Definition 1.2.1 An integer \( p > 1 \) is called a prime in case there is no divisor \( d \) of \( p \) satisfying \( 1 < d < p \). If an integer \( a < 1 \) is not a prime, it is called a composite number.

Theorem 1.2.2 Every integer \( n > 1 \) can be expressed as a product of primes.

Lemma 1.2.3 If \( p \mid a_1 a_2 \cdots a_n \), \( p \) being a prime, then \( p \) divides at least one factor \( a_i \).

Theorem 1.2.4 (Fundamental theorem of arithmetic) The factorization of any integer \( n > 1 \) into primes is unique apart from the order of the prime factors. [Two proofs.]

Remark 1.2.5 (a) For any positive integer \( a \), \( a = \prod_p p^\alpha(p) \) is called the canonical factoring of \( n \) into prime powers.
   (b) let \( a = \prod_p p^\alpha(p) \), \( b = \prod_p p^\beta(p) \), \( c = \prod_p p^\gamma(p) \). If \( c = ab \), then \( \gamma(p) = \alpha(p) + \beta(p) \).
   \( (a, b) = \prod_p p^{\min(\alpha(p), \beta(p))} \), \( [a, b] = \prod_p p^{\max(\alpha(p), \beta(p))} \).
   \( a \) is a perfect square if and only if, for all \( p \), \( \alpha(p) \) is even.
   (c) The second proof of 1.2.4 is independent of the previous theorems, so the formulas of \((a, b), [a, b]\) can be used to prove many results in Section 1.1.

Example 1.2.6 The number systems in which the factorization is not unique.
   (a) \( \mathcal{E} = \{2, 4, 6, 8, \cdots \} \).
   (b) \( \mathcal{C} = \{a + b\sqrt{6} : a, b \in \mathbb{Z}\} \).

Example 1.2.7 (Pythagoras) The number \( \sqrt{2} \) is irrational.

1.2.8 The Sieve of Eratosthnes (276-194 B.C.) Write down the integers from 2 to \( n \) in natural order and then systematically eliminate all the composite numbers by striking out all multiples of \( p \) of the primes \( p \leq \sqrt{n} \). The integers that left on the list are primes.

Theorem 1.2.9 (Euclid) The number of primes is infinite. [Three proofs.]

Remark 1.2.10 It is not known whether there are infinitely many prime \( p \) for which \( p^# + 1 \) is also prime, where \( p^# \) is the product of all primes that less than or equal to \( p \).
   At present, 19 primes of the form \( p^# + 1 \) have been identified: \( p = 2, 3, 5, 7, 11, 31, 379, 1019, 1021, 2657, 3229, 4547, 4787, 11549, 13649, 18523, 23801, \)
24029, 42209 (discovered in 2000). The integer $p\# + 1$ is composite for all other $p \leq 120000$.

**Remark 1.2.11** Let $p_n$ denote the $n$th of the prime numbers in natural order.

(a) $p_n < p_1 p_2 \cdots p_{n-1} + 1$, $n \geq 2$.
(b) $p_n < p_1 p_2 \cdots p_{n-1} - 1$, $n \geq 3$.
(c) (Bonse inequality) $p_n^2 < p_1 p_2 \cdots p_{n-1}$, $n \geq 5$.
(d) $p_{2n} \leq p_2 p_3 \cdots p_n - 2$, $n \geq 3$.

**Theorem 1.2.12** If $p_n$ is the $n$th prime number, then $p_n \leq 2^{2^{n-1}}$.

**Corollary 1.2.13** For $n \geq 1$, there are at least $n + 1$ primes less than $2^{2^n}$.

**Theorem 1.2.14** (Bertrand conjecture 1845, proved by P.L. Tchebycheff in 1852) Between $n \geq 2$ and $2n$ there is at least one prime.

**Corollary 1.2.15** $p_n < 2^n$.

**Theorem 1.2.16** For every real number $y \geq 2$, $\sum_{\text{prime } p \leq y} \frac{1}{p} > \ln \ln y - 1$.

**Remark 1.2.17** (a) A corollary of 1.2.16 is 1.2.9.
(b) It can be shown that $\sum_{\text{prime } p \leq y} \frac{1}{p} - \ln \ln y$ is a bounded function of $y$.
(c) (Prime Number Theorem) $\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1$, that is $\pi(x) \sim \frac{x}{\ln x}$, where $\pi(x)$ is the number of primes $\leq x$.

**Remark 1.2.18** A repunit is an integer written as a string of 1’s. Let $R_n$ denote the repunit consisting of $n$ consecutive 1’s. $R_2, R_{19}, R_{23}, R_{317}, R_{1031}, R_{49081}, R_{86453}$ (discovered in 2001) are primes. These are the only possible $R_n$ for all $n \leq 45000$.

