Math 347: Fundamental Mathematics

Lanxiao Hermite Bai

January 23, 2017

Contents

1 Numbers, sets and functions **3**
- 1.1 Elementary Inequalities . . . 3
- 1.2 Sets . . . 3
- 1.3 Functions . . . 4

2 Logic and Proofs **5**
- 2.1 Quantifiers and Logical Statements . . . 5
- 2.2 Methods of proof . . . 6

3 Induction **6**
- 3.1 Principle of Induction . . . 6

4 Bijection and Cardinality **7**
- 4.1 Representing integers . . . 7
- 4.2 Bijection . . . 9
- 4.3 Cardinality . . . 9

5 The Real Numbers **10**
- 5.1 Completeness Axiom . . . 10
- 5.2 Limits and Continuity . . . 11
- 5.3 K-ary expansion and discountability . . . 12

6 Series and Sequences **12**
- 6.1 Limits . . . 12
- 6.2 Cauchy Sequence . . . 13
- 6.3 Infinite Series . . . 13

7 Number Theory **15**
- 7.1 Divisibility in the Integers . . . 15
- 7.2 Modular Arithmetic . . . 19

1 Numbers, sets and functions

1.1 Elementary Inequalities

Proposition 1.1.1 *If* $0 < a < b$*, then* $a^2 < ab < b^2$ *and* $0 < \sqrt{a} < \sqrt{b}$

Definition 1.1.1 (Absolute Value)

$$|x| = \begin{cases} x & if\ x \geq 0 \\ -x & if\ x \leq 0 \end{cases}$$

Proposition 1.1.2 (Triangle Inequality) *If* $x, y \in \mathbb{R}$, $|x+y| \leq |x| + |y|$

Proposition 1.1.3 (AGM Inequality) *If* $x, y \in \mathbb{R}$, $2xy \leq x^2 + y^2$ *and* $xy \leq (\frac{x+y}{2})^2$.

Proof: Since $(x-y)^2 \geq 0$, $x^2 - 2xy + y^2 \geq 0$, when we add $2xy$ to both sides, we have $2xy \leq x^2 + y^2$, when we add $4xy$ on both sides and calculate the square root, we have $xy \leq (\frac{x+y}{2})^2$.

Corollary 1.1.1 *If* $x, y > 0$, $\frac{2xy}{x+y} \leq \sqrt{xy} \leq \frac{x+y}{2}$*, equality holds only when* $x = y$.[1]

1.2 Sets

Definition 1.2.1 (Set) *The objects in a* ***set*** *are its* ***elements*** *or* ***members****. When* x *is an element of* A*, we write* $x \in A$*, if not, we write* $x \notin A$*. If* $\forall x \in A, x \in B$*, then* A *is a* ***subset*** *of* B*, and* B ***contains*** A*, we write* $A \subseteq B$ *or* $B \supseteq A$.[2]

Definition 1.2.2 *Sets* $A = B$ *if they have the same elements. The* ***empty set*** $\emptyset$*, is the unique set with no elements. A* ***proper subset*** *of a set* A *is a subset of* A *that is not* A*. The* ***power set*** *of a set* A *is the set of all its subsets.*

Definition 1.2.3 *When* $a, b \in \mathbb{Z}$ *and* $a \leq b$*, we use* $a, ..., b$ *to* $i \in Z | a \leq i \leq b$*. When* $n \in N$*, we write* $[n]$ *for* $1...n$*. The set of even numbers is* $\{2k | k \in \mathbb{Z}\}$ *and the set of odd numbers is* $\{2k+1 | k \in Z\}$.

[1] Arithmetic Mean: $\frac{x+y}{2}$, Geometric Mean: $\sqrt{xy}$, Harmonic Mean: $\frac{2xy}{x+y}$

[2] Important sets: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, in this class $0 \notin \mathbb{N}$.

