MAT246: Concepts in Abstract Mathematics:

Theorem Quick Reference Sheet

Tianyu Du

December 9, 2018

Contents

1 Introduction to the Natural Numbers

Lemma 1.1 (1.1.1)**.** Every natural number greater than 1 has a prime divisor.

Proof. Decompose iteratively if composite. ■

Theorem 1.1 (1.1.2)**.** There is no largest prime number.

Proof. Let S be the finite set containing all primes.
Consider $M = p_1 p_2 \dots p_n + 1 \notin S$ has no prime divisor, contradiction. ■

2 Mathematical Induction

Theorem 2.1 (The Principle of Mathematical Induction 2.1.1)**.** If S is any set of natural numbers with properties that

1. 1 is in S, and
2. $k + 1$ is in S whenever k is any number in S.

then S is the set of all natural numbers.

Proof. Let $T = S^c$ and suppose $T \neq \emptyset$. By WOP, let $t = \min T$.
Then by definition of minimum, $t - 1 \notin T$, i.e. $t - 1 \in S$.
By assumption of PMI, $t - 1 + 1 = t \in S$, contradiction.
$T = \emptyset \wedge S = \mathbb{N}$. ■

Theorem 2.2 (The Well-Ordering Principle 2.1.2)**.** Every set of natural numbers that contains at least one element has a smallest element in it.

Proof. Let $T \neq \emptyset$ and T has no minimal element.
Let $S = T^c \subseteq \mathbb{N}$. Clearly $1 \notin T$.
i.e. $1 \in S$. And suppose $1, 2, \dots k \notin T$, then $k + 1 \notin T$.
By principle of complete induction, $S = \mathbb{N}$, i.e. $T = \emptyset$.
Contradiction, thus T has a smallest element. ■

Theorem 2.3 (The Generalized Principle of Mathematical Induction 2.1.4)**.** Let m be a natural number. If S is a set of natural numbers with the properties that

1. m is in S, and
2. $k + 1$ is in S whenever k is in S and it greater than or equal to m.

then S contains every natural number greater than or equal to m.

Proof. Prove using PMI. ■

Theorem 2.4 (The Principle of Complete Mathematical Induction 2.2.1)**.** If S is any set of natural numbers with the properties that

1. $1 \in S$, and
2. $\{1, 2, \ldots, k\} \subset S \implies k + 1 \in S$,

then S is the set of all natural numbers.

Theorem 2.5 (The Generalized Principle of Complete Mathematical Induction 2.2.2)**.** If S is any set of natural numbers with the properties that

1. $m \in S$, and
2. $\{m, m + 1, \ldots, k\} \subset S \implies k + 1 \in S$,

then S contains all natural numbers greater than or equal to m.

Theorem 2.6 (2.2.4)**.** Every natural number other than 1 is a product of prime numbers.

Proof. Case 1: $n \in \mathbb{P}$.
Case 2: $n \notin \mathbb{P} \implies n = a \times b$, proven by GPCI. ■

3 Modular Arithmetic

[3.1.2]

Theorem 3.1. If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.

Theorem 3.2 (3.1.3)**.** When a and b are nonnegative integers, the relationship $a \equiv b \mod m$ is equivalent to a and b leaving equal reminders upon division by m.

Theorem 3.3 (3.1.4)**.** For a given modulus m, each integer is congruent to exactly one of the numbers in the set $\{0, 1, \ldots, m - 1\}$.

Theorem 3.4 (3.2.1)**.** Every natural number $d_n \ldots d_2 d_1 d_0$ is congruent to the sum of its digits modulo 9. In particular, a natural number is divisible by 9 if and only if the sum of its digits is divisible by 9.

$$\sum_{i=0}^{n} 10^i d_i \equiv \sum_{i=0}^{n} d_i \mod 9$$

Proof. Note that $10^i \equiv 1 \mod 9, \ \forall i \geq 0$. ■

4 The Fundamental Theorem of Arithmetic

Theorem 4.1 (The Fundamental Theorem of Arithmetic 4.1.1)**.** Every natural number greater than 1 can be written as a product of primes, and the expression of a number as a product of primes is unique except for the order of the factors

Corollary 4.1 (4.1.3)**.** If p is a prime number and a and b are natural numbers such that p divides ab, then p divides at least one of a and b. (That is, if a prime divides a product, then it divides at least one of the factors.)

$$p|ab \implies p|a \vee p|b$$

5 Fermat's Theorem and Wilson's Theorem

Theorem 5.1 (5.1.1)**.** If p is a prime and a is not divisible by p, and if $ab \equiv ac \mod p$, then $b \equiv c \mod p$.