**Conjecture 1.2.19** (a) There are infinitely many primes of the form $n^2 - 2$.
(b) There are infinitely many primes of the form $2^n + 1$.
(c) There are infinitely many primes of the form $n^2 + 1$.
(d) There are infinitely many primes of the form $2^n - 1$.
(e) There are infinitely many primes $p$ such that $p + 50$ is also prime.
(f) Every even integer can be written as the difference of two consecutive primes in infinitely many ways.

**Remark 1.2.20** There is an unsolved question: Whether there are infinitely many pairs of twin primes.

The largest twins are $33218925 \cdot 2^{169690} \pm 1$ (discovered in 2002).

**Theorem 1.2.21** There are arbitrarily large gaps in the series of primes.
Remark 1.2.22 (a) The largest gap discovered is 1132 after the prime 1693182318746371.
(b) Conjecture: There is a prime gap for every even integer.

Remark 1.2.23 (a) Goldbach Conjecture (1972): Every even integer is the sum of two numbers that are either primes or 1.
(b) More generally, every even integer greater than 4 is the sum of two odd prime numbers.
(c) This conjecture implies that each odd number larger than 7 is a sum of three odd primes.
(d) It is known that every even integer is a sum of six or fewer primes.

Theorem 1.2.24 (Hardy, Littlewood, 1922; I.M. Vinogradov, 1937; Borozdkin, 1956; 2002) All odd integers large than $10^{1346}$ can be written as a sum of three odd primes.

Proposition 1.2.25 There are infinitely many primes of the form $4n + 3$.

Theorem 1.2.26 (P.G.L. Dirichlet, 1837) If $a$ and $d$ are relatively prime positive integers, then the arithmetic progression $a, a + d, a + 2d, a + 3d, \ldots$ contains infinitely many primes.

Theorem 1.2.27 If all the terms of the arithmetic progression $p, p+d, p+2d, p+3d, \ldots, p+(n-1)d$ are prime numbers, then $d$ is divisible by every prime $q < n$.

Remark 1.2.28 (a) There is an unsolved problem: Whether there exist arbitrary long arithmetic progression consists only of primes.
(b) The longest progression found to date is $114103378550553+4609098694200n$, $0 \leq n \leq 21$.
(c) A sequence of 10 consecutive primes which is an arithmetic progression was discovered, the common difference is 210.

Remark 1.2.29 (a) Let $f(n) = n^2 + n + 41$. Then $f(k)$ are primes for $k = 0, 1, 2, \ldots, 40$.
(b) Let $g(n) = 103n^2 - 3945n + 34381$. Then $g(k)$ are primes for $k = 0, 1, 2, \ldots, 42$.
(c) Let $h(n) = 36n^2 - 810n + 2753$. Then $h(k)$ gives a string of 45 prime values.

Lemma 1.2.30 It is impossible to find a polynomial $f(n)$ such that $f(k)$ are primes for all $k \in \mathbb{N}$.

Theorem 1.2.31 (W.H.Mills, 1947) There is a positive real number $r$ such that $f(n) = [r^{3^n}]$ is prime for $n = 1, 2, 3, \ldots$. 
Section 1.3 The Binomial Theorem

Definition 1.3.1 Let $\alpha \in \mathbb{R}$, and $k \in \mathbb{N}$. Then the binomial coefficient $\binom{\alpha}{k}$ is given by $\frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!}$.

Lemma 1.3.2 The product of any $k$ consecutive integers is divisible by $k!$.

Theorem 1.3.3 (The binomial Theorem) For any integer $n \geq 1$ and any real numbers $x, y$, $(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$. [Combinatorial proof, analytic proof]

Lemma 1.3.4 Let $P(z) = \sum_{k=0}^{n} a_k z^k \in \mathbb{C}[z]$. Then $a_r = \frac{P^{(r)}(0)}{r!}$ for $0 \leq r \leq n$.

Lemma 1.3.5 $\binom{n}{k} + \binom{n+1}{k} = \binom{n+1}{k+1}$ for $n, k \in \mathbb{N}$.

Theorem 1.3.6 $(1 + z)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} z^k$ for $|z| < 1$. [Combinatorial proof, analytic proof]

Example 1.3.7 The Catalan numbers defined by $C_n = \frac{1}{n+1} \binom{2n}{n}$, $n \geq 0$. It first appeared in 1938 when Eugène Catalan (1814-1894) show that there are $C_n$ ways of parenthesizing a nonassociative product of $n + 1$ factors.