Definition 1.2.4 (Intervals) *When $a, b \in \mathbb{R}$ with $a \leq b$, the **closed interval** $[a, b]$ is $\{x \in \mathbb{R} | a \leq x \leq b\}$ and the **open interval** (a, b) is $\{x \in \mathbb{R} | a < x < b\}$.*

Definition 1.2.5 *A **list** with entries in A consists of elements of A in a specific order, with repetition allowed. A **k-tuple** is a list with k entries. We write A^k for the set of k-tuples with entries in A.*

*An **ordered pair** is a list with two entries. The **Cartesian product** of sets S and T, $S \times T = \{(x, y) | x \in S, y \in T\}$*

Definition 1.2.6 (Set Operations) *Let A and B be sets,*

- *Union $A \cup B = \{x | x \in A \text{ or } x \in B\}$*
- *Intersection $A \cap B = \{x | x \in A \text{ and } x \in B\}$*
- *Difference $A - B = \{x | x \in A \text{ and } x \notin B\}$*
- *Complement $A^c = U - A$*

*If $A \cup B = \emptyset$, they are **disjoint**.*

1.3 Functions

Definition 1.3.1 (Function) *A **function** f from a set A to a set B assigns to each $a \in A$ a single element $f(a) \in B$, called the **image** of a under f. For a function $f : A \to B$, A is the **domain**, B is the **target**. The **image** of f is $\{f(a), a \in A\}$.*[3]

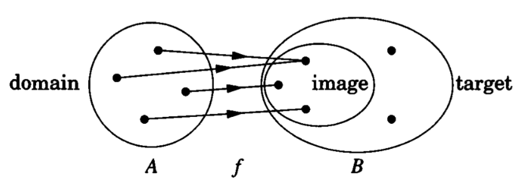

Figure 1: Mapping

[3] A function is called **well-defined** means that rules assign to each element of A exactly one element, belongling to B.

Definition 1.3.2 *For 2 functions f and g, $f = g$ when they have same domain, same targer and $\forall x \in$ domain, $f(x) = g(x)$.*

Definition 1.3.3 *A function is **real-valued** if its image is a subset of $\mathbb{R}$. If f and g are real-valued functions on A, $f + g$ and fg will be real-valued functions on A defined by $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$.*

Definition 1.3.4 (Polynomial) *A real **polynomial** in one variable is a function $f : \mathbb{R} \to \mathbb{R}$ defined by*

$$f(x) = \sum_{i=0}^{k} c_i x^i$$

*where k is a nonnegative integer and $c_0, ..., c_k$ are real numbers called the coefficients of f. The **degree** of f is the largest d such that $c_d \neq 0$.*

Definition 1.3.5 *A set $S \subseteq \mathbb{R}$ is **bounded** if $\exists M \in \mathbb{R}, \forall x \in S, |x| \leq M$, or the set is **unbounded**.*

Definition 1.3.6 *A function is **increasing** in a certain interval if $\forall x_2 > x_1, f(x_2) > f(x_1)$, **decreasing** if $f(x_2) < f(x_1)$.*

2 Logic and Proofs

2.1 Quantifiers and Logical Statements

Definition 2.1.1 (Mathematical Statement) *A **mathematical statement** is a statement that can be evaluated to be true or false.*

Definition 2.1.2 (Quantifier) *Suppose $P(x)$ is a statement involving the variable x which can take values in a set S, then:*

- ***Universally quantified:*** *For all $x \in S, P(x)$ is true, denoted as $\forall x \in S$, such that $P(x)$ is true.*
- ***Existentially quantified:*** *There exists an $x \in S$ such that $P(x)$ is true, denoted as $\exists x \in S, P(x)$ is true.*

Definition 2.1.3 (Logical Connectives) *Suppose P and Q are mathematical statements,*

- *Negation(not P):* $\neg P$
- *Conjunction(P and Q):* $P \wedge Q$
- *Disjunction(P or Q):* $P \vee Q$
- *Bicondition(P if & only if Q):* $P \Leftrightarrow Q$
- *Condition(P implies Q)*[4]*:* $P \Rightarrow Q$

Rule of negation:

- $\neg[(\forall x)P(x)] \Leftrightarrow (\exists x)(\neg P(x))$
- $\neg[(\exists x)P(x)] \Leftrightarrow (\forall x)(\neg P(x))$

2.2 Methods of proof

Direct method of proof: Assume P and argue via logical decuction that Q is also true ($P \Rightarrow Q$).

