

Math 453: Elementary Number Theory
Definitions and Theorems

Version 3/23/2008

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 are 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.*