MAT246: Concepts in Abstract Mathematics:
Theorem Quick Reference Sheet

Tianyu Du

December 3, 2018

This work is licensed under a Creative Commons "Attribution-NonCommercial 4.0 International" license.

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 $1, 2, \ldots k \notin T$, 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 m and n 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 rational.

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.

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

References

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