Contrapositive Assume $\neg Q$ follow deductions and conclude $\neg P$ is true ($\neg Q \Rightarrow \neg P$).

Methods of Contradiction Assume p and $\neg Q$, follow deductions and obtain a contradiction.

3 Induction

3.1 Principle of Induction

Definition 3.1.1 *The set* $\mathbb{N}$ *of natrual numbers is the intersection of all sets* $S \subseteq \mathbb{R}$ *that have the following properties:*

1. $1 \in S$
2. *If* $x \in S$*, then* $x + 1 \in S$

[4] P - **Hypothesis**, Q - **Conclusion**, $Q \Rightarrow P$ - **Converse** It is always true if the hypothesis is false.

Theorem 3.1.1 (Principle of Induction) *$\forall n \in \mathbb{N}$, let $P(n)$ be a mathematical statement. If*

- *$P(1)$ is true*
- *$\forall k \in \mathbb{N}, P(k) \Rightarrow P(k+1)$*

Then $\forall n \in \mathbb{N}, P(n)$.

Theorem 3.1.2 (Strong Induction) *$\forall n \in \mathbb{N}$, let $P(n)$ be a mathematical statement. If*

- *P(1) is true*
- *$\forall k \geq 2$ and $i < k$, $P(i) \Rightarrow P(k)$*

Then $\forall n \in \mathbb{N}, P(n)$.

4 Bijection and Cardinality

4.1 Representing integers

Usual way Decimal representation:
E.x.

$$1735 = 10^3 + 7 \cdot 10^2 + 3 \cdot 10 + 5$$

Definition 4.1.1 *Let $q \geq 2$ be a natural number. A **q-ary expansion** or **base-q expansion** of n is a list $a_m, \cdots, a_0$ of integers that $a_i \in \{0, 1, 2, \cdots, q-1\}$ such that*

$$n = \sum_{j=0}^{m} a_j q^j$$

We write $(a_m, \cdots, a_0)_q$ for base-q expansion.[5]

Theorem 4.1.1 *$\forall q \in \mathbb{N} \forall n \in \mathbb{N}$, n has a unique q-ary expansion.*

[5] When $q = 2$, binary, $n = 3$, ternary.

Proof: The base case, $n = 1$ is true since 1 is represented by $a_0 = 1$.

Suppose, $n = k$ is true, then when $n = k+1$. If $a_0 = a_1 = ... = a_m = q-1$,

$$\begin{aligned} k+1 &= \sum_{j=0}^{m}(q-1)q^j + 1 \\ &= (q-1)\sum_{j=0}^{m} q^j + 1 \\ &= (q-1)\frac{q^{m+!}-1}{q-1} + 1 \\ &= q^{m+1} - 1 + 1 = q^{m+1} \end{aligned}$$

So $k+1$ is represented by $a_{m+1} = 1$, $a_i = 0$ for $i \leq m$ If a_i is the first a that $a \neq q-1$, then

$$k+1 = \sum_{j=0}^{i-1} a_j q^j + a_i q^i + \sum_{j=i+1}^{m} a_j q^j = \sum_{j=0}^{i-1} a_j q^j + (a_j+1)q^i$$

So we can conclude that $\forall q \in \mathbb{N}, \forall n \in \mathbb{N}$, n has a q-ary expansion.

Suppose an integer n has 2 distinct q-ary expansions

$$\begin{aligned} n &= \sum_{j=0}^{r} a_j q^j \\ &= \sum_{j=0}^{s} b_j q^j \end{aligned}$$

According to the definition of polynomial, we have $a_j = b_j$ for all $j \leq m$ which is controversial to the hypothesis. Thus such expansion is unique.

