

Math 453: Elementary Number Theory
Definitions and Theorems

(Class Notes, Spring 2008 – A.J. Hildebrand)

Version 4/30/2008

Contents

1	Divisibility and Factorization	5
1.1	Divisibility	5
1.2	Primes	5
1.3	The greatest common divisor	6
1.4	The least common multiple	8
1.5	The Fundamental Theorem of Arithmetic	8
1.6	Primes in arithmetic progressions	9
2	Congruences	10
2.1	Definitions and basic properties; applications	10
2.2	Linear congruences in one variable	11
2.3	The Chinese Remainder Theorem	12
2.4	Wilson's Theorem	12
2.5	Fermat's Theorem	12
2.6	Euler's Theorem	13
3	Arithmetic functions	14
3.1	Some notational conventions	14
3.2	Arithmetic functions: Definitions and basic examples	16
3.3	The algebra of arithmetic functions	17
3.4	The Moebius function and the Moebius inversion formula	18
3.5	The Euler phi function	18
3.6	The number-of-divisors and sum-of-divisors functions	19
4	Quadratic residues	21

4.1	Quadratic residues and nonresidues	21
4.2	The Legendre symbol	22
4.3	The law of quadratic reciprocity	23
5	Primitive roots	24
5.1	The order of an integer	24
5.2	Primitive roots	25
5.3	The Primitive Root Theorem	25
6	Continued fractions	26
6.1	Definitions and notations	26
6.2	Expansions of real numbers into continued fractions	27
6.3	Convergents	28
6.4	Rational approximations	28

About these notes

One purpose of these notes is to serve as a handy reference for homework problems, and especially for proof problems. The definitions given here (e.g., of divisibility) are the “authoritative” definitions, and you should use those definitions in proofs. The results stated here are those you are free to use and refer to in proofs; in general, anything else (e.g., a theorem you might have learned in high school) is not allowed.

Another purpose is to serve as a cheat/review sheet when preparing for exams. The definitions and theorems contained in these notes are those you need to know in exams.

Finally, the notes may be useful as a quick reference or refresher on elementary number theory for those taking more advanced number theory classes (e.g., analytic or algebraic number theory).

The notes are loosely based on the Strayer text, though the material covered is pretty standard and can be found, in minor variations, in most undergraduate level number theory texts. The chapters correspond to those in Strayer, but I have made a few small changes in the subdivision of the chapters.

The definitions and results can all be found (in some form) in Strayer, but the numbering is different, and I have made some small rearrangements, for example, combining several lemmas into one proposition, demoting a “theorem” in Strayer to a “proposition”, etc. The goal in doing this was to streamline the presentation by having several layers of results, with a clear delineation between the various types of results:

- **Theorems:** Those are the key results, usually with descriptive names attached (e.g., “Fundamental Theorem of Arithmetic”). These results typically have more difficult proofs, often well above homework level.
- **“Starred” theorems:** Results whose statement you should know, but whose proof is beyond the scope of an undergraduate number theory course, are indicated by an asterisk. A typical example is the Prime Number Theorem.
- **Propositions:** A proposition typically collects some simple, but very useful, properties of a concept. The proofs are generally on the easy side, and many (but not all) are at a level that would be reasonable to ask for in an exam.
- **Corollaries:** A corollary is attached to a particular theorem (or proposition), and presents a simple consequence of the theorem, or restates the theorem in a special

case. The derivation of a corollary from the corresponding theorem is usually easy, and often immediate.

- **Lemmas:** A lemma is an auxiliary result that is needed (usually) for the proof of a theorem. Lemmas are rarely of interest in their own right, and therefore in general not worth memorizing (in contrast to the other theorem-like structures). Since I do not include the proofs here, I have generally avoided stating lemmas that arise in those proofs. If a result that is stated as “Lemma” in Strayer is important in its own right and worthy of memorizing, I have elevated it to the status of a “Proposition” or “Theorem”.

Chapter 1

Divisibility and Factorization

1.1 Divisibility

Definition (Divisibility) Let $a, b \in \mathbf{Z}$. We say that a **divides** b (equivalently, a is a **divisor of** b , or b is **divisible by** a , or a is a **factor of** b) if there exists $c \in \mathbf{Z}$ such that $b = ac$. We write $a \mid b$ if a divides b , and $a \nmid b$ if a does *not* divide b .

Proposition 1.1 (Elementary properties of divisibility)

- (i) (*Transitivity*) Let $a, b, c \in \mathbf{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.
- (ii) (*Linear combinations*) Let $a, b, c \in \mathbf{Z}$. If $a \mid b$ and $a \mid c$, then $a \mid bn + cm$ for any $n, m \in \mathbf{Z}$. In particular, if $a \mid b$ and $a \mid c$, then $a \mid b + c$ and $a \mid b - c$.
- (iii) (*Size of divisors*) Let $a, b \in \mathbf{Z}$, with $b \neq 0$. If $a \mid b$, then $|a| \leq |b|$. In particular, any positive divisor a of a positive integer b must fall in the interval $1 \leq a \leq b$.
- (iv) (*Divisibility and ratios*) Let $a, b \in \mathbf{Z}$ with $a \neq 0$. Then $a \mid b$ holds if and only if $\frac{b}{a} \in \mathbf{Z}$.

Definition (Greatest integer function) For any $x \in \mathbf{R}$, the **greatest integer function** $[x]$ is defined as the greatest integer m satisfying $m \leq x$. An alternative notation for $[x]$ is $\lfloor x \rfloor$, the **floor function**.

Theorem 1.2 (Division Algorithm) Given $a, b \in \mathbf{Z}$ with $b > 0$ there exist unique $q, r \in \mathbf{Z}$ such that $a = qb + r$ and $0 \leq r < b$. Moreover, q and r are given by the formulas $q = [a/b]$ and $r = a - [a/b]b$.

1.2 Primes

Definition (Primes and composite numbers) Let $n \in \mathbf{N}$ with $n > 1$. Then n is called a **prime** if its only *positive* divisors are 1 and n ; it is called **composite** otherwise. Equivalently, n is composite if it can be written in the form $n = ab$ with $a, b \in \mathbf{Z}$ and $1 < a < n$ (and hence also $1 < b < n$); and n is prime otherwise.

Remark The number 1 is not classified in this manner, i.e., 1 is neither prime nor composite.

