# Theory of Numbers

Hechen Hu

November 29, 2017

# Contents

# 1

# Divisibility, the Fundamental Theorem of Number Theory

## 1.1 Divisibility

**Definition.** The divisors of a number that are less than the number itself is called its *parts*. If a number is the sum of its parts, it's called a *perfect number*(e.g. 6, 28, and 496). If two numbers are the sum of the other one's parts, they are called *amicable*(e.g. 220 and 284).

**Theorem 1.1.1** (Remainder Theorem)**.** *For all numbers $a$ and $b \neq 0$, there is an integer $c$ and a number $d$ such that*

$$a = bc + d \quad \text{and} \quad 0 \leqslant d < |b|$$

*and only one such $c$ and $d$ exist. We say that $a$ divided by $b$ has quotient $c$ with remainder $d$.*

**Proposition.** For all numbers $a$ and $b \neq 0$, there is an integer $c'$ and a number $d'$ such that

$$a = bc' + d' \quad \text{and} \quad -\frac{|b|}{2} < d' \leqslant \frac{|b|}{2}$$

and only one such $c'$ and $d'$.

**Theorem 1.1.2** (Four Number Theorem)**.** *If $a$ and $c$ are numbers and $b$ and $d$ are integers such that*

$$ab = cd$$

*then there exists a positive number $r$ and positive integers $s$, $t$, and $u$ such that the following equalities hold:*

$$a = rs, \quad b = tu, \quad c = rt, \quad d = su$$

*If, in addition, $a$ and $c$ are integers, then $r$ may be taken to be an integer.*

**Definition.** An integer $a$ is a *divisor* of an integer $b$ if there exists a number $c$ such that

$$b = ac$$

In this case we also say that $b$ is *divisible* by $a$ and denoted $a|b$. Otherwise, it is denoted $a \nmid b$. Among the divisors of $a$, 1, $-1$, $a$, and $-a$ is called its *trivial divisors*. Other positive divisors smaller than $a$ are called its *proper divisors*. 1 and $-1$ is called *units*.

**Definition.** Two numbers that do not have a common divisor other than the units are called *relatively prime*.

***Example* 1.1.** *for any number $a$*

- $a|0$;
- $0$ *is only a divisor of* $0$.
- *If $a|b$ and $b|c$, then $a|c$.*

Division is reflexive and transitive. In general it is not symmetric.

If $b_i$ are integers such that $a|b_i$, and $c_i$ are arbitrary integers ($i = 1, 2, \cdots, k$), then $a|\sum_{i=1}^{k} b_i c_i$.

**Definition.** A number $a$ and $-a$ is said to be *associates* of each other. Theorems relating to divisibility apply to the classes of associated numbers.

***Example* 1.2.** *If $a|b$, then $ca|cb$, and if $c \neq 0$, then the first relation follows from the second.*

**Lemma** (Euclid's Lemma)**.** *If a number divides the product of two numbers and is relatively prime to one of the factors, then it must divide the other factor.*

## 1.2 Prime Numbers

**Definition.** If a number only has the trivial ones as its divisors, it's called *prime*. If a number is not prime and not unit, it's called a *composite number*.

**Theorem 1.2.1.** *Every number larger than one has a prime divisor.*

**Theorem 1.2.2.** *There are infinitely many prime numbers.*

**Theorem 1.2.3.** *Every number different from 0 and not a unit can be decomposed into the product of finitely many primes.*

**Definition.** For certain number, if it divide a product of numbers, it also divide one of the factors. Numbers of this type that are different from 0 and the units have the *prime property*.

**Theorem 1.2.4.** *The prime numbers are precisely those with the prime property.*

**Theorem 1.2.5** (Fundamental Theorem of Arithmetic)**.** *The prime factorization of a nonzero number that is not a unit is unique up to the order and signs of the factors.*

**Proposition.** If $a_1, \cdots, a_j; b_1, \cdots, b_k$ are integers such that

$$a_1 a_2 \cdots a_j = b_1 b_2 \cdots b_k$$

then there exists integer $t_{uv}$ $(1 \leqslant u \leqslant j, 1 \leqslant v \leqslant k)$ such that

$$a_u = \prod_{v=1}^{k} t_{uv}, \qquad b_v = \prod_{u=1}^{j} t_{uv}$$

# 2

# Congruences

3

# Rational and Irrational Numbers. Approximation of Numbers by Rational Numbers (Diophantine Approximation)

# 4

# Geometric Methods in Number Theory

# 5

# Properties of Prime Numbers

# 6

# Sequences of Integers

# 7

# Diophantine Problems

# 8

# Arithmetic Functions