If $r = s = m$, Then

$$\sum_{j=0}^{m} a_j q^j - \sum_{j=0}^{m} b_j q^j == \sum_{j=0}^{m}(a_j - b_j)q^j = 0$$

If $r \neq s$, without losing generality, we can suppose that $r > s$, then

$$\sum_{j=0}^{r} a_j q^j - \sum_{j=0}^{s} b_j q^j = \sum_{j=0}^{s}(a_j - b_j)q^j + \sum_{j=s+1}^{r} b_j q^j = 0$$

According to the definition of polynomial, we have $s \leq a_j = b_j$ for all $j \leq s$ and $b_j = 0$ for all $s \leq j \leq r$, which is controversial to the hypothesis. Thus such expansion is unique.

So we can conclude that $\forall q \in \mathbb{N}, \forall n \in \mathbb{N}$, n has a unique q-ary expansion.

4.2 Bijection

Definition 4.2.1 *A function $f : A \to B$ is a **bijection** if $\forall b \in B, \exists$ exactly one $x \in A$ such that $f(x) = b$.*[6] [7]

Definition 4.2.2 *Power set of a set S is the set that is formed by all S's subsets.*

Definition 4.2.3 *If $f : a \to b$ is a bijection that $f(a) = b$. The inverse of f, $f^{-1} : B \to A$ is $f(b) = a$. The inverse of a bijection is a bijection.*

4.3 Cardinality

Definition 4.3.1 *The cardinality of a set A is the number of elements of the set. Denote as $|A|$.*

Definition 4.3.2 *A set A is finite if there is a bijection $f : A \to [n]$ for some $n \in \mathbb{N}$*

Proposition 4.3.1 *If two set A and B are disjoint, $|A| \cup |B| = |A + B|$.*

Corollary 4.3.1

$$|A \cup |B| = |A| + |B| - |A \cap B|$$

Definition 4.3.3 *If a set infinite if it is not finite. If there is a bijection $f : A \to \mathbb{N}$, then A is **countably infinite** or it is **uncountably infinite**.*

Definition 4.3.4 *$|A| = |B|$ if there is a bijection $f : A \to B$.*

[6] Alternative terminology: one-to-one correspondence

[7] f is a bijection if and only if f is both injective and surjective.

5 The Real Numbers

Assumption

- $\mathbb{Q} \subseteq \mathbb{R}$
- $\mathbb{R}$ is a **field**, which means it's legal to:
  - add / subtract
  - multiply
  - divide by nonzero real number
  - associativity
  - commutativity
  - distributivity
- $\mathbb{R}$ has an ordering
- $\mathbb{R}$ satisfies the completeness axiom

5.1 Completeness Axiom

Definition 5.1.1 *Let $S \subseteq \mathbb{R}$. A number $\alpha \in \mathbb{R}$ is an* ***least upper bound*** *or* ***supremum*** *of S if S has no upper bound less than α. $\beta \in \mathbb{R}$ is an* ***greatest lower bound*** *or* ***infimum*** *of S if S has no lower bound larger than β.*[8]

Axiom 5.1.1 (Completeness Axiom) *Every nonempty subset of $\mathbb{R}$ that has an upper bound has a least upper bound.*

Theorem 5.1.1 (Archimedean Property) *Given any positive real numbers a, b there exists $n \in \mathbb{N}$ such that $na > b$.*

Equivalently, $\mathbb{N} \subseteq \mathbb{R}$ is not upper bounded.

[8] Notation: $\text{Sup}(S)$ = supremum of S, $\inf(S)$ = infimum of S

5.2 Limits and Continuity

Definition 5.2.1 (Limit) *Let (a_n) be a sequence of real numbers, we say that (a_n) **converges** to $L \in \mathbb{R}$ provided that given an $\varepsilon > 0$, $\exists N \in \mathbb{N}$ such that*

$$|a_n - L| < \varepsilon$$

for every $n \geq N$.[9]

e.g.1

Proof: The sequence $a_n = \frac{1}{n}$ converges to 0.
Let $\varepsilon > 0$ be given. There is $N \in \mathbb{N}$ so that

$$\frac{1}{\varepsilon} < N$$

so $\varepsilon > \frac{1}{N}$. Then $\forall n \geq N$ we have

$$|a_N - 0| = |\frac{1}{n}| = \frac{1}{n} \leq \frac{1}{N} < \varepsilon$$

■

Definition 5.2.2 *If $(a_n), (b_n)$ are sequences. Assume that $a_n \to 0$. If*

$$|b_n - L| \leq |a_n|$$

Then

$$b_n \to L$$

Terminology: Say (a_n) is convergent if it converges to some $L \in \mathbb{R}$.