Theorem 5.2 (Fermat's Theorem 5.1.2)**.** If p is a prime number and a is any natural not divisible by p, then

$$a^{p-1} \equiv 1 \mod p$$

Corollary 5.1 (5.1.3)**.** If p is a prime number and a is any natural number, then

$$a^p \equiv a \mod p$$

Definition 5.1 (5.1.4)**.** A **multiplicative inverse modulo** p for a natural number a is a natural number b such that $ab \equiv 1 \mod p$.

Corollary 5.2 (5.1.5)**.** If p is a prime and a is a natural number that is not divisible by p, then there exists a natural number x such that

$$ax \equiv 1 \mod p$$

Proof. Using Fermat's Theorem and take $x = a^{p-2}$. ∎

Lemma 5.1 (5.1.6)**.** If a and c have the same multiplicative inverse modulo p, then a is congruent to c modulo p.

Proof. Suppose $ab \equiv 1 \mod p$ and $cb \equiv 1 \mod p$,
then $abc \equiv c \mod p$, which implies $a \equiv c \mod p$. ∎

Theorem 5.3 (5.1.7)**.** Let $p \in \mathbb{P}$, and $x \in \mathbb{Z}$ satisfying $x^2 \equiv 1 \mod p$, then $x \equiv 1 \mod p$ or $x \equiv -1 \mod p$.

Proof. $x^2 \equiv 1 \mod p \iff p|x^2 - 1 \iff p|(x-1)(x+1) \implies p|(x-1) \vee p|(x+1)$. ■

Theorem 5.4 (Wilson's Theorem 5.2.1)**.** If p is a prime number, then

$$(p-1)! \equiv -1 \mod p$$

Theorem 5.5 (5.2.2)**.** If m is a composite number larger than 4, then

$$(m-1)! \equiv 0 \mod m$$

Theorem 5.6 (Extended version of Wilson's theorem 5.2.3)**.** If m is a natural number other than 1, then $(m-1)! \equiv -1 \mod m$ if and only if $m \in \mathbb{P}$.

6 Sending and Receiving Secret Messages

Theorem 6.1 (6.1.2)**.** Let $N = pq$, where p and q are distinct prime numbers, and let $\phi(N) = (p-1)(q-1)$. If k and a are any natural natural numbers, then

$$a \cdot a^{k\phi(N)} \equiv a \mod N$$

7 The Euclidean Algorithm and Applications

RSA encryption procedure(7.2.5):

1. Phase 1 (Receiver)
   (a) pick large $p, q \in \mathbb{P}$ such that $p \neq q$.
   (b) compute $N = pq$ and $\phi(N) = (p-1)(q-1)$.
   (c) pick e relatively prime to $\phi(N)$.
   (d) announce N, e.
2. Phase 2 (Sender)
   (a) pick message $M < N$.
   (b) compute encoded message R from $M^e \equiv R \mod N$.
   (c) announce R.
3. Phase 3 (Receiver)

(a) compute decoder $d > 0$ from $de + k\phi(N) = 1$.
(b) compute decoded message M from $R^d \equiv 1 \mod N$.

Lemma 7.1 (7.2.2)**.** If a prime number divides the product of two natural numbers, then it divides at least one of the numbers.

Lemma 7.2 (Extended version of lemma 7.2.2, 7.2.3)**.** For any natural number n, if a prime divides the product of n natural numbers, then it divides at least one of the numbers.

