Introduction to Analytic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Induction and Well-Ordering

The Principle of Induction

- Many of our proofs make use of the following property of integers.

The Principle of Induction

If Q is a set of integers such that:

(a) $1 \in Q$;

(b) $n \in Q$ implies $n + 1 \in Q$,

then

(c) all integers ≥ 1 belong to Q.

- There are alternate formulations of this principle.
  - In Statement (a), the integer 1 can be replaced by any integer k, provided that the inequality ≥ 1 is replaced by $\geq k$ in (c).
  - (b) can be replaced by $1, 2, 3, \ldots, n \in Q$ implies $(n + 1) \in Q$.

The Well-Ordering Principle

- We also assume familiarity with the following principle, which is logically equivalent to the principle of induction.

The Well-Ordering Principle

If A is a nonempty set of positive integers, then A contains a smallest member.

- This principle has also equivalent formulations:
  - "positive integers" can be replaced by "integers $\geq k$ for some k".

Subsection 2

Divisibility

Divisibility

- Small latin letters a, b, c, d, n, etc., denote integers, positive, negative, or zero.

Definition of Divisibility

We say d **divides** n and we write $d \mid n$ whenever $n = cd$, for some c.
We also say that n is a **multiple** of d, that d is a **divisor** of n, or that d is a **factor** of n.
If d does not divide n, we write $d \nmid n$.

Properties of Divisibility

Theorem

Divisibility has the following properties:

(a) $n \mid n$; (**Reflexive Property**)

(b) $d \mid n$ and $n \mid m$ implies $d \mid m$; (**Transitive Property**)

(c) $d \mid n$ and $d \mid m$ implies $d \mid (an + bm)$; (**Linearity Property**)

(d) $d \mid n$ implies $ad \mid an$; (**Multiplication Property**)

(e) $ad \mid an$ and $a \neq 0$ implies $d \mid n$; (**Cancelation Law**)

(f) $1 \mid n$; (1 divides every integer)

(g) $n \mid 0$; (every integer divides zero)

(h) $0 \mid n$ implies $n = 0$; (zero divides only zero)

(i) $d \mid n$ and $n \neq 0$ implies $|d| \leq |n|$; (**Comparison Property**)

(j) $d \mid n$ and $n \mid d$ implies $|d| = |n|$;

(k) $d \mid n$ and $d \neq 0$ implies $(n/d) \mid n$.

Proof of the Properties of Divisibility ((a)-(d))

(a) $n \mid n$.

Since $n = 1 \cdot n$, we get $n \mid n$.

(b) $d \mid n$ and $n \mid m$ implies $d \mid m$.

$d \mid n$ implies there exists c_1, such that $n = c_1 d$. $n \mid m$ implies there exists c_2, such that $m = c_2 n$. Thus, we obtain $m = c_2 n = (c_2 c_1) d$. Hence $d \mid m$.

(c) $d \mid n$ and $d \mid m$ implies $d \mid (an + bm)$.

$d \mid n$ implies there exists c_1 such that $n = c_1 d$. $d \mid m$ implies there exists c_2 such that $m = c_2 d$. Now we get $an + bm = ac_1 d + bc_2 d = (ac_1 + bc_2) d$. Thus, $d \mid (an + bm)$.

(d) $d \mid n$ implies $ad \mid an$.

$d \mid n$ implies there exists c such that $n = cd$. Thus, $an = cad$. So $ad \mid an$.

Proof of the Properties of Divisibility ((e)-(i))

(e) $ad \mid an$ and $a \neq 0$ implies $d \mid n$.

$ad \mid an$ implies there exists c such that $an = cad$. Since $a \neq 0$, we get $n = cd$. Thus, $d \mid n$.

(f) $1 \mid n$.

Since $n = n \cdot 1$, we get $1 \mid n$.

(g) $n \mid 0$.

Since $0 = 0 \cdot n$ we get $n \mid 0$.

(h) $0 \mid n$ implies $n = 0$.