Proposition 5.2.1 *A convergent sequence has a unique limit.*

Proposition 5.2.2 *Let $S \subseteq \mathbb{R}$ be a subset, then $(S) = \alpha \Leftrightarrow \exists (a_n)$ with $a_n \in S$ and $a_n \to \alpha$.*

Definition 5.2.3 *A sequence is **monotone** if it is either nondecreasing($n \geq m \Rightarrow a_n \geq a_m$) or nonincreasing($n \leq m \Rightarrow a_n \leq a_m$)*

[9]Notation: (a_n) converges to L $\equiv \lim_{n\to\infty} a_n = L \equiv \lim a_n = L \equiv a_n \to L$.

Theorem 5.2.1 (Monotone Convergence Theorem) *If (a_n) is a bounded monotone sequence, then it converges. If (a_n) is bounded nondecreasing, then* $\lim_{x\to\infty} a_n = \mathrm{Sup}(a_n)$. *If (a_n) is bounded nonincreasing, then* $\lim_{x\to\infty} = \mathrm{Inf}(a_n)$

Lemma 5.2.1 *If $a_n \leq M \forall a \in \mathbb{N}$, then if $a_n \to L$ then $L \leq M$.*

Proposition 5.2.3 *If (a_n) is nonincreasing, (b_n) is nondecreasing and if*

$$a_n - b_n \to 0$$

then both a_n and b_n converge and have the same limit.

Lemma 5.2.2 *If $a_n \to L$, then $a_n^2 \to L^2$.*

Theorem 5.2.2 $\sqrt{x} \in \mathbb{R}$ *if $x \geq 0$.*

5.3 K-ary expansion and discountability

Definition 5.3.1 *The **canonical k-ary expansion** of α is the sequence (l_n) defined by l_n = largest multiple of $\frac{1}{k^n}$ such that $l_n \leq \alpha$.*

Theorem 5.3.1 *Let $k \in \mathbb{N}, k \geq 2$, then*

- $\forall \alpha \in [0, 1)$ *has a canonical k-ary expansion*
- *Every k-ary expansion represent a real number in $[0, 1)$.*

Theorem 5.3.2 (Cantor) $\mathbb{R}$ *is uncountable.*

Lemma 5.3.1 *If a set S contains an uncountable subset, then S is uncountable.*

6 Series and Sequences

6.1 Limits

Theorem 6.1.1 *Let $(S_n), (T_n)$ be sequences, $\lambda \in \mathbb{R}$, then*

- $$\lambda \lim S_n = \lim \lambda S_n$$

- $$\lim S_n \pm \lim T_n = \lim(S_n \pm T_n)$$
- $$\lim S_n \cdot \lim T_n = \lim(S_n \cdot T_n)$$
- $$\lim \frac{1}{S_n} = \frac{1}{\lim S_n}$$

Lemma 6.1.1 *If (a_n) is convergent, then it is bounded.*

Proposition 6.1.1 *Suppose (a_n) is a sequence such that $\frac{a_{n+1}}{a_n}$ converges to a number $0 \leq x < 1$. Then $\lim a_n = 0$.*

Theorem 6.1.2 (Squeeze Theorem) *Suppose $a_n \leq b_n \leq c_n$ for all n. Then if $\lim a_n = L, \lim c_n = L$, then $\lim b_n = L$.*

6.2 Cauchy Sequence

Definition 6.2.1 *A sequence is said to be Cauchy provided given any $\varepsilon > 0$ there is $N \in \mathbb{N}$ such that for all $n, m > N \in \mathbb{N}$*

$$|a_n - a_m| < \varepsilon$$

Proposition 6.2.1 *Any convergent sequence is a Cauchy sequence.*

Lemma 6.2.1 *Every Cauchy sequences is bounded.*

6.3 Infinite Series

Definition 6.3.1 *An* ***infinite series*** *is an infinite summation $\sum_{k=1}^{\infty} a_k$. The sequence is* ***partial sums*** *is $S_n = \sum_{k=1}^{n} a_k$. Say that $\sum_{k=1}^{\infty} a_k$ converges if $\lim_{n\to\infty} S_n$ exists.*

Theorem 6.3.1 *The geometric theories*

$$\sum_{k=0}^{\infty} x^k$$

converges to

$$\frac{1}{1-x}$$

if $|x| < 1$ and diverges otherwise.

