AS.110.304 Elementary Number Theory

Contents

1 Mathematical Induction, Euclid's Division Lemma

Sections 1.1, 2.1

1.1 Principle of Mathematical Induction

Principle of Mathematical Induction

A statement about integers is true for all integers greater than or equal to 1 if

1. (base case) it is true for all integer 1, and
2. (inductive step) whenever is it true for all the in integers $1, 2, \cdots$, then it is true for the integer $k+1$.

Axiom: Well-Ordering Principle

Every nonempty set of positive integers has a least element.

1.2 Euclid's Division Lemma

Theorem 2.1 (Euclid's Division Lemma)

For any integers a and b ($b > 0$), there exist unique integers q and r such that $0 \leq r < b$ and

$$a = qb + r$$

Proof (Existence) Suppose

$$S := \{a - nb \,|\, n \in \mathbb{Z}, a - nb \geq 0\} \subset \mathbb{Z}_{>0}$$

$S \neq \varnothing$ because since $b > 0$, when n is sufficiently small, $a - nb$ can be arbitrarily large. By well-ordering principle, S contains a least element $r \geq 0$. Suppose $r = a - qb$ for some $r \in \mathbb{Z}$. If $r \geq b$, then $r - q = a - (q+1)b \in S$ and $r - b < r$, contradicting the fact that r is the least element in S. Thus, $0 \geq r < b$, and there exists q, r where $0 \leq r < q$ such that $a = qb + r$.

(Uniqueness) Suppose $0 \leq r, r' < b$, $a = qb + r = q'b + r'$. Then

$$(q - q')b = r' - r$$

Since $r, r' < b$, $|r' - r| < b$. We have $q - q' = 0 \Leftrightarrow q = q'$ and thus $r = r'$.

Q.E.D.

2 Divisibility, Linear Diophantine Equation, Fundamental Theorem of Arithmetic

Sections 2.2 - 2.4

2.1 Divisibility

2.1.1 Divisibility

Divisibility Let a, b be integers, we say b ***divides*** a, or b is a divisor of a, if a/b is an integer.
Notation: $b \mid a$ indicates b divides a, and ba indicate $b \nmid a$ does not divide a.

Note: b can be zero by the definition above.

Proposition

Let a, b, c be integers, if $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for all integers m, n.

Proposition Proof Suppose $a \mid b$ and $a \mid c$, there exist integers q_1, q_2 such that $b = q_1 a$ and $c = q_2 a$. Then

$$mb + nc = mq_1 a + nq_2 a = (mq_1 + nq_2)a$$

Since $mq_1 = nq_2 \in \mathbb{Z}$, we have $a \mid (mb + nc)$.

Q.E.D.

2.1.2 Greatest Common Divisor

Greatest Common Divisor If a and b are integers, not both zero, then an integer d is called the ***greatest common divisor*** of a and b if

(i) $d > 0$,
(ii) d is a common divisor of a and b, and
(iii) each integer f that is a common divisor of both a and b is also a divisor of d.

Notation: $\gcd(a, b)$, or simply (a, b)

Remark: (Theorem 2.2) If a, b are integers, not both zero, then $\gcd(a, b)$ always exists and is unique.

Euclidean Algorithm Suppose a, b are integers, without loss of generality, $a \geq b$. Put $a = qb + r$ for some integers q, r such that $0 \leq r < b$. Then, by Proposition 3.1,

$$\gcd(a, b) = \gcd(qb + r, b) = \gcd(r, b) = \gcd(b, r)$$

Repeat this process until $r = 0$, we find $\gcd(a, b)$, which equals to the smaller number of the two numbers remained at the end of the Euclidean Algorithm.

Corollary 2.1

If $d = \gcd(a, b)$, then there exist integers x and y such that $ax + by = d$.

Sketch of the Proof Construct r_m by Euclid' Division Lemma: $r_0 = |a|$, $r_1 = |b|$, and for all $m > 1$, $0 \le r_m < r_{m-1}$ and

$$r_{m-2} = c_{m-1}r_{m-1} + r_m$$

The Euclidean Algorithm implies $r_n = 0$ for some n, and $\gcd(a, b) = r_{n-1}$. Using strong induction on m yields that $\exists\, x, y : ax + by = r_{n-1} = \gcd(a, b)$.

Corollary 2.2

Let a, b, c be integers, and a, b are not both zero. There exist integers x and y such that $ax + by = c$ if and only if $d \mid c$, where $d = \gcd(a, b)$.

2.1.3 Prime

Prime A positive integer p other than 1 is said to be a ***prime*** if its only positive divisors are 1 and p.

Relatively Prime a and b are ***relatively prime*** (**coprime**) if $\gcd(a, b) = 1$.

Theorem 2.3

If a, b, c are integers, where a and c are relatively prime, and if $c \mid ab$, then $c \mid b$.

Proof Since $\gcd(a, c) = 1$, there exists integers x, y such that $ax + cy = 1$. Then

$$b = b(ax + cy) = abx + bcy$$

Since $c \mid ab$, $c \mid (abx + bcy)$, followed by $c \mid b$.

Q.E.D.

Corollary 2.3 Let a, b be integers and p be a prime. If $p \mid ab$ and $p \nmid a$, then $p \mid b$.

Sketch of the Proof: The proof relies on Theorem 2.3 and the fact that if p is a prime and $a \in \mathbb{Z}$, then $p \nmid a$ iff $\gcd(p, a) = 1$.