Since $0 \mid n$ there exists c such that $n = c \cdot 0 = 0$.

(i) $d \mid n$ and $n \neq 0$ implies $|d| \leq |n|$.

$d \mid n$ and $n \neq 0$ imply that there exists $c \neq 0$, such that $n = cd$. Therefore, $|n| = |cd| = |c||d| \geq |d|$.

Proof of the Properties of Divisibility ((j)-(k))

(j) $d \mid n$ and $n \mid d$ implies $|d| = |n|$.

If $n = 0$, then $d = 0$ and $|d| = |n|$.

So suppose that $n \neq 0$. $d \mid n$ implies there exists c_1 such that $n = c_1 d$. $n \mid d$ implies there exists c_2 such that $d = c_2 n$. So we get $n = c_1 d = c_1 c_2 n$. Since $n \neq 0$, $c_1 c_2 = 1$. Since c_1, c_2 are integers, we must have $|c_1| = |c_2| = 1$. Now we obtain $|d| = |c_2 n| = |c_2||n| = |n|$.

(k) $d \mid n$ and $d \neq 0$ implies $(n/d) \mid n$.

$d \mid n$ implies there exists c, such that $n = cd$. Since $d \neq 0$, we get $c = \frac{n}{d}$, an integer. Therefore, $n = dc = d \cdot \frac{n}{d}$. Thus, $\frac{n}{d} \mid n$.

Note: If $d \mid n$, then n/d is called the **divisor conjugate to** d.

Subsection 3

Greatest Common Divisor

Existence of Greatest Common Divisor

- If d divides two integers a and b, then d is called a **common divisor** of a and b.
- Thus, 1 is a common divisor of every pair of integers a and b.

Theorem

Given any two integers a and b, there is a common divisor d of a and b of the form

$$d = ax + by,$$

where x and y are integers. Moreover, every common divisor of a and b divides this d.

- First we assume that $a \geq 0$ and $b \geq 0$.

  We use induction on n, where $n = a + b$.

  If $n = 0$, then $a = b = 0$.

  Then we can take $d = 0$, with $x = y = 0$.

Existence of Greatest Common Divisor (Cont'd)

- Assume that the theorem has been proved for $0, 1, 2, \ldots, n-1$.

  By symmetry, we can assume $a \geq b$.

  If $b = 0$ take $d = a$, $x = 1$, $y = 0$.

  If $b \geq 1$, apply the theorem to $a - b$ and b.

  Now $(a-b) + b = a = n - b \leq n - 1$.

  So the induction assumption is applicable.

  Thus, there is a common divisor d of $a - b$ and b of the form

  $$d = (a-b)x + by.$$

  This d also divides $(a-b) + b = a$.

  So d is a common divisor of a and b.

  Moreover, $d = ax + (y-x)b$, a linear combination of a and b.

Existence of Greatest Common Divisor (Cont'd)

- Finally, we need to show that every common divisor divides d.

  But a common divisor divides a and b.

  Hence, by linearity, it divides d.

  If $a < 0$ or $b < 0$, we apply the result just proved to $|a|$ and $|b|$.

  Then there is a common divisor d of $|a|$ and $|b|$ of the form

$$d = |a|x + |b|y.$$

  If $a < 0$, $|a|x = -ax = a(-x)$.

  Similarly, if $b < 0$, $|b|y = b(-y)$.

  Hence d is again a linear combination of a and b.

Uniqueness of the Greatest Common Divisor

Theorem

Given integers a and b, there is one and only one number d with the following properties:

(a) $d \geq 0$ (d is nonnegative);

(b) $d \mid a$ and $d \mid b$ (d is a common divisor of a and b);

(c) $e \mid a$ and $e \mid b$ implies $e \mid d$ (every common divisor divides d).

- By the preceding theorem, there is at least one d satisfying Conditions (b) and (c). Also, $-d$ satisfies these conditions.

  But if d' satisfies (b) and (c), then $d \mid d'$ and $d' \mid d$. So $|d| = |d'|$. Hence there is exactly one $d \geq 0$ satisfying (b) and (c).