Remark: If $(a_k) \to L \neq 0$, then $\sum_{k=1}^{\infty} a_k$ diverges.

Proposition 6.3.1 (Harmonic Series)

$$\sum_{k=1}^{\infty} 1/k$$

diverges.

Lemma 6.3.1 *If $\sum_{k=1}^{\infty} a_k$ converges, then $a_k \to 0$.*

Proposition 6.3.2 (Comparison Test) *Suppose that $c_n \geq 0$ for all n. If*

$$\sum_{n=1}^{\infty} c_n$$

converges and

$$|a_n| \leq c_n$$

for all n, then

$$\sum_{n=1}^{\infty} a_n$$

converges.

If

$$\sum_{n=1}^{\infty} c_n$$

diverges to ∞, then if $a_n \geq c_n$ for all n,

$$\sum_{n=1}^{\infty} a_n$$

diverges.

Corollary 6.3.1 *If $\sum |a_n|$ converges then $\sum a_n$ converges as well.*

Proposition 6.3.3 *The sequence $\sum \frac{1}{n^p}$ converges if $p > 1$ and diverges if $p \leq 1$.*

Theorem 6.3.2 (Ratio Test) *Let (a_n) be a sequence such that $|a_{k+1}/a_k|$ converges to a number p. If $p < 1$, then $\sum a_k$ converges, if $p > 1$, then $\sum a_k$ diverges.*

Theorem 6.3.3 *Consider a series*

$$\sum_{n=1}^{\infty}(-1)^{n+1}a_n$$

where $a_n \geq 0$ such that

1. $$\lim_{n\to\infty} a_n = 0$$

2. *(a_n) is nonincreasing*

then

$$\sum_{n=1}^{\infty}(-1)^{n+1}a_n$$

converges.

Lemma 6.3.2 *If (x_n) is a sequence, $\lim_{n\to\infty} x_{2n} = L = \lim_{n\to\infty} x_{2n+1}$, then $\lim_{n\to\infty} x_n = L$ as well.*

7 Number Theory

7.1 Divisibility in the Integers

Definition 7.1.1 (Integer) *We denote the set of **integers** $\{0, \pm 1, \pm 2, \ldots\}$ by $\mathbb{Z}$.*

Definition 7.1.2 (Natural Number) *We denote the set of natural numbers $\{1, 2, 3, \ldots\}$ by $\mathbb{N}$.*

Proposition 7.1.1 *: Addition and Multiplication*

1. *Addition on $\mathbb{Z}$ is commutative and associative.*

2. *0 is an identity element for addition; $\forall a \in \mathbb{Z}, 0 + a = a$.*

3. *Every element* a *of* $\mathbb{Z}$ *has an additive inverse* $-a$ *that* $a + (-a) = 0$.

4. *Multiplication on* $\mathbb{Z}$ *is commutative and associative.*

5. *1 is is an identity element for multiplication;* $\forall a \in \mathbb{Z}, 1a = a$.

6. *The distribute law holds;* $a(b + c) = ab + ac$.

7. $\mathbb{N}$ *is closed under addition and multiplication.*

8. *The product of non-zero integers is non-zero.*

Definition 7.1.3 (Divisibility) *We say that an interger* a ***divides*** b, *(or that* b *is divisible by* a*), if there is an interger* q *such that* $aq = b$*; we write* $a|b$ *for "*a *divides* b*"*

Proposition 7.1.2 *Properties of Divisibility:*

Let a, b, c, u, *and* v *denote integers.*

1. *If* $uv = 1$, *then* $u = v = 1$ *or* $u = v = -1$.