Proposition 1.3 (Existence of prime factors) *Let $n \in \mathbf{N}$ with $n > 1$. Then n has at least one prime factor (possibly n itself); i.e., there exists a prime p with $p \mid n$.*

Proposition 1.4 (Primality test) *Let $n \in \mathbf{N}$ with $n > 1$. Then n is prime if and only if n is not divisible by any prime p with $p \leq \sqrt{n}$.*

Theorem 1.5 (Euclid's Theorem) *There are infinitely many primes.*

Theorem 1.6 (Gaps between primes) *There are arbitrarily large gaps between primes; i.e., for every $n \in \mathbf{N}$, there exist at least n consecutive composite numbers.*

Definition (Prime counting function) Let $x \in \mathbf{R}$ with $x > 0$. Then $\pi(x)$ is the number of primes p with $p \leq x$.

***Theorem 1.7 (Prime Number Theorem)** *The prime counting function $\pi(x)$ satisfies*

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1.$$

Definition (Mersenne and Fermat primes)

- (i) The numbers of the form $M_p = 2^p - 1$, where p is prime, are called **Mersenne numbers**; a Mersenne number that is prime is called a **Mersenne prime**.
- (ii) The numbers of the form $F_n = 2^{2^n} + 1$, where $n = 0, 1, \dots$, are called **Fermat numbers**; a Fermat number that is prime is called a **Fermat prime**.

Conjectures (Famous conjectures about primes)

- (i) **Mersenne primes:** *There are infinitely many Mersenne primes.*
- (ii) **Fermat primes:** *There are only finitely many Fermat primes.*
- (iii) **Twin Prime Conjecture:** *There infinitely many primes p such that $p + 2$ is also prime.*
- (iv) **Goldbach Conjecture:** *Every even integer $n \geq 4$ can be expressed as a sum of two primes (not necessarily distinct), i.e., n can be written in the form $n = p_1 + p_2$, where p_1 and p_2 are primes.*

1.3 The greatest common divisor

Definition (Greatest common divisor) Let $a, b \in \mathbf{Z}$, with a and b not both 0. The **greatest common divisor (gcd)** of a and b , denoted by $\gcd(a, b)$, or simply (a, b) , is defined as the largest among the common divisors of a and b ; i.e.,

$$(a, b) = \gcd(a, b) = \max\{d : d \mid a \text{ and } d \mid b\}.$$

If $(a, b) = 1$, then a and b are called **relatively prime** or **coprime**.

More generally, the greatest common divisor of n integers a_1, \dots, a_n , not all 0, is defined as

$$(a_1, \dots, a_n) = \max\{d : d \mid a_i \text{ for } i = 1, 2, \dots, n\}.$$

Proposition 1.8 (Elementary properties of the gcd) *Let $a, b \in \mathbf{Z}$, with a and b not both 0.*

- (i) $(a, b) = (-a, b) = (a, -b) = (-a, -b)$.
- (ii) $(a, b) = (a + bn, b) = (a, b + am)$ for any $n, m \in \mathbf{Z}$.
- (iii) $(ma, mb) = m(a, b)$ for any $m \in \mathbf{N}$.
- (iv) If $d = (a, b)$, then $(a/d, b/d) = 1$.
- (v) Let $d \in \mathbf{N}$. Then $d \mid (a, b)$ holds if and only if $d \mid a$ and $d \mid b$.

Theorem 1.9 (Linear combinations and the gcd) *Let $a, b \in \mathbf{Z}$ with a and b not both 0, and let $d = (a, b)$. Then there exist $n, m \in \mathbf{Z}$ such that $d = na + mb$, i.e., d is a linear combination of a and b with integer coefficients. Moreover, the set of all such linear combinations is exactly equal to the set of integer multiples of d , and d is the least positive element of this set; i.e.,*

$$\{an + bm : n, m \in \mathbf{Z}\} = \{dq : q \in \mathbf{Z}\}$$

and

$$d = \min\{an + bm : n, m \in \mathbf{Z}, an + bm > 0\}.$$

Theorem 1.10 (Euclidean Algorithm) *Let $a, b \in \mathbf{Z}$ with $a \geq b > 0$. Set $r_0 = a$, $r_1 = b$ and define r_2, r_3, \dots, r_j by iteratively applying the division algorithm as follows, until a remainder 0 is obtained:*

$$\begin{aligned} r_0 &= r_1q_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_2 + r_3, & 0 < r_3 < r_2 \\ &\dots \\ r_{j-2} &= r_{j-1}q_{j-1} + r_j, & 0 < r_j < r_{j-1} \\ r_{j-1} &= r_jq_j. \end{aligned}$$

Then (a, b) is equal to the last non-zero remainder, i.e., $(a, b) = r_j$. Moreover, by tracing back the above chain of equations, one obtains an explicit representation of (a, b) as a linear combination of a and b .

1.4 The least common multiple

Definition (Least common multiple) Let $a, b \in \mathbf{Z}$, with a and b both nonzero. The **least common multiple (lcm)** of a and b , denoted by $[a, b]$, is defined as the smallest positive integer that is divisible by both a and b ; i.e.,

$$[a, b] = \min\{m \in \mathbf{N} : a \mid m \text{ and } b \mid m\}.$$

More generally, the least common multiple of n nonzero integers a_1, \dots, a_n is defined as

$$[a_1, \dots, a_n] = \min\{m \in \mathbf{N} : a_i \mid m \text{ for } i = 1, 2, \dots, n\}.$$

Proposition 1.11 (Elementary properties of the lcm) Let a, b be nonzero integers.

- (i) $[a, b] = [-a, b] = [a, -b] = [-a, -b]$.
- (ii) $[ma, mb] = m[a, b]$ for any $m \in \mathbf{N}$.
- (iii) $[a, b] = \frac{|ab|}{(a, b)}$.
- (iv) Let $m \in \mathbf{N}$. Then $[a, b] \mid m$ holds if and only if $a \mid m$ and $b \mid m$.

1.5 The Fundamental Theorem of Arithmetic

Lemma 1.12 (Euclid's Lemma) If $a, b \in \mathbf{Z}$, and p is a prime such that $p \mid ab$, then $p \mid a$ or $p \mid b$. More generally, if $a_1, \dots, a_n \in \mathbf{Z}$ and p is a prime such that $p \mid a_1 \cdots a_n$, then there exists an i with $1 \leq i \leq n$ such that $p \mid a_i$.

Theorem 1.13 (Fundamental Theorem of Arithmetic) Every integer greater than 1 has a unique factorization into primes; that is, every integer $n > 1$ can be represented in the form

$$n = \prod_{i=1}^r p_i^{\alpha_i},$$

where the p_i are distinct primes, and the exponents α_i are positive integers. Moreover, this representation is unique except for the ordering of the primes p_i .