Proof. Using lemma 7.2.2 and PMI. ■

Theorem 7.1 (7.2.8)**.** The *Diophantine* equation $ax + by = c$, with a, b, and c integers, has integral solutions if and only if $\gcd(a, b)$ divides c.

Definition 7.1 (7.2.12)**.** For any natural number m, the **Euler ϕ function**, $\phi(m)$, is defined to be the number of numbers in $\{1, 2, \ldots, m-1\}$ that are relatively prime to m. (Note that 1 is relatively prime to every natural number)

Theorem 7.2 (7.2.14)**.** If p is prime, then $\phi(p) = p - 1$.

Proof. Directly form the definition of Euler-ϕ function. ■

Theorem 7.3 (7.2.15)**.** If p and q are distinct primes, then $\phi(pq) = (p-1)(q-1)$.

Proof. Consider the multiples of p and q in set $\{1, 2, \ldots, pq-1\}$.
There would be $p-1$ multiples of q and $q-1$ multiples of p.
Total number of multiples is $(p-1) + (q-1) = p + q - 2$.
Any number other than the multiples above will be relatively prime to pq.
There would be $pq - 1 - p - q + 2 = pq - p - q + 1 = (p-1)(q-1)$. ■

Theorem 7.4 (unnumbered, result from Euclidean algorithm)**.** Let $a, b \in \mathbb{N}$, then there exists integers z_1, z_2 such that

$$z_1 a + z_2 b = \gcd(a, b)$$

Theorem 7.5. If a is relatively prime to m and $ax \equiv ay \mod m$, then $x \equiv y \mod m$.

Theorem 7.6 (Euler's Theorem 7.2.17)**.** If m is a natural number greater than 1 and a is a natural number that is relatively prime to m, then

$$a^{\phi(m)} \equiv 1 \mod m$$

Theorem 7.7 (7.3.Q27)**.** Let $n \in \mathbb{N}$, and suppose n can be factorized into $p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ then

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_m^{k_m} - p_m^{k_m-1})$$

8 Rational Numbers and Irrational Numbers

Theorem 8.1 (The Rational Roots Theorem 8.1.9)**.** If $\frac{m}{n}$ is a rational root of the polynomial

$$a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$$

where a_j are integers and $\underline{m \text{ and } n \text{ are relatively prime}}$, then $m | a_0$ and $n | a_k$.

Theorem 8.2 (8.2.6)**.** If p is a prime number, then $\sqrt{p}$ is irrational.

Theorem 8.3 (8.2.8)**.** If the square root of a natural number is rational, then the square root is an integer.

Theorem 8.4 (Extended 8.2.8)**.** Let $n \in \mathbb{N}$, then $\sqrt{n} \in \mathbb{Q}$ <u>if and only if</u> n is a perfect square.

Theorem 8.5 (Extended 8.2.8)**.** Let $n \in \mathbb{N}$, then $\sqrt[3]{n} \in \mathbb{Q}$ <u>if and only if</u> n is a perfect cube.

Remark 8.1. As immediate result from (8.2.8), we can conclude that the square or cubic root is integer.

$$\sqrt{n} \in \mathbb{Q} \implies \sqrt{n} \in \mathbb{Z}$$
$$\sqrt[3]{n} \in \mathbb{Q} \implies \sqrt[3]{n} \in \mathbb{Z}$$

9 The Complex Numbers

Theorem 9.1 (9.2.3)**.** The modulus of the product of two complex numbers is the product of their moduli. The argument of the product of two complex numbers is the sum of their arguments.

Theorem 9.2 (9.2.5)**.** Every complex number has a complex square root.

Theorem 9.3 (De Moivre's Theorem 9.2.6)**.** For every natural number n

$$(r(\cos\theta + i\sin\theta))^n = r^n(\cos n\theta + i\sin n\theta)$$

Theorem 9.4 (The Fundamental Theorem of Algebra 9.3.1)**.** Every non-constant polynomial with complex coefficients has a complex root.

