq 0, \pm 1$. Then p is prime if and only if p has this property:

$$\text{whenever } p|bc, \text{ then } p|b \text{ or } p|c.$$

Remarks:

(a) This theorem is especially useful when proving that if $p|b^2$ for any prime p and some integer b, then $p|b$ or $p|b$

COROLLARY 1.6 If p is prime and $p|a_1a_2\cdots a_n$, then p divides at least on eof the a_i.

THEOREM 1.7 Every integer n except $0, \pm 1$ is a product of primes.

THEOREM 1.8 Every integer n except $0, \pm 1$ is a product of primes. This prime factorization is unique in the following sense: If

$$n = p_1p_1\cdots p_r \text{ and } n = q_1q_1\cdots q_s$$

with each p_i, q_j prime, then $r = s$ (that is, the number of factors is the same) and after reordering and relabeling the $q's$,

$$p_1 = \pm q_1, \ , p_2 = \pm q_2, \ , p_3 = \pm q_3, \ , ..., p_r = \pm q_r.$$

COROLLARY 1.9 Every integer $n > 1$ can be written in one and only one way in the form $n = p_1p_2p_3\cdots p_r$ where p_i are positive primes such that $p_1 \leq p_2 \leq p_3 \leq \cdots p_r$.

THEOREM 1.10 Let $n > 1$. If n has no positive prime factor less than or equal to $\sqrt{n}$, then n is prime.

Helpful Proofs

Euclidean Algorithm Find $(4631, 42371)$.

By the Euclidean Algorithm, we have

$$\begin{aligned}
42371 &= 9 \cdot 4361 + 3122 \\
4361 &= 1 \cdot 3122 + 1239 \\
3122 &= 2 \cdot 1239 + 644 \\
1239 &= 1 \cdot 644 + 595 \\
644 &= 1 \cdot 595 + 49 \\
595 &= 12 \cdot 49 + 7 \\
49 &= 7 \cdot 7 + 0
\end{aligned}$$

therefore $(4361, 42371) = 7$.

Famous Induction Proof If n is a positive integer, then

$$1 + 2 + \cdots + n = \tfrac{n(n+1)}{2}.$$

To verify that a proposition $P(n)$ holds for all natural numbers n, the **Principle of Mathematical Induction** consists of successfully carrying out the following two steps:

- **Base Case**: Prove that $P(0)$ is true.
- **Induction Step**: Assume that $P(n)$ is true for any arbitrary n, then prove that $P(n+1)$ is true.

We will proceed by induction that, for all $n \in \mathbb{Z}_+$,

$$\sum_{n=1}^{n} i = \frac{n(n+1)}{2}.$$

Base Case When $n = 1$, the LHS is the sum of the first 1 integer, which is simply 1. The RHS is $1(1+1)/2 = 1$. Both sides are equal, and the inductive hypothesis holds for the base case.

Inductive Case Let m and k be integers such that $m \geq 1$ and $1 \leq k \leq m$. Suppose that $P(k)$ holds. We then want to prove that $P(k+1)$ holds

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \frac{(k+1)(k+2)}{2} \\ &= [1 + 2 + \cdots + k] + (k+1)\end{aligned}$$

Well, by the summation,

$$\begin{aligned}\sum_{i=1}^{k+1} i &= 1 + 2 + \cdots + k + (k+1) \\ &= [1 + 2 + \cdots + k] + (k+1)\end{aligned}$$

By the induction hypothesis,

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + (k+1) \\
&= \frac{k(k+1)}{2} + (k+1) \\
&= \frac{k^2+k)}{2} + \frac{2(k+1)}{2} \\
&= \frac{k^2+k)}{2} + \frac{2k+2)}{2} \\
&= \frac{k^2+3k+2)}{2} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

Thus, $P(k+1)$ holds, and the proof of the induction step is complete. We may now conclude that, by the principle of mathematical induction, $P(n)$ holds true for all $n \in \mathbb{Z}_+$.