Notation Given an integer $n > 1$, its prime factorization can be represented in any one of the following forms:

- (i) $n = \prod_{i=1}^s p_i$, p_1, \dots, p_s primes (not necessarily distinct);
- (ii) $n = \prod_{i=1}^r p_i^{\alpha_i}$, p_1, \dots, p_r distinct primes, $\alpha_1, \dots, \alpha_r$ positive integers;
- (iii) $n = \prod_{i=1}^t p_i^{\alpha_i}$, p_1, \dots, p_t distinct primes, $\alpha_1, \dots, \alpha_t$ nonnegative integers;
- (iv) $n = \prod_{p \text{ prime}} p^{\alpha_p}$, α_p nonnegative integers, $\alpha_p = 0$ for all but finitely many p .

In the last form, p runs through all primes, so the product is formally an infinite product. However, since $\alpha_p = 0$ for all but finitely p , all but finitely many terms of the product are 1, so the product is de facto a finite product.

The forms (iii) and (iv) are particularly useful when considering the prime factorizations of several integers, since they allow one to express all factorizations with respect to a common “basis” of primes p_i (e.g., the set of all primes that divide at least *one* of the given integers, or the set of *all* primes). As an illustration, here are some representations of the prime factorization of $n = 20$:

$$\begin{aligned} 20 &= 2 \cdot 2 \cdot 5, \\ 20 &= 2^2 \cdot 5^1, \\ 20 &= 2^2 \cdot 3^0 \cdot 5^1 \\ 20 &= 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdot 13^0 \dots \end{aligned}$$

An additional advantage of the forms (iii) and (iv) is that they allow one to represent the integer 1 (to which the Fundamental Theorem of Arithmetic does not apply) *formally* in the same form, as a product of prime powers, by taking all exponents to be 0:

$$1 = \prod_{i=1}^t p_i^0 \quad \text{or} \quad 1 = \prod_p p^0.$$

Proposition 1.14 (Divisibility, gcd, and lcm in terms of prime factorizations) *Let $a, b \in \mathbf{N}$ with prime factorizations (of the form (iii) above) given by*

$$a = \prod_{i=1}^r p_i^{\alpha_i}, \quad b = \prod_{i=1}^r p_i^{\beta_i},$$

where the p_i are distinct primes and the exponents α_i and β_i are nonnegative integers.

- (i) Then “ a divides b ” holds if and only if $\alpha_i \leq \beta_i$ for all i .
- (ii) The gcd and lcm of a and b are given by

$$(a, b) = \prod_{i=1}^r p_i^{\min(\alpha_i, \beta_i)}, \quad [a, b] = \prod_{i=1}^r p_i^{\max(\alpha_i, \beta_i)}.$$

1.6 Primes in arithmetic progressions

Definition (Arithmetic progression) A sequence of the form

$$(1.1) \quad a, a + b, a + 2b, a + 3b, \dots,$$

where a and b are integers, is called an **arithmetic progression**.

***Theorem 1.15 (Dirichlet’s Theorem on Primes in Arithmetic Progressions)** *Let $a, b \in \mathbf{N}$ with $(a, b) = 1$. Then the arithmetic progression (1.1) contains infinitely many primes.*

Chapter 2

Congruences

2.1 Definitions and basic properties; applications

Definition (Congruences) Let $a, b \in \mathbf{Z}$ and $m \in \mathbf{N}$. We say that a is **congruent to b modulo m** , and write $a \equiv b \pmod{m}$, if $m \mid a - b$ (or, equivalently, if $a = b + mx$ for some $x \in \mathbf{Z}$). The integer m is called the **modulus** of the congruence.

Proposition 2.1 (Elementary properties of congruences) Let $a, b, c, d \in \mathbf{Z}$, $m \in \mathbf{N}$.

- (i) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.
- (ii) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
- (iii) If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for any $n \in \mathbf{N}$.
- (iv) If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$ for any polynomial $f(n)$ with integer coefficients.
- (v) If $a \equiv b \pmod{m}$, then $a \equiv b \pmod{d}$ for any positive divisor d of m .

Proposition 2.2 (Congruences as equivalence relation) Let $m \in \mathbf{N}$. The congruence relation modulo m is an equivalence relation, i.e., satisfies the following properties, for any $a, b, c \in \mathbf{Z}$:

- (i) (*Reflexivity*) $a \equiv a \pmod{m}$.
- (ii) (*Symmetry*) If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
- (iii) (*Transitivity*) If $a \equiv b$ and $b \equiv c$, then $a \equiv c$.

Definition (Residue classes) Let $m \in \mathbf{N}$. The equivalence classes defined by the congruence relation modulo m are called the **residue classes modulo m** . For any $a \in \mathbf{Z}$, $[a]$ denotes the equivalence class to which a belongs, i.e.,

$$[a] = \{n \in \mathbf{Z} : n \equiv a \pmod{m}\}.$$

Definition (Complete residue system) A set of integers r_1, \dots, r_m is called a **complete residue system modulo m** , if it contains exactly one integer from each equivalence class modulo m .

Definition (Least nonnegative residue) Let $m \in \mathbf{N}$. Given any integer n , the **least nonnegative residue of n modulo m** is the unique integer r such that $n \equiv r \pmod{m}$ and $0 \leq r < m$; i.e., r is the remainder upon division of n by m by the division algorithm.

2.2 Linear congruences in one variable

Theorem 2.3 (Solutions of linear congruences in one variable) Let $a, b \in \mathbf{Z}$ and $m \in \mathbf{N}$, and consider the congruence

$$(2.1) \quad ax \equiv b \pmod{m}.$$

Let $d = (a, m)$.

- (i) *(Existence of a solution)* The congruence (2.1) has a solution $x \in \mathbf{Z}$ if and only if $d \mid b$.
- (ii) *(Number of solutions)* Suppose $d \mid b$. Then $ax \equiv b \pmod{m}$ has exactly d pairwise incongruent solutions x modulo m . The solutions are of the form $x = x_0 + km/d$, $k = 0, 1, \dots, d-1$, where x_0 is a particular solution.
- (iii) *(Construction of a solution)* Suppose $d \mid b$. Then a particular solution can be constructed as follows: Apply the Euclidean algorithm to compute $d = (a, m)$, and, working backwards, obtain a representation of d as a linear combination of a and m . Multiply the resulting equation through with (b/d) . The new equation can be interpreted as a congruence of the desired type, (2.1), and reading off the coefficient of a gives a particular solution.

Corollary Let $a \in \mathbf{Z}$ and $m \in \mathbf{N}$. If $(a, m) = 1$, the congruence

$$(2.2) \quad ax \equiv 1 \pmod{m}$$

has a unique solution x modulo m ; if $(a, m) \neq 1$, the congruence has no solution.

Definition (Modular inverses) A solution x to the congruence (2.2), if it exists, is called a **modular inverse of a** (with respect to the modulus m) and denoted by \bar{a} .

Remark Note that \bar{a} is not uniquely defined. The definition depends implicitly on the modulus m . In addition, for a given modulus m , \bar{a} is only *unique modulo m* ; i.e., any $x \in \mathbf{Z}$ with $x \equiv \bar{a} \pmod{m}$ is also a modular inverse of a .