Theorem 9.5 (The Factor Theorem 9.3.6)**.** The complex number r is a root of polynomial $p(z)$ if and only if $z - r$ is a factor of $p(z)$. That's

$$\exists f(z),\ p(z) = f(z)(z - r)$$

Theorem 9.6 (9.3.8)**.** A polynomial of degree n has at most n complex roots; if "multiplicities" are counted, it has exactly n roots.

10 Sizes of Infinite Sets

Definition 10.1 (10.1.8)**.** The sets $\mathcal{S}$ and $\mathcal{T}$ have the **same cardinality** if there is a bijective function $f : \mathcal{S} \to$ Ţ.

Theorem 10.1 (10.1.13)**.**

$$|\mathbb{N}| = |\mathbb{Q}^{+}|$$

Definition 10.2 (10.2.1)**.** A set is **countable** if it is either finite or has the same cardinality as the set of natural numbers.

Theorem 10.2 (10.2.2)**.**

$$|[0, 1]| > \aleph_0$$

Theorem 10.3 (10.2.4)**.** Let $a, b \in \mathbb{R}$ and $a < b$, then

$$|[a, b]| = |[0, 1]|$$

Theorem 10.4 (Unnumbered, generalized)**.** All open, half-open and closed intervals in $\mathbb{R}$ have the same cardinality c.

Theorem 10.5 (10.2.7)**.** If $|\mathcal{S}| = |\mathcal{T}|$ and $|\mathcal{T}| = |\mathcal{U}|$, then $|\mathcal{S}| = |\mathcal{U}|$.

Theorem 10.6 (10.2.10)**.** The union of a countable number of countable sets is countable.

Theorem 10.7 (The Cantor-Bernstein Theorem 10.3.5)**.** If $\mathcal{S}$ and $\mathcal{T}$ are sets such that $|\mathcal{S}| \leq |\mathcal{T}|$ and $|\mathcal{T}| \leq |\mathcal{S}|$, then $|\mathcal{S}| = |\mathcal{T}|$.

Corollary 10.1 (10.3.6)**.** If $\mathcal{S}$ is a subset of $\mathcal{T}$ and there exists a function $f : \mathcal{T} \to \mathcal{S}$ that is injective, then $\mathcal{S}$ and $\mathcal{T}$ have the same cardinality.

Theorem 10.8. A subset of a countable set is countable.

Corollary 10.2 (10.3.10)**.** Is $\mathcal{S}$ is any set and there exists a injective function $f : \mathcal{S} \to \mathbb{N}$, then $\mathcal{S}$ is countable.

Theorem 10.9 (10.3.12)**.** The set of all finite sequences of natural numbers countable.

Remark 10.1. All sequences are countable.

Definition 10.3 (10.3.14)**.** Let $\mathcal{S}$ and $\mathcal{T}$ by any sets. We will say that $\mathcal{T}$ **can be labelled** by the set $\mathcal{S}$ if there is way of assigning a finite sequence of elements of $\mathcal{S}$ to each element of $\mathcal{T}$ so that each finite sequence corresponds to at most one element $\mathcal{T}$.

Theorem 10.10 (The Enumeration Principle 10.3.16)**.** Every set that can be labelled by a countable set is countable.

Definition 10.4 (10.3.19)**.** The real number of x_0 is said to be **algebraic** if it is the root of a polynomial with integer coefficients. The real number x_0 is said to be **transcendental** if there is no polynomial with integer coefficients that x_0 as a root.

Theorem 10.11 (Theorem 10.3.20)**.**

$$|\mathcal{A}| \leq \aleph_0$$

Corollary 10.3 (10.3.21)**.** There exist transcendental numbers.

Theorem 10.12 (10.3.24)**.** If $\mathcal{S}$ is an infinite set, then $\aleph_0 \leq |\mathcal{S}|$.

Theorem 10.13 (10.3.27)**.** For every set $\mathcal{S}$, then

$$|\mathcal{S}| < |\mathcal{P}(\mathcal{S})|$$

Theorem 10.14 (10.3.28)**.** The cardinality of the set of all sets of natural numbers is the same as the cardinality of the set of real numbers. That is,

$$|\mathcal{P}(\mathbb{N})| = 2^{\aleph_0} = c$$

Theorem 10.15 (10.3.30 and extended)**.** The cardinality of the unit square and unit cube are c.