- In the theorem, $d = 0$ if, and only if, $a = b = 0$.

  Otherwise $d \geq 1$.

The Greatest Common Divisor

Definition

The number d of the preceding theorem is called the **greatest common divisor** (**gcd**) of a and b. It is denoted by (a, b).
If $(a, b) = 1$ then a and b are said to be **relatively prime**.

Theorem

The gcd has the following properties:

(a) $(a, b) = (b, a)$ (**commutative law**)

(b) $(a, (b, c)) = ((a, b), c)$ (**associative law**)

(c) $(ac, bc) = |c|(a, b)$ (**distributive law**)

(d) $(a, 1) = (1, a) = 1$, $(a, 0) = (0, a) = |a|$.

(a) By definition, $(a, b) \mid a$ and $(a, b) \mid b$.
So, we get $(a, b) \mid (b, a)$. By symmetry, $(b, a) \mid (a, b)$.
Since they are both nonegative, $(a, b) = (b, a)$.

The Greatest Common Divisor (Cont'd)

(b) By definition $(a,(b,c)) \mid a$ and $(a,(b,c)) \mid (b,c)$. Since $(b,c) \mid b$ and $(b,c) \mid c$, we get $(a,(b,c)) \mid a$, $(a,(b,c)) \mid b$ and $(a,(b,c)) \mid c$. Thus, $(a,(b,c)) \mid (a,b)$ and $(a,(b,c)) \mid c$. We conclude $(a,(b,c)) \mid ((a,b),c)$. By symmetry, $((a,b),c) \mid (a,(b,c))$. Since both are nonnegative, it follows that $((a,b),c) = (a,(b,c))$.

(c) There exist x, y, such that $(a,b) = ax + by$. So $c(a,b) = c(ax+by) = x(ca) + y(cb)$. From this equation, we get:

- $c(a,b) \mid (ca,cb)$, since $c(a,b) \mid ca$ and $c(a,b) \mid cb$.
- $(ca,cb) \mid c(a,b)$.

Thus, $|(ca,cb)| = |c(a,b)|$. Equivalently, $(ca,cb) = |c|(a,b)$.

(d) Since $1 \mid 1$ and $1 \mid a$, we get $1 \mid (1,a)$. But $(a,1) \mid 1$. Since both are nonnegative, $(a,1) = 1$.

We have $|a| \mid a$ and $|a| \mid 0$. Thus, $|a| \mid (a,0)$. But $(a,0) \mid a \mid |a|$. Thus, $(a,0) = |a|$.

Euclid's Lemma

Theorem (Euclid's Lemma)

If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

- Since $(a, b) = 1$ we can write

  $$1 = ax + by.$$

  Therefore,

  $$c = acx + bcy.$$

  But $a \mid acx$ and $a \mid bcy$.

  So $a \mid c$.

Subsection 4

Prime Numbers

Prime Numbers

Definition

An integer n is called **prime** if $n > 1$ and if the only positive divisors of n are 1 and n.

If $n > 1$ and if n is not prime, then n is called **composite**.

Examples: The prime numbers less than 100 are

$$\begin{array}{l} 2, 3, 5, 7, 11, 13, 17, 19, 23, \\ 29, 31, 37, 41, 43, 47, 53, 59, \\ 61, 67, 71, 73, 79, 83, 89, 97. \end{array}$$

Notation: Prime numbers are usually denoted by p, p', p_i, q, q', q_i.

Prime Number Decomposition

Theorem

Every integer $n > 1$ is either a prime number or a product of prime numbers.

- We use induction on n.

  The theorem is clearly true for $n = 2$.

  Assume it is true for every integer $< n$.

  Then if n is not prime, it has a positive divisor $d \neq 1$, $d \neq n$.

  Hence $n = cd$, where $c \neq n$.

  But both c and d are $< n$ and > 1.

  So each of c, d is a product of prime numbers.