2.3 Simultaneous linear congruences. The Chinese Remainder Theorem

Theorem 2.5 (Chinese Remainder Theorem) Let $a_1, \dots, a_r \in \mathbf{Z}$ and let $m_1, m_2, \dots, m_r \in \mathbf{N}$ be given such that $(m_i, m_j) = 1$ for $i \neq j$. Then the system

$$(2.3) \quad x \equiv a_i \pmod{m_i} \quad (i = 1, \dots, r)$$

has a unique solution x modulo $m_1 \cdots m_r$.

Corollary (Structure of residue systems modulo $m_1 \cdots m_r$) Let $m_1, \dots, m_r \in \mathbf{N}$ with $(m_i, m_j) = 1$ for $i \neq j$ be given and let $m = m_1 \cdots m_r$. There exists a 1-1 correspondence between complete systems of residues modulo m and r -tuples of complete systems of residues modulo m_1, \dots, m_r . More precisely, if, for each i , a_i runs through a complete system of residues modulo m_i , then the corresponding solution x to the simultaneous congruence (2.3) runs through a complete system of residues modulo m .

2.4 Wilson's Theorem

Theorem 2.7 (Wilson's Theorem) Let p be a prime number. Then

$$(2.4) \quad (p-1)! \equiv -1 \pmod{p}.$$

Theorem 2.8 (Converse to Wilson's Theorem) If p is an integer ≥ 2 satisfying (2.4), then p is a prime number.

Remark The converse to Wilson's Theorem can be stated in contrapositive form as follows: If n is composite, then $(n-1)!$ is **not** congruent to -1 modulo n . In fact, the following much stronger statement holds: If $n > 4$ and n is composite, then $(n-1)! \equiv 0 \pmod{n}$. Thus, for $n > 4$, $(n-1)!$ is congruent to either -1 or 0 modulo n ; the first case occurs if and only if n is prime, and the second occurs if and only if n is composite.

2.5 Fermat's Theorem

Theorem 2.9 (Fermat's Little Theorem) Let p be a prime number. Then, for any integer a satisfying $(a, p) = 1$,

$$(2.5) \quad a^{p-1} \equiv 1 \pmod{p}.$$

Corollary (Fermat's Little Theorem, Variant) Let p be a prime number. Then, for any integer a ,

$$(2.6) \quad a^p \equiv a \pmod{p}.$$

Corollary (Inverses via Fermat's Theorem) Let p be a prime number, and let a be an integer such that $(p, a) = 1$. Then $\bar{a} = a^{p-2}$ is an inverse of a modulo p .

Remark In contrast to Wilson's Theorem, Fermat's Theorem does not have a corresponding converse; in fact, there exist numbers p that satisfy the congruence in Fermat's Theorem, but which are composite. Such "false positives" to the Fermat test are rare, but they do exist, motivating the following definition:

Definition (Pseudoprimes and Carmichael numbers) An integer $p \geq 2$ that is composite, but satisfies the Fermat congruence (2.5), is called a **pseudoprime to the base a** , or **a -pseudoprime**. A 2-pseudoprime is simply called a **pseudoprime**. An integer p that is a pseudoprime to all bases $a \in \mathbf{N}$ with $(a, p) = 1$ is called a **Carmichael number**.

2.6 Euler's Theorem

Definition (Reduced residue system) Let $m \in \mathbf{N}$. A set of integers is called a **reduced residue system modulo m** , if (i) its elements are pairwise incongruent modulo m , and (ii) every integer n with $(n, m) = 1$ is congruent to an element of the set. Equivalently, a reduced residue system modulo m is the subset of a complete residue system consisting of those elements that are relatively prime with m .

Definition (Euler phi-function) Let $m \in \mathbf{N}$. The **Euler phi-function**, denoted by $\varphi(m)$, is defined by

$$\varphi(m) = \#\{1 \leq n \leq m : (n, m) = 1\},$$

i.e., $\varphi(m)$ is the number of elements in a reduced system of residues modulo m .

Proposition 2.12 *If $\{r_1, r_2, \dots, r_{\varphi(m)}\}$ is a reduced residue system modulo m , then so is the set $\{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$, for any integer a with $(a, m) = 1$.*

Theorem 2.13 (Euler's generalization of Fermat's theorem) *Let $m \in \mathbf{N}$. Then, for any integer a such that $(a, m) = 1$,*

$$(2.7) \quad a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Chapter 3

Arithmetic functions

3.1 Some notational conventions

Divisor sums and products: Let $n \in \mathbf{N}$.

- $\sum_{d|n} f(d)$ denotes a sum of $f(d)$, taken over all **positive divisors** d of n .
- $\sum_{p|n} f(p)$ denotes a sum of $f(p)$, taken over all **prime** divisors p of n .
- $\sum_{p^\alpha||n} f(p^\alpha)$ denotes a sum of $f(p^\alpha)$, taken over all **prime powers** p^α that occur in the standard prime factorization of n . (Here the double bar in $p^\alpha||n$ indicates that p^α is the exact power of p dividing n , i.e., $p^\alpha | n$, but $p^{\alpha+1} \nmid n$.)
- **Products** over $d | n$, $p | n$, etc., are defined analogously.

Empty sum/product convention: A sum over an empty set is defined to be 0; a product over an empty set is defined to be 1. Thus, for example, we have

$$\sum_{p^\alpha||1} f(p^\alpha) = 0, \quad \prod_{p^\alpha||1} f(p^\alpha) = 1,$$

since there is no prime power p^α satisfying the condition $p^\alpha||1$.

The above notational conventions greatly simplify the statements of formulas involving arithmetic functions. For example, using these conventions the rather clumsy formula

$$\varphi(n) = \begin{cases} 1 & \text{if } n = 1, \\ \prod_{i=1}^r p_i^{\alpha_i-1} (p_i - 1) & \text{if } n \geq 2 \text{ and } n = \prod_{i=1}^r p_i^{\alpha_i} \\ & \text{with distinct primes } p_i \text{ and } \alpha_i \in \mathbf{N}, \end{cases}$$

can be rewritten as

$$\varphi(n) = \prod_{p^\alpha \parallel n} p^{\alpha-1}(p-1),$$

without having to introduce subscripts or single out the case $n = 1$. (In the latter case, the product is an empty product, so by the empty product convention, it produces the value 1, which is exactly what we need.)

Sums over 1's (“Bateman summation”): A sum in which each summand is equal to 1 simply counts the number of terms in it; for example, $\sum_{d|n} 1$ is the same as $\#\{d \in \mathbf{N} : d \mid n\}$. While this might seem like a contrived way to represent a counting function, in the context of the general theory of arithmetic functions, such representations are often very useful.