Theorem 10.16 (Generalized 10.3.30)**.** Let $n \in \mathbb{N}$, then

$$|\mathbb{R}^n| = c$$

Definition 10.5 (10.3.31)**.** If S is a set and S_0 is a subset of S, then the **characteristic function** of S_0 as a subset of S is the function f, with domain S, defined by

$$f(s) = \begin{cases} 1 \text{ if } s \in S_0 \\ 0 \text{ if } s \notin S_0 \end{cases}$$

12 Constructibility

Definition 12.1 (12.2.2)**.** A real number is **constructible** if the point corresponding to it one the number line can be obtained from marked points 0 and 1 by performing a finite sequence of constructions using only a straightedge and compass.

Theorem 12.1 (12.2.9)**.** If $\mathcal{F}$ is any subfield of $\mathbb{R}$, then $\mathcal{F}$ contains all rational numbers.

Theorem 12.2 (12.2.10)**.** The set of constructible number is a subfield of $\mathbb{R}$.

Theorem 12.3 (12.2.12& 12.2.13)**.** Let $\mathcal{F}$ be any subfield of $\mathbb{R}$ and suppose that $0 < r \in \mathcal{F}$ and $\sqrt{r} \notin \mathcal{F}$, then the field obtained by adjoining $\sqrt{r}$ to $\mathcal{F}$ is defined as

$$\mathcal{F}(\sqrt{r}) = \{a + b\sqrt{r} : a, b \in \mathcal{F}\}$$

is called the extension of $\mathcal{F}$ by $\sqrt{r}$. And then $\mathcal{F}(\sqrt{r})$ is a subfield of $\mathbb{R}$.

Theorem 12.4 (12.2.15)**.** If r is a positive constructible number, then $\sqrt{r}$ is constructible.

Definition 12.2 (12.2.16)**.** A **tower of fields** is a finite sequence $\mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ of subfields of $\mathbb{R}$ such that $\mathcal{F}_0 = \mathbb{Q}$ and, for each i from 1 to n, there is a positive number r_i in $\mathcal{F}_{i-1}$ such that $\sqrt{r_i}$ is not in $\mathcal{F}_{i-1}$ and $\mathcal{F}_i = \mathcal{F}_{i-1}(\sqrt{r_i})$.

Definition 12.3 (12.3.1)**.** A **surd** is a number that is in some field that is in a tower. That is, x is a surd if there exists a tower:

$$\mathcal{F}_0 \subset \mathcal{F}_1 \subset \mathcal{F}_2 \subset \cdots \subset \mathcal{F}_n$$

Theorem 12.5 (12.3.2)**.** The set of all surds is a subfield of $\mathbb{R}$. Moreover, if r is a positive surd, then $\sqrt{r}$ is a surd.

Theorem 12.6 (12.3.3)**.** Every surd is constructible.

Theorem 12.7 (12.3.10)**.** The points of intersection of a line that has an equation with surd coefficients and a circle that has an equation with surd coefficients lie in the surd plane.

Theorem 12.8 (12.3.11)**.** The points of intersection of two distinct circles that have equations with surd coefficients lie in the surd plane.

Theorem 12.9 (12.3.12)**.** The field of constructible numbers is the same as the field of surds.

Theorem 12.10 (12.3.13)**.**

$$\theta \in C \iff \cos\theta \in C$$

Theorem 12.11 (12.3.16)**.**

$$\cos 3\theta = 4\cos^2\theta - 3\cos\theta$$

Theorem 12.12 (12.3.21)**.** If $a + b\sqrt{r}$ is in $\mathcal{F}(\sqrt{r})$ and is a root of a polynomial with rational coefficients, then $a - b\sqrt{r}$ is also a root of the polynomial.

Theorem 12.13 (12.3.22)**.** If a cubic equation with rational coefficients has a constructible root, then the equation has a rational root.

References

Rosenthal, D., Rosenthal, D., & Rosenthal, P. (2014). A Readable Introduction to Real Mathematics. Springer.