  It follows that n is also a product of prime numbers.

Euclid's Theorem on the Infinity of Primes

Theorem (Euclid)

There are infinitely many prime numbers.

Euclid's Proof: Suppose there are only a finite number, say $p_1, p_2, \ldots, p_n$. Let

$$N = 1 + p_1 p_2 \cdots p_n.$$

Since $N > 1$ either N is prime or N is a product of primes.

Of course N is not prime since it exceeds each p_i.

Moreover, no p_i divides N.

If $p_i \mid N$, then p_i divides the difference $N - p_1 p_2 \cdots p_n = 1$.

This contradicts the prime decomposition theorem.

Non-Divisibility and Divisibility by a Prime

Theorem

If a prime p does not divide a, then $(p, a) = 1$.

- Let $d = (p, a)$. Then $d \mid p$. So $d = 1$ or $d = p$. But $d \mid a$. So $d \neq p$, because $p \nmid a$. Hence $d = 1$.

Theorem

If a prime p divides ab, then $p \mid a$ or $p \mid b$. More generally, if a prime p divides a product $a_1 \cdots a_n$, then p divides at least one of the factors.

- Assume $p \mid ab$ and that $p \nmid a$. We shall prove that $p \mid b$. By the preceding theorem, $(p, a) = 1$. So, by Euclid's Lemma, $p \mid b$.

  To prove the more general statement we use induction on n, the number of factors.

Subsection 5

The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every integer $n > 1$ can be represented as a product of prime factors in only one way, apart from the order of the factors.

- We use induction on n.
  The theorem is true for $n = 2$.
  Assume, then, that it is true for all integers greater than 1 and less than n. We shall prove it is also true for n.
  If n is prime there is nothing more to prove.
  Assume n is composite and has two factorizations, say

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t.$$

  We wish to show that $s = t$ and that each p equals some q.
  Since p_1 divides $q_1 q_2 \cdots q_t$, it must divide at least one factor.
  Relabel $q_1, q_2, \ldots, q_t$, so that $p_1 \mid q_1$.
  Then $p_1 = q_1$, since both p_1 and q_1 are primes.

The Fundamental Theorem of Arithmetic (Cont'd)

- In $p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ we may cancel p_1 on both sides to obtain

$$\frac{n}{p_1} = p_2 \cdots p_s = q_2 \cdots q_t.$$

If $s > 1$ or $t > 1$, then $1 < \frac{n}{p_1} < n$.

The induction hypothesis tells us that the two factorizations of $\frac{n}{p_1}$ must be identical, apart from the order of the factors.

Therefore,

$$s = t$$

and the factorizations of n are also identical, apart from order.

Factorization Into Prime Powers

- In the factorization of an integer n, a particular prime p may occur more than once.
- Suppose the distinct prime factors of n are $p_1, \ldots, p_r$.
- Suppose that p_i occurs as a factor a_i times.
- Then we can write

$$n = p_1^{a_1} \cdots p_r^{a_r}$$

  or, more briefly,

$$n = \prod_{i=1}^{r} p_i^{a_i}.$$

- This is called the **factorization of n into prime powers**.
- We can also express 1 in this form by taking each exponent a_i to be 0.

Prime Factorization and Set of Divisors

Theorem

If $n = \prod_{i=1}^{r} p_i^{a_i}$, the set of positive divisors of n is the set of numbers of the form $\prod_{i=1}^{r} p_i^{c_i}$, where $0 \leq c_i \leq a_i$, for $i = 1, 2, \ldots, r$.

- The proof of the nontrivial direction is similar to that of the Fundamental Theorem.
- Suppose we label the primes in increasing order $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ..., $p_n =$ the n-th prime.
- Then every positive integer n (including 1) can be expressed in the form $n = \prod_{i=1}^{\infty} p_i^{a_i}$, where now each exponent $a_i \geq 0$.
- The positive divisors of n are all numbers of the form $\prod_{i=1}^{\infty} p_i^{c_i}$, where $0 \leq c_i \leq a_i$.
- The products are, of course, finite.