3.2 Arithmetic functions: Definitions and basic examples

Function	value at $n(\in \mathbf{N})$	value at a prime p	value at a prime power p^α	properties
$\delta(n)$ (delta function)	1 if $n = 1$, 0 else	0	0	completely multiplicative, $\delta \star f = f \star \delta = f$, identity element for Dirichlet product
$\mathbf{1}(n)$ (unit function)	1	1	1	completely multiplicative
$\mathbf{i}(n)$ (identity function)	n	p	p^α	completely multiplicative
$\mu(n)$ (Moebius function)	1 if $n = 1$, $(-1)^r$ if $n = \prod_{i=1}^r p_i$ (p_i distinct), 0 otherwise	-1	-1 if $\alpha = 1$, 0 if $\alpha > 1$	multiplicative, $\mu \star \mathbf{1} = \delta$ (Dirichlet inverse of $\mathbf{1}$)
$\nu(n)$ ($= d(n) = \tau(n)$) (number-of-divisors function)	$\#\{d \in \mathbf{N} : d \mid n\}$	2	$\alpha + 1$	multiplicative, $\nu = \mathbf{1} \star \mathbf{1}$
$\varphi(n)$ (Euler phi function)	$\#\{1 \leq m \leq n : (m, n) = 1\}$	$p - 1$	$p^{\alpha-1}(p - 1)$	multiplicative, $\varphi \star \mathbf{1} = \mathbf{i}$ (Gauss identity)
$\sigma(n)$ (sum-of-divisors function)	$\sum_{d \mid n} d$	$p + 1$	$\frac{p^{\alpha+1} - 1}{p - 1}$	multiplicative, $\sigma = \mathbf{i} \star \mathbf{1}$

Table 3.1: Summary of important arithmetic functions

Definition (Multiplicative arithmetic function) A function $f : \mathbf{N} \rightarrow \mathbf{C}$ is called an **arithmetic function**. An arithmetic function f is called **multiplicative** if it satisfies the relation

$$(3.1) \quad f(n_1 n_2) = f(n_1) f(n_2)$$

whenever $((n_1, n_2) = 1)$. If (3.1) holds for **all** $n_1, n_2 \in \mathbf{N}$ (i.e., without the restriction $(n_1, n_2) = 1$), then f is called **completely multiplicative**.

Proposition 3.1 (Multiplicative functions and prime factorization) *An arithmetic function f that is not identically 0 (i.e., such that $f(n) \neq 0$ for at least one $n \in \mathbf{N}$) is multiplicative if and only if it satisfies*

$$f(n) = \prod_{p^\alpha || n} f(p^\alpha) \quad (n \in \mathbf{N}).$$

In particular, any multiplicative function f that is not identically 0 is uniquely determined by its values $f(p^\alpha)$ at prime powers and satisfies $f(1) = 1$.

3.3 The algebra of arithmetic functions

Definition (Dirichlet product of arithmetic functions) Given two arithmetic functions f and g , the **Dirichlet product (or Dirichlet convolution)** $f \star g$ is the arithmetic function defined by

$$(f \star g)(n) = \sum_{d|n} f(d)g(n/d) \quad (n \in \mathbf{N}).$$

Proposition 3.2 (Algebraic properties of Dirichlet product) *Let f, g, h be arithmetic functions.*

- (i) *(Commutativity)* $f \star g = g \star f$.
- (ii) *(Associativity)* $(f \star g) \star h = f \star (g \star h)$.
- (iii) *(Identity element)* $f \star \delta = \delta \star f = f$, where δ is defined as above, i.e., $\delta(1) = 1$ and $\delta(n) = 0$ if $n > 1$.
- (iv) *(Dirichlet inverse)* If $f(1) \neq 0$, then f has a unique Dirichlet inverse f^{*-1} , in the sense that $f \star f^{*-1} = \delta$.

Proposition 3.3 (Dirichlet product of multiplicative functions) *If f and g are multiplicative, then so is their Dirichlet product $f \star g$.*

3.4 The Moebius function and the Moebius inversion formula

Definition (Moebius function) The **Moebius function** is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^r & \text{if } n = p_1 p_2 \dots p_r \text{ with distinct primes } p_i, \\ 0 & \text{if } n \text{ is not squarefree, i.e., divisible by a prime power } p^\alpha \text{ with } \alpha > 1. \end{cases}$$

Proposition 3.4 (Properties of $\mu(n)$)

- (i) *(Multiplicativity) The Moebius function is multiplicative (though not completely multiplicative).*
- (ii) *(Inverse of the unit function) The function μ is the Dirichlet product inverse of the function $\mathbf{1}$: $\mu \star \mathbf{1} = \mathbf{1} \star \mu = \delta$; explicitly,*

$$\sum_{d|n} \mu(d) = \sum_{d|n} \mu(n/d) = \delta(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 3.5 (Moebius inversion formula) *If f and g are arithmetic functions related by $f = g \star \mathbf{1}$, then $g = f \star \mu = \mu \star f$; explicitly, if*

$$f(n) = \sum_{d|n} g(d) \quad (n \in \mathbf{N}),$$

then

$$g(n) = \sum_{d|n} f(d) \mu(n/d) = \sum_{d|n} \mu(d) f(n/d) \quad (n \in \mathbf{N}).$$

3.5 The Euler phi function. The Carmichael conjecture

Definition (Euler phi function) The Euler phi function is defined by

$$\varphi(n) = \#\{1 \leq m \leq n : (m, n) = 1\}.$$

Proposition 3.6 (Properties of $\varphi(n)$)

- (i) *(Multiplicativity) The Euler phi function is multiplicative (though not completely multiplicative).*
- (ii) *(Explicit formula) For any $n \in \mathbf{N}$,*

$$\varphi(n) = \prod_{p^\alpha || n} p^{\alpha-1} (p-1) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

(iii) (*Gauss identity*) $\varphi \star 1 = \mathbf{i}$; explicitly,

$$\sum_{d|n} \varphi(d) = n \quad (n \in \mathbf{N}).$$

Conjecture (Carmichael conjecture) Given $n \in \mathbf{N}$, the equation $\varphi(x) = n$ has either no solution $x \in \mathbf{N}$ or more than one solution.

Remark The Carmichael conjecture has several local (UIUC) connections: Its originator, R.D. Carmichael, spent most of his career as a professor here at the U of I, and the conjecture first appeared as an “exercise” in a textbook on number theory he wrote (and which he presumably assigned to his students). Also, most of the current records on this conjecture are held by Kevin Ford, who earned his PhD here in the mid 1990s and is now back as a professor. In particular, Ford showed the following:

- (i) The Carmichael conjecture is true for all $n \leq 10^{1000000000}$.
- (ii) For any $k \in \mathbf{N}$ except possibly $k = 1$, there exist infinitely many $n \in \mathbf{N}$ such that the equation $\varphi(x) = n$ has exactly k solutions $x \in \mathbf{N}$. Thus, only the question of whether multiplicity $k = 1$ can occur remains open, and this is precisely the question addressed by the Carmichael conjecture.