2. *If* $a|b$ *and* $b|a$, *then* $a = \pm b$.

3. *Divisibility is transitive; if* $a|b$, $b|c$, *then* $a|c$.

4. *If* $a|b$ *and* $a|c$, *then* $a|(sb + tc)$, *where* s *and* t *are integers.*

Definition 7.1.4 (Prime) *A natural number is* ***prime*** *if it is greater than 1 and not divisible by any natural number other than 1 and itself.*

Proposition 7.1.3 *Any natural number other than 1 can be written as a product of prime numbers.*

Theorem 7.1.1 *There are infinitely many prime numbers.*

Proposition 7.1.4 *Given integers* a *and* b, *with* $d \geq 1$, *there exist unique intergers* q *and* r[10] *such* $a = qd + r$ *and* $0 \leq r < d$.

[10] The q is called **quotient** and the r is called **remainder**.

Definition 7.1.5 (Greatest Common Divisor) *A natural number d is the greatest common divisor of nonzero integers m and n if*

1. $d|m$ *and* $d|n$;
2. *whenever* $x \in \mathbb{N}$ *divides* m *and* n, *then* x *also divides* d.

Proposition 7.1.5 *For integers m and n, let*

$$I(m,n) = \{am + bn : a, b \in \mathbb{Z}\}. \tag{1}$$

1. *For* $x, y \in I(m,n)$, $x + y \in I(m,n)$ *and* $-x \in I(m,n)$.
2. $\forall x \in \mathbb{Z}, xI(m,n) \subseteq I(m,n)$
3. *If* $b \in \mathbb{Z}$ *divides* m *and* n, *then* b *divides all elements of* $I(m,n)$.

Lemma 7.1.1 *Let m and n be nonzero integers. If a natural number d is a common divisor of m and n and an element of $I(m,n)$, then d is the greatest common divisor of m and n.*

Proposition 7.1.6 *Let* $m, n, n_1, ..., n_k..., q_1, q_2, ...q_k \in \mathbb{Z}$

$$m = q_1 n + n_1 \tag{2}$$

$$n = q_2 n_1 + n_2 \tag{3}$$

$$...$$

$$n_{k-2} = q_k n_{k-1} + n_k \tag{4}$$

$$...$$

$$n_{r-1} = q_{r+1} n_r \tag{5}$$

The natural number n_r is the greatest common divisor of m and n, and furthermore $n_r \in I(m,n)$.

Corollary 7.1.1 *Let m and n be nonzero integers, and write $d = g.c.d.(m,n)$*

1. d *is the least element of* $\mathbb{N} \cap I(m,n)$.

2. *$I(m, n) = \mathbb{Z}d$, the set of all integer multiples of d.*

Definition 7.1.6 (Relatively Prime) *Nonzero integers m and n are* ***relatively prime*** *if g.c.d.(m, n).*

Corollary 7.1.2 *Two nonzero integers m and n are relatively prime if and only if there exist integers s and t such that $1 = sm + tn$.*

Corollary 7.1.3 *Suppose that a and b are relatively prime natural numbers, that x is an integer, and that both a and b divide x. Then ab divides x.*

Proposition 7.1.7 *If p is a prime number and a is any nonzero integer, then either p divides a or p and a are relatively prime.*

Proposition 7.1.8 *Let p be a prime number, and a and b nonzero integers. If $p|ab$, then $p|a$ or $p|b$.*

Corollary 7.1.4 *Suppose that a prime number $p|a_1a_2...a_r$, which for $r \in [1, r], a_n \neq 0$, then p divides one of the factors.*

Theorem 7.1.2 *The prime factorization of a natural number is unique.*

Definition 7.1.7 *Greatest common Divisor of Several Numbers A natural nnumber d is the greatest common divisor of nonzero integers $a_1, a_2, ..., a_n$, if*

1. *d divides each a_i and*
2. *whenever $x \in \mathbb{N}$ divides each a_i, then x also divides d.*