Prime Factorization and GCDs

Theorem

If two positive integers a and b have the factorizations

$$a = \prod_{i=1}^{\infty} p_i^{a_i}, \quad b = \prod_{i=1}^{\infty} p_i^{b_i},$$

then their gcd has the factorization $(a, b) = \prod_{i=1}^{n} p_i^{c_i}$, where each $c_i = \min\{a_i, b_i\}$, the smaller of a_i and b_i.

- Let $d = \prod_{i=1}^{\infty} p_i^{c_i}$. Since $c_i \leq a_i$ and $c_i \leq b_i$, we have $d \mid a$ and $d \mid b$.
  So d is a common divisor of a and b.
  Let e be any common divisor of a and b. Write $e = \prod_{i=1}^{\infty} p_i^{e_i}$.
  Then $e_i \leq a_i$ and $e_i \leq b_i$. So $e_i \leq c_i$. Hence, $e \mid d$.
  So d is the gcd of a and b.

Subsection 6

The Series of Reciprocals of the Primes

Series of Reciprocals of Primes

Theorem

The infinite series $\sum_{n=1}^{\infty} \frac{1}{p_n}$ diverges.

- We assume the series converges and obtain a contradiction.
  If the series converges, there is a k, such that $\sum_{m=k+1}^{\infty} \frac{1}{p_m} < \frac{1}{2}$.
  Let $Q = p_1 \cdots p_k$.
  Consider the numbers $1 + nQ$, for $n = 1, 2, \ldots$.
  None of these is divisible by any of the primes $p_1, \ldots, p_k$.
  So all the prime factors of $1 + nQ$ are among $p_{k+1}, p_{k+2}, \ldots$.
  Therefore, for each $r \geq 1$, we have

$$\sum_{n=1}^{r} \frac{1}{1 + nQ} \leq \sum_{t=1}^{\infty} \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t,$$

  since the sum on the right includes among its terms all the terms on the left.

Series of Reciprocals of Primes (Cont'd)

- We got

$$\sum_{n=1}^{r} \frac{1}{1+nQ} \leq \sum_{t=1}^{\infty} \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t .$$

The right-hand side of this inequality is dominated by the convergent geometric series $\sum_{t=1}^{\infty} (\frac{1}{2})^t$.

Therefore the series $\sum_{n=1}^{\infty} \frac{1}{1+nQ}$ has bounded partial sums.

It follows that

$$\sum_{n=1}^{\infty} \frac{1}{1+nQ}$$

converges.

But this is a contradiction because, by the Integral Test or by the Limit Comparison Test, this series diverges.

Remarks on the Series of Reciprocals of Primes

- The divergence of the series

$$\sum \frac{1}{p_n}$$

  was first proved by Euler.
- Euler noted that it implies Euclid's Theorem on the existence of infinitely many primes.
- Later, we will obtain an asymptotic formula which shows that the partial sums $\sum_{k=1}^{n} \frac{1}{p_k}$ tend to infinity like $\log(\log n)$.

Subsection 7

The Euclidean Algorithm

The Division Algorithm

Theorem (The Division Algorithm)

Given integers a and b, with $b > 0$, there exists a unique pair of integers q and r, such that

$$a = bq + r, \text{ with } 0 \leq r < b.$$

Moreover, $r = 0$ if and only if $b \mid a$.

- We say that q is the **quotient** and r the **remainder** obtained when b is divided into a.
- Let S be the set of nonnegative integers given by

$$S = \{y : y = a - bx, \ x \text{ is an integer}, \ y \geq 0\}.$$

  This is a nonempty set of nonnegative integers.

  So it has a smallest member, say $a - bq$. Let $r = a - bq$.

  Then $a = bq + r$ and $r \geq 0$.

The Division Algorithm (Cont'd)

Claim: $r < b$.

Assume $r \geq b$. Then $0 \leq r - b < r$.

But $r - b \in S$, since $r - b = a - b(q+1)$.