3.6 The number-of-divisors and sum-of-divisors functions. Perfect numbers

Definition (Number-of-divisors function) The **number-of-divisors function** is defined by

$$\nu(n) = \#\{d \in \mathbf{N} : d \mid n\} = \sum_{d|n} 1 = (\mathbf{1} \star \mathbf{1})(n) \quad (n \in \mathbf{N}).$$

This function is often simply called the **divisor function**; alternate, and more common, notations for it are $d(n)$ (for “**divisor**”) and $\tau(n)$ (for “**Teiler**”, the German word for “divisor”).

Proposition 3.7 (Properties of $\nu(n)$)

- (i) (*Multiplicativity*) The function $\nu(n)$ is multiplicative (though not completely multiplicative).
- (ii) (*Explicit formula*) For any $n \in \mathbf{N}$,

$$\nu(n) = \prod_{p^\alpha \parallel n} (\alpha + 1)$$

Definition Sum-of-divisors function The **sum-of-divisors function** is defined by

$$\sigma(n) = \sum_{d|n} d = (\mathbf{i} \star \mathbf{1})(n) \quad (n \in \mathbf{N}).$$

Proposition 3.8 (Properties of $\sigma(n)$)

- (i) (Multiplicativity) The function $\nu(n)$ is multiplicative (though not completely multiplicative).
- (ii) (Explicit formula) For any $n \in \mathbf{N}$,

$$\sigma(n) = \prod_{p^\alpha || n} \frac{p^\alpha - 1}{p - 1}$$

Definition (Perfect numbers) An positive integer n is called **perfect** if it is equal to the sum of its positive divisors $d | n$, with $1 \leq d < n$ (i.e., not counting $d = n$). Equivalently, n is perfect if and only if $\sigma(n) = 2n$.

Example 1 The first 4 perfect numbers are $6(= 1 + 2 + 3)$, $28(= 1 + 2 + 4 + 7 + 14)$, 496, and 8128.

Theorem 3.9 (Characterization of even perfect numbers) An even positive integer n is perfect if and only if it is of the form

$$n = 2^{p-1}(2^p - 1),$$

where $2^p - 1$ is a Mersenne prime.

Corollary There exist infinitely many even perfect numbers if and only if there exist infinitely many Mersenne primes.

Example 2 The above four perfect numbers 6, 28, 496, 8128 correspond to the first four Mersenne primes, $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, and $2^7 - 1 = 127$.

Chapter 4

Quadratic residues

4.1 Quadratic residues and nonresidues

Definition (Quadratic residues and nonresidues) Let $m \in \mathbf{N}$ and $a \in \mathbf{Z}$ be such that $(a, m) = 1$. Then a is called a **quadratic residue modulo m** if the congruence

$$(4.1) \quad x^2 \equiv a \pmod{m}$$

has a solution (i.e., if a is a “perfect square modulo m ”), and a is called a **quadratic nonresidue modulo m** if (4.1) has no solution.

Remarks (i) Note that, by definition, integers a that do not satisfy the condition $(a, m) = 1$ are not classified as quadratic residues or nonresidues. In particular, 0 is considered neither a quadratic residue nor a quadratic nonresidue (even though, for $a = 0$, (4.1) has a solution, namely $x = 0$).

(ii) While the definition of quadratic residues and nonresidues allows the modulus m to be an arbitrary positive integer, in the following we will focus exclusively on the case when m is an *odd prime* p .

Proposition 4.1 (Number of solutions to quadratic congruences) Let p be an odd prime, and let $a \in \mathbf{Z}$ with $(a, p) = 1$.

- (i) If a is a quadratic nonresidue modulo p , the congruence (4.1) has no solution.
- (ii) If a is a quadratic residue modulo p , the congruence (4.1) has exactly two incongruent solutions x modulo p . More precisely, if x_0 is one solution, then a second, incongruent, solution is given by $p - x_0$.

Proposition 4.2 (Number of quadratic residues and nonresidues) Let p be an odd prime. Then among the integers $1, 2, \dots, p - 1$, exactly half (i.e., $(p - 1)/2$) are quadratic residues modulo p , and exactly half are quadratic nonresidues modulo p .

4.2 The Legendre symbol

Definition (Legendre symbol) Let p be an odd prime, and let a be an integer with $(a, p) = 1$ (or, equivalently, $p \nmid a$). The **Legendre symbol of a modulo p** , denoted by $\left(\frac{a}{p}\right)$, is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a nonquadratic residue modulo } p. \end{cases}$$

Remark Note that the modulus in this definition, and in all results below, is restricted to odd primes (i.e., a prime other than 2). One can extend the definition, and most of the results, to composite moduli, but things get a lot more complicated then.

Proposition 4.3 (Properties of the Legendre Symbol) Let p be an odd prime, and let $a, b \in \mathbf{Z}$ with $(a, p) = 1$ and $(b, p) = 1$.

- (i) (Periodicity in numerator) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
- (ii) (Complete multiplicativity in numerator) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.
- (iii) (Value at squares) $\left(\frac{a^2}{p}\right) = 1$.
- (iv) (Value at -1)

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$
- (v) (Value at 2)

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

Proposition 4.4 (Euler's Criterion) Let p be an odd prime, and let $a \in \mathbf{Z}$ with $(a, p) = 1$. Then a is a quadratic residue modulo p if $a^{(p-1)/2} \equiv 1 \pmod{p}$, and a quadratic nonresidue if $a^{(p-1)/2} \equiv -1 \pmod{p}$; equivalently,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Proposition 4.5 (Gauss's Lemma) Let p be an odd prime, and let $a \in \mathbf{Z}$ with $(a, p) = 1$. Consider the $(p-1)/2$ integers $a, 2a, \dots, ((p-1)/2)a$. Reduce each of these integers modulo p , obtaining $(p-1)/2$ integers, all in the interval $(0, p)$. Let n be the number among those latter integers that are greater than $p/2$ (i.e., which fall in the top half of the interval $(0, p)$). Then a is a quadratic residue modulo p if n is even, and a quadratic nonresidue if n is odd; equivalently,

$$\left(\frac{a}{p}\right) = (-1)^n = \begin{cases} 1 & \text{if } n \text{ is even,} \\ -1 & \text{if } n \text{ is odd.} \end{cases}$$

4.3 The law of quadratic reciprocity

Theorem 4.6 (Quadratic reciprocity law (Gauss 1795)) *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Equivalently,

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4}, \\ \left(\frac{q}{p}\right) & \text{otherwise.} \end{cases}$$

Remarks (i) The first form of the reciprocity law is the cleaner and more elegant form, and the one in which the law is usually stated. However, for applications, the second form is more useful. In this form the law says that numerator and denominator in a Legendre symbol (assuming both are distinct odd primes) can be interchanged in all cases except when both numerator and denominator are congruent to 3 modulo 4, in which case the sign of the Legendre symbol flips after interchanging numerator and denominator. Put differently, this form states that p is a quadratic residue modulo q if and only if q is a quadratic residue modulo p , except in the case when both p and q are congruent to 3 modulo 4; in the latter case p is a quadratic residue modulo q if and only if q is a quadratic nonresidue modulo p .