Lemma 7.1.2 *Given nonzero integers $a_1, a_2, ..., a_n (n \leq 2)$, there is a natural number d and an n-by-n integer matrix Q such that Q is invertible, Q^-1 also has integer entries, and*

$$(d, 0, ..., 0) = (a_1, a_2, ..., a_n)Q \tag{6}$$

Proposition 7.1.9 *The greatest common divisor of nonzero integers $a_1, a_2, ..., a_n$ exists, and is an integer linear combination of $a_1, a_2, ..., a_n$.*

Definition 7.1.8 (Relatively Prime) *We say that nonzsro integers $a_1, ..., a_n$ are* ***relatively prime*** *if their greatest common divisor is 1. We say that they are* ***pairwise relatively prime*** *if a_i and a_j are relatively prime whenever $i \neq j$.*

7.2 Modular Arithmetic

Definition 7.2.1 (Congruence) *Given integers a and b, and a natural number n, we say that "a is congruent to b modulo n" and we write $a \equiv b \mod n$ if $n|(a-b)$.*

Lemma 7.2.1 *Properties of Mod*

1. $\forall a \in \mathbb{Z}, a \equiv a \mod n$ *(Reflexive)*
2. $\forall a, b \in \mathbb{Z}$, *if* $a \equiv b \mod n$ *if and only if* $b \equiv a \mod n$. *(Symmetric)*
3. $\forall a, b, c \in \mathbb{Z}$, *if* $a \equiv b \mod n$ *and* $b \equiv c \mod n$, *then* $a \equiv v \mod n$. *(Transitive)*

Lemma 7.2.2 *For $a, b \in \mathbb{Z}$, the following are equivalent:*

- $a \equiv b \mod n$.
- $[a] = [b]$.[11]
- $rem_n(a) = rem_n(b)$.[12]
- $[a] \cap [b] \neq \varnothing$

Corollary 7.2.1 *There exist exactly n distinct residue classes modulo n, namely $[0], [1], ...[n-1]$. These classes are mutually disjoint.*

Lemma 7.2.3 *Let a, a', b, b' be integers with $a \equiv a' \mod n$ and $b \equiv b \mod n$. Then $a + b \equiv a' + b' \mod n$ and $ab \equiv a'b' \mod n$.*

Proposition 7.2.1 *Properties of Modulo Congruence:*

1. *Addition on $\mathbb{Z}_n$ is commutative and associative, $\forall [a], [b], [c] \in \mathbb{Z}_n$*

$$[a] + [b] = [b] + [a] \tag{7}$$

and,

$$[a] + [b] + [c] = [a] + ([b] + [c]) \tag{8}$$

[11]The set a is called the residue class or congruence class of a modulo n.

[12]Denote by $rem_n(a)$ the unique number r such that $0 \leq r < n$ and $a - r$ is divisible by n.

0 is an identity element for addition, $\forall [a] \in \mathbb{Z}_n$,

$$[0] + [a] = [a] \tag{9}$$

2. *Every element* $[a]$ *of* $\mathbb{Z}_n$ *has an additive inverse* $[-a]$, *that*

$$[a] + [-a] = [0] \tag{10}$$

3. *Multiplication on* $\mathbb{Z}_n$ *is commutative and associative;* $\forall [a], [b], [c] \in \mathbb{Z}_n$,

$$[a][b] = [b][a] \tag{11}$$

,and

$$[a][b][c] = [a]([b][c]) \tag{12}$$

4. $[1]$ *is an identity for multiplication;* $\forall [a] \in \mathbb{Z}_n$,

$$[1][a] = [a][1] \tag{13}$$

5. *The distributive law hold;* $\forall [a], [b], [z] \in \mathbb{Z}_n$,

$$[a]([b] + [c]) = [a][b] + [a][c] \tag{14}$$

Proposition 7.2.2 (Chinese Reminder Theorem) *Suppose* a *and* b *are relatively prime natural numbers, and* α *and beta are integers. There exists an integer* x *such that* $x \equiv \alpha \mod a$ *and* $x \equiv \beta \mod b$. *Moreover,* x *is unique up to congruence modulo* ab.