Hence $r - b$ is a member of S smaller than its smallest member, r.

This contradiction shows that $r < b$.

Claim: The pair q, r is unique.

If there were another such pair, say q', r', then $bq + r = bq' + r'$.

So $b(q - q') = r' - r$. Hence, $b \mid (r' - r)$.

If $r' - r \neq 0$, this implies $b < |r - r'|$, a contradiction.

Therefore, $r' = r$ and $q' = q$.

Finally, it is clear that $r = 0$ if and only if $b \mid a$.

Note: The proof gives us a method for computing q and r.

Subtract from a (or add to a) enough multiples of b until the smallest nonnegative number of the form $a - bx$ has been obtained.

The Euclidean Algorithm

Theorem (The Euclidean Algorithm)

Given positive integers a and b, where $b \nmid a$. Let $r_0 = a$, $r_1 = b$, and apply the division algorithm repeatedly to obtain a set of remainders $r_2, r_3, \ldots, r_n, r_{n+1}$ defined successively by the relations

$$\begin{array}{rcll} r_0 & = & r_1 q_1 + r_2, & 0 < r_2 < r_1, \\ r_1 & = & r_2 q_2 + r_3, & 0 < r_3 < r_2, \\ & \vdots & & \\ r_{n-2} & = & r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} & = & r_n q_n + r_{n+1}, & r_{n+1} = 0. \end{array}$$

Then r_n, the last nonzero remainder, is (a, b), the gcd of a and b.

- There is a stage at which $r_{n+1} = 0$ because the r_i are decreasing and nonnegative.

The Euclidean Algorithm (Cont'd)

- The last relation, $r_{n-1} = r_n q_n$ shows that $r_n \mid r_{n-1}$.

  The next to last shows that $r_n \mid r_{n-2}$.

  By induction we see that r_n divides each r_i.

  In particular $r_n \mid r_1 = b$ and $r_n \mid r_0 = a$.

  So r_n is a common divisor of a and b.

  Now let d be any common divisor of a and b.

  The definition of r_2 shows that $d \mid r_2$.

  The next relation shows that $d \mid r_3$.

  By induction, d divides each r_i.

  So $d \mid r_n$.

  Therefore, r_n is the required gcd.

Subsection 8

The Greatest Common Divisor of More than Two Numbers

The Greatest Common Divisor of More than Two Numbers

- The greatest common divisor of three integers a, b, c is denoted by (a, b, c) and is defined by the relation

$$(a, b, c) = (a, (b, c)).$$

- By a previous theorem, we have $(a, (b, c)) = ((a, b), c)$.
- So the gcd depends only on a, b, c and not on their order.
- Similarly, the gcd of n integers $a_1, \ldots, a_n$ is defined inductively by the relation

$$(a_1, \ldots, a_n) = (a_1, (a_2, \ldots, a_n)).$$

- Again, this number is independent of the order in which the a_i appear.

Properties of the Greatest Common Divisor

- If $d = (a_1, \ldots, a_n)$, it may be verified that:
  - d divides each of the a_i;
  - Every common divisor divides d.
- Moreover, d is a linear combination of the a_i.
- That is, there exist integers $x_1, \ldots, x_n$, such that

$$(a_1, \ldots, a_n) = a_1 x_1 + \cdots + a_n x_n.$$

Relatively Prime Numbers

- If $d = (a_1, \ldots, a_n) = 1$ the numbers a_i are said to be **relatively prime**.

  Example: $2, 3$ and 10 are relatively prime.
- If $(a_i, a_j) = 1$ whenever $i \neq j$, the numbers $a_1, \ldots, a_j$ are said to be **relatively prime in pairs** or **pairwise relative prime**.
- If $a_1, \ldots, a_n$ are relatively prime in pairs, then $(a_1, \ldots, a_n) = 1$.
- The converse is not necessarily true.

  Example: $(2, 3, 10) = 1$, but $(2, 10) = 2 \neq 1$.