(ii) Note that the reciprocity law requires numerator and denominator to be distinct odd primes. In particular, it does not apply directly to cases where the numerator is composite, negative, or an even number. However, these cases can be reduced to the prime case using the multiplicativity of the Legendre symbol along with the special values at -1 and 2 (see Proposition 4.3):

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

and

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

In fact, these last two relations are called the **First Supplementary Law** and **Second Supplementary Law**, as they “supplement” the quadratic reciprocity law.

(iii) Repeated application of the quadratic reciprocity law, along with the periodicity and multiplicativity properties of the Legendre symbol, allows one to quickly and efficiently compute Legendre symbols, even if the numbers involved are very large. The resulting algorithm is reminiscent of the gcd algorithm.

Chapter 5

Primitive roots

5.1 The order of an integer

Definition (Order of an integer) Let $m \in \mathbf{N}$ and $a \in \mathbf{Z}$ be such that $(a, m) = 1$. The **order of a modulo m** , denoted by $\text{ord}_m a$, is the least positive integer k such that

$$(5.1) \quad a^k \equiv 1 \pmod{m}.$$

In order for this definition to make sense, there has to be at least one positive integer k for which (5.1) holds. The existence of such a k is guaranteed by Euler's Theorem (Theorem 2.13), which states that, under the same assumptions on m and a as in the definition, (5.1) holds for $k = \varphi(m)$. Thus, the order $\text{ord}_m a$ is well-defined, and it is at most equal to $\varphi(m)$.

Proposition 5.1 (Properties of an order) Let $m \in \mathbf{N}$ and $a \in \mathbf{Z}$ be such that $(a, m) = 1$, and let $\text{ord}_m a$ be the order of a modulo m . Then:

- (i) (Periodicity) If $b \equiv a \pmod{m}$, then $\text{ord}_m b = \text{ord}_m a$.
- (ii) (Relation to Euler phi) $\text{ord}_m a$ is a divisor of $\varphi(m)$.
- (iii) (Characterization of "good" exponents) The set of positive integers k for which the congruence (5.1) holds consists exactly of the positive integer multiples of $\text{ord}_m a$.
- (iv) (Order of powers of a) For any positive integer i ,

$$\text{ord}_m a^i = \frac{\text{ord}_m a}{(\text{ord}_m a, i)}.$$

In particular, $\text{ord}_m a^i = \text{ord}_m a$ if and only if $(\text{ord}_m a, i) = 1$.

Proposition 5.2 (Number of elements of given order) Let p be an odd prime. Then the possible orders of integers modulo p are exactly the positive divisors of $p - 1 (= \varphi(p))$. Moreover, given any positive divisor $d \mid p - 1$, there exist exactly $\varphi(d)$ incongruent integers a with $\text{ord}_p a = d$.

5.2 Primitive roots

The question when the order of an integer a modulo m is equal to its maximal possible value, the “Euler order” $\varphi(m)$, motivates the following definition.

Definition (Primitive root) Let $m \in \mathbf{N}$ and $a \in \mathbf{Z}$ be such that $(a, m) = 1$. Then a is called a **primitive root modulo m** if $\text{ord}_m a = \varphi(m)$, i.e., if the order of a is equal to the maximal possible value.

Proposition 5.3 (Primitive roots and reduced systems of residues) Let $m \in \mathbf{N}$, and suppose r is a primitive root modulo m . Then the set

$$\{r, r^2, \dots, r^{\varphi(m)}\}$$

is a system of reduced residues modulo m . That is, the elements in this set are pairwise incongruent modulo m , and every integer a with $(a, m) = 1$ is congruent modulo m to an element in the above set.

5.3 The Primitive Root Theorem

Theorem 5.4 (Existence of Primitive Roots) Let m be a positive integer. Then there exists a primitive root modulo m if and only if m has one of the following forms:

- (i) $m = p^\alpha$, where p is an odd prime and $\alpha \in \mathbf{N}$.
- (ii) $m = 2p^\alpha$, where p is an odd prime and $\alpha \in \mathbf{N}$.
- (iii) $m = 1, 2, 4$.

Theorem 5.5 (Number of primitive roots) Let m be of one of the forms in the Primitive Root Theorem, so that there exists at least one primitive root modulo m . Then there exist exactly $\varphi(\varphi(m))$ incongruent primitive roots modulo m .

Chapter 6

Continued fractions

6.1 Definitions and notations

Definition (Continued fractions) A finite or infinite expression of the form

$$(6.1) \quad a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}},$$

where the a_i are real numbers, with $a_1, a_2, \dots > 0$, is called a **continued fraction** (c.f.). The numbers a_i are called the **partial quotients** of the c.f.

The continued fraction (6.1) is called **simple** if the partial quotients a_i are all integers. It is called **finite** if it terminates, i.e., if it is of the form

$$(6.2) \quad a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_n}}},$$

and **infinite** otherwise.

Notation (Bracket notation for continued fractions) The continued fractions (6.1) and (6.2) are denoted by $[a_0, a_1, a_2, \dots]$ and $[a_0, a_1, a_2, \dots, a_n]$, respectively. In particular,

$$[a_0] = a_0, \quad [a_0, a_1] = a_0 + \frac{1}{a_1}, \quad [a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}}, \quad \dots$$

Remarks (i) Note that the first term, a_0 , is allowed to be negative or 0, but all subsequent terms a_i must be positive. This requirement ensures that there are no zero denominators and that any finite c.f. (6.2), and all of its convergents, are well-defined.

(ii) In the sequel we will almost exclusively focus on the case of simple c.f.'s, i.e., c.f.'s where all partial quotients are integers. There one important exception are c.f.'s of the

form $[a_0, a_1, \dots, a_n, x]$, where a_0, a_1, \dots, a_n are integers (with a_i positive for $i \geq 1$), but the final partial quotient, x , can be any positive real number.