Infinitude of Primes Suppose that there are actually a finite number of primes such that $p_1 < p_2 < ... < p_r$. Then, let $N = p_1 p_2 \cdots p_r$. By the Fundamental Theorem of Arithmetic, $N+1$ also has a unique prime factorization. $N-1$ is either prime or composite. If $N-1$ is prime, then we have found another prime and contradict our original assumption. If $N-1$ is composite, it is a product of primes such that it has a prime p_i in common with N. So, p_i divides $N-(N-1) = 1$, which is a contradiction. There is no prime q such that $q|1$ because that would imply that $q \leq 1$, but by definition, $q > 1$. Thus, there are an infinite number of primes. $\square$

Chapter 2

Section 2.1: Congruence and Congruence Classes

Definition Let a, b, n be integers with $n > 0$. Then a is congruent b modulo n, written "$a \equiv b(\text{mod} n)$", provided n divides $a - b$.

Theorem 2.1 Let n be a positive integer. for all $a, b, c \in \mathbb{Z}$,

1. $a \equiv a(\text{mod} n)$;
2. If $a \equiv b(\text{mod} n)$, then $b \equiv a(\text{mod} n)$;
3. If $a \equiv b(\text{mod} n)$ and $b \equiv c(\text{mod} n)$, then $a \equiv c(\text{mod} n)$.

Theorem 2.2 If $a \equiv b(\text{mod} n)$ and $b \equiv c(\text{mod} n)$,

1. $a + c \equiv b + d(\text{mod} n)$

2. $ac \equiv bd(\text{mod}n)$

Definition Let a an n be integers $n > 0$. The congruence class of a modulo n (denoted by $[a]$) is the set of all those integers that are congruent to a modulo n, that is,

$$[a] = \{b | b \in \mathbb{Z} \text{ and } b \equiv a(\text{mod}n)\}.$$

Theorem 2.3 $a \equiv c(\text{mod}n)$ if and only if $[a]$=$[c]$.

Corollary 2.4 Two congruence classes modulo n are either disjoint or identical.

Corollary 2.5 Let $n > 1$ be an integer and consider congruence modulo n.

1. If a is any integer and r is the remainder when a is divided by n, then $[a]$=$[r]$.

2. There are exactly n distinct congruence classes, namely, $[0]$, $[1]$, $[2]$, $\cdots$, $[n-1]$.

Definition The set of all congruence classes modulo n is denoted $\mathbb{Z}_n$ (which is read "$\mathbb{Z}$ mod n).

Theorem 2.6 If $[a]$=$[b]$ and $[c]$=$[d]$ in $\mathbb{Z}_n$, then

$$[a + c] = [b + d] \text{ and } [ac] = [bd].$$

Definition Addition and multiplication in $\mathbb{Z}_n$ are defined by

$$[a] \oplus [r] = [a + c] \text{ and } [a] \odot [c] = [ac].$$

Theorem 2.7 For any classes $[a]$, $[b]$, $[c]$ in $\mathbb{Z}_n$,

1. If $[a] \in \mathbb{Z}_n$ and $[b] \in Z_n$, then $[a] \oplus [b] \in \mathbb{Z}_n$.

a $\oplus([b] \oplus [c]) = ([b] \oplus [a]) \oplus [c]$.

a $\oplus([0] = [0] \oplus [a]$.

a $\oplus([0] = [a] = [0] \oplus [a]$.

2. For each [a] in $\mathbb{Z}_n$, the equation $[a] \oplus X = [0]$ has a solution in $\mathbb{Z}_n$.

3. If $[a] \in \mathbb{Z}_n$ and $[b] \in \mathbb{Z}_n$, then $[a] \odot [b] \in \mathbb{Z}_n$.

$a \odot([b]\odot[c])=([a]\odot[b])\odot[c]$.

$a \odot[b]=[b]\odot[a]$.

$a \odot[1]=[a]=[1]\odot[a]$.

Theorem 2.8 If $p > 1$ is an integer, then the following conditions are equivalent:

1. p is prime
2. For any $a \neq 0 \in \mathbb{Z}_p$, the equation $ax = 1$ has a solution in $\mathbb{Z}_p$.
3. Whenever $bc = 0$ in $\mathbb{Z}_p$, then $b = 0$ or $c = 0$.

Theorem 2.9 Let a an n be integers with $n > 1$. Then

$$\text{The equation } [a]x = [1] \text{ has a solution in } \mathbb{Z}_n \text{ if and only if } (a, n) = 1 \text{ in } \mathbb{Z}.$$

Theorem 2.10 Let a and n be integers with $n > 1$. Then

$$[a] \text{ is a unit with } \mathbb{Z}_n \text{ if and only if } (a, n) = 1 \text{ in } \mathbb{Z}.$$