Definition (Convergents) Let $\alpha = [a_0, a_1, \dots]$ be a finite or infinite c.f. Then the i -th convergent of α is defined as the c.f.

$$C_i = [a_0, a_1, \dots, a_i].$$

Definition (Convergence of infinite continued fractions) An infinite c.f. $[a_0, a_1, \dots]$ is called **convergent** if its sequence of convergents converges in the usual sense, i.e., if the limit $\lim_{i \rightarrow \infty} C_i$ exists and is equal to some real number α . In this case, we say that the continued fraction $[a_0, a_1, a_2, \dots]$ **represents** the number α , or is a **continued fraction expansion** of α , and we write

$$\alpha = [a_0, a_1, a_2, \dots].$$

Theorem 6.1 (Convergence of infinite simple c.f.'s) *Any infinite simple c.f. $[a_0, a_1, \dots]$ is convergent.*

6.2 Expansions of real numbers into continued fractions

Proposition 6.2 (Continued fraction algorithm) *Given a real number α , define successively real numbers $\alpha_0, \alpha_1, \dots$, and integers a_0, a_1, \dots by*

$$\begin{aligned} \alpha_0 &= \alpha, & a_0 &= [\alpha_0], \\ \alpha_1 &= \frac{1}{\alpha_0 - [\alpha_0]}, & a_1 &= [\alpha_1], \\ \alpha_2 &= \frac{1}{\alpha_1 - [\alpha_1]}, & a_2 &= [\alpha_2], \\ &\dots & &\dots \end{aligned}$$

where $[x]$ denotes the integer part of x (i.e., the “floor function”). Stop the algorithm if α_n is an integer (and thus $a_n = \alpha_n$); otherwise continue indefinitely. Then $[a_0, a_1, \dots]$ is a simple c.f. that represents the number α . Moreover, for any $i \geq 0$ we have

$$\alpha_i = [a_i, a_{i+1}, \dots], \quad \alpha = [a_0, a_1, \dots, a_{i-1}, \alpha_i].$$

Theorem 6.3 (Continued fraction expansion of rational numbers) *Any finite simple c.f. represents a rational number. Conversely, any rational number α can be expressed as a simple finite c.f. $\alpha = [a_0, a_1, \dots, a_n]$. Moreover, under the requirement that $a_n > 1$, this representation is unique. Thus, there is a one-to-one correspondence between rational numbers and finite simple c.f.'s with last partial quotient greater than 1.*

Theorem 6.4 (Continued fraction expansion of irrational numbers) *Any infinite simple c.f. represents an irrational number. Conversely, any irrational number α can be expressed as a simple infinite c.f. $\alpha = [a_0, a_1, a_2, \dots]$, and this representation is unique. Thus, there is a one-to-one correspondence between irrational numbers and infinite simple c.f.'s.*

Theorem 6.5 (Continued fraction expansion of quadratic irrationals) *The c.f. expansion of a quadratic irrational (i.e., a solution of a quadratic equation with integer coefficients) is eventually periodic, i.e., of the form*

$$[a_0, \dots, a_N, \overline{a_{N+1}, \dots, a_{N+p}}],$$

where the bar indicates the periodic part. Conversely, any infinite simple c.f. that is eventually periodic represents a quadratic irrational. Thus, there is a one-to-one correspondence between quadratic irrationals and infinite, eventually periodic simple c.f.'s.

6.3 Convergents

Proposition 6.6 (Algorithm for convergents) *Let $\alpha = [a_0, a_1, \dots]$ be a simple c.f. The i -th convergent to α , $C_i = [a_0, a_1, \dots, a_i]$, is given by $C_i = p_i/q_i$ for $i \geq 0$, where p_i and q_i are integers defined recursively by*

$$(6.3) \quad \begin{cases} p_{-1} = 1, & q_{-1} = 0, \\ p_0 = a_0, & q_0 = 1, \\ p_i = a_i p_{i-1} + p_{i-2}, & q_i = a_i q_{i-1} + q_{i-2} \quad (i \geq 1). \end{cases}$$

Remarks (i) Note that the values $(p_{-1}, q_{-1}) = (1, 0)$ have no natural interpretation in terms of convergents; there is no convergent C_{-1} corresponding to index $i = -1$, and the fraction p_{-1}/q_{-1} is not defined. However, these values are needed (along with the values $(p_0, q_0) = (a_0, 1)$) to get the recursive definition started.

(ii) The equations for q_i are the same as those for p_i , except for different initial values: the p_i 's start out with 1 and a_0 at $i = -1, 0$, while the q_i 's start out with 0 and 1.

Theorem 6.7 (Properties of convergents) *The convergents $C_i = p_i/q_i$, (with p_i and q_i defined by (6.3)) of an infinite simple continued fraction $\alpha = [a_0, a_1, a_2, \dots]$ satisfy:*

- (i) $(p_i, q_i) = 1$ for $i = 0, 1, \dots$; i.e., the fractions p_i/q_i are reduced.
- (ii) $q_1 < q_2 < \dots$; i.e., for $i \geq 1$, the denominators q_i are strictly increasing.
- (iii) $C_0 < C_2 < C_4 < \dots < \alpha < \dots < C_5 < C_3 < C_1$. That is, the even-indexed convergents form an increasing sequence, while the odd-indexed convergents form a decreasing sequence, with the value of the c.f. sandwiched between both sequences.
- (iv) $|C_i - C_{i+1}| = 1/(q_i q_{i+1})$ for $i = 0, 1, 2, \dots$. That is, the difference between two consecutive convergents is equal to the reciprocal of the product of the two denominators.

6.4 Rational approximations

Theorem 6.8 (Approximation of irrational numbers by rationals) *Let α be an irrational number, and let p_i/q_i be the convergents to the simple c.f. fraction expansion of α .*

(i) Any convergent p_i/q_i satisfies

$$\left| \frac{p_i}{q_i} - \alpha \right| < \frac{1}{q_i q_{i+1}} < \frac{1}{q_i^2}.$$

(ii) Conversely, any rational number a/b with $a \in \mathbf{Z}$, $b \in \mathbf{N}$, $(a, b) = 1$, that satisfies

$$\left| \frac{a}{b} - \alpha \right| < \frac{1}{2b^2},$$

is a convergent to α , i.e., $a/b = p_i/q_i$ for some i .

(iii) Among all rational numbers with denominator $\leq q_i$, the convergent p_i/q_i is the best-possible approximation to α ; i.e., for any rational number a/b with $a \in \mathbf{Z}$, $b \in \mathbf{N}$, and $1 \leq b \leq q_i$,

$$\left| \frac{p_i}{q_i} - \alpha \right| \leq \left| \frac{a}{b} - \alpha \right|,$$

with equality if and only if $a/b = p_i/q_i$.