Corollary 2.4 Let $a_1, a_2, \cdots, a_n$ be integers, and let p be a prime. If $p \mid a_1a_2 \cdots a_n$, then there exists an i such that $p \mid a_i$.

Sketch of the Proof: By induction on n.

2.2 The Linear Diophantine Equation

Theorem 2.4

The linear Diophantine equation

$$ax + by = c$$

has a (integer) solution if and only if $d \mid c$, where $d = \gcd(a, b)$. Furthermore, if (x_0, y_0) is a solution of this equation, then the set of solutions of the equation consists of all integer pairs (x, y), where

$$x = x_0 + t\,\frac{b}{d} \quad \text{and} \quad y = y_0 - t\,\frac{a}{d} \quad (\text{for all } t \in \mathbb{Z}) \tag{2.2.1}$$

Lemma: (First, we reduced to the case where $\gcd(a, b) = 1$.) If $\gcd(a, b) = 1$ and (x_0, y_0) is a solution to 2.2.1, then the set of all solutions is $\{(x, y) \mid x = x_0 + bt, y = y_0 - bt, t \in \mathbb{Z}\}$.

Proof: For any $t \in \mathbb{Z}$, $(x_0 + bt, y_0 - bt)$ is a solution because

$$a(x_0 + bt) + b(y_0 - bt) = ax_0 + by_0 = c$$

Now let (x, y) be any solution, then $ax + by = c = ax_0 + by_0$, implying that $a(x - x_0) = -b(y - y_0)$. Recall $\gcd(a, b) = 1$, we have $b \mid (x - x_0)$ (Theorem 2.3). There exist $t \in \mathbb{Z}$ such that $x - x_0 = bt$, namely $x = x_0 + bt$. Substitute x back in the equation above yields

$$abt = -b(y - y_0), \quad \text{so} \quad y = y_0 - at.$$

Therefore, any solutions $(x, y) = (x_0 + bt, y_0 - at)$ for some $t \in \mathbb{Z}$. ■

Proof Suppose $d = \gcd(a, b)$ and $c = kb$ where $k \in \mathbb{Z}$. Dividing both sides of the equation yields

$$\frac{a}{d}x + \frac{b}{d}y = k$$

Notice that $\gcd(a/d, b/d) = 1$ (the proof is omitted). If (x_0, y_0) is a solution, by the lemma above, the set of solutions is

$$x = x_0 + t\,\frac{b}{d} \quad \text{and} \quad y = y_0 - t\,\frac{a}{d} \quad (\text{for all } t \in \mathbb{Z})$$

for all $t \in \mathbb{Z}$.

Q.E.D.

2.3 The Fundamental Theorem of Arithmetic

Theorem 2.5 (Fundamental Theorem of Arithmetic)

For each integer $n > 1$, there exist primes $p_1 \leq p_2 \leq \cdots \leq p_r$ such that

$$n = p_1 p_2 \cdots p_r$$

this factorization is unique.

Proof (*Existence*) We will use strong induction on n. For all $n > 2$, assume the statement holds for all $1 < i < n$. If n is a prime, the itself is a prime factorization. If n is not prime, there exists a divisor d such that $1 < d < n$, and then clearly $1 < n/d < n$. By inductive hypothesis, both d and n/d has a prime factorization. Rearranging the product of prime factorizations of d and n/d yields a prime factorization of n. By strong induction, we have proved the existence of prime factorization for all integer $n > 1$.

(*Uniqueness*) We will prove the uniqueness by strong induction on n. Clearly, 2 has a unique factorization. Assume the prime factorization of k is unique for all $1 < k < n$. Suppose $p_1 p_2 \cdots p_r$ and $p'_1 p'_2 \cdots p'_m$ are two prime factorizations of n. $p_1 p_2 \cdots p_r = p'_1 p'_2 \cdots p'_m$ yields $p_1 \mid p'_i$ for some i and $p'_1 \mid p_j$ for some j (Corollary 2.4), followed by $p_1 = p'_i$ and $p'_1 = p_j$, since all p and p' are prime. Note that $p'_1 \leq p'_i = p_1 \leq p_j = p'_1$, we have $p_1 = p'_1$. The result is trivial if $n = p_1$. If $n \neq p_1$, $1 < n/p_1 < n$, so

$$\frac{n}{p_1} = p_2 p_3 \cdots p_r = p'_2 p'_3 \cdots p'_m.$$

By inductive hypothesis, $r = m$ and $p_i = p'_i$ for all i. Hence two prime factorizations are identical, implying that the prime factorization is unique.

Q.E.D.

3 Permutations and Combinations

Sections 3.1

3.1 Permutations and Combinations

r-Permutation An ***r-permutation*** of a set S of n objects is an ordered selection of r elements from S.

Theorem 3.1

If ${}_nP_r$ denotes the number of r-permutations of a set of n objects, then

$$ {}_nP_r = n(n-1)\cdots(n-r+1) $$

Sketch of the Proof We can make our first selection in n ways, second selection in $n-1$ ways, and generally, i-th selection in $n-r+1$ ways.

Notation: $r!$, r factorial, is defined as $r! = r(r-1)\cdots 1 =_r P_r$, and we specify $0! = 1$.

r-Combination An ***r-combination*** of a set S of n objects is a subset of S having r elements.

Theorem 3.2

If $\binom{n}{r}$ denotes the number of r-combinations taken from a set S of n elements, then

$$ \binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{r!} $$

Sketch of the Proof To each r-combinations, we may give ${}_rP_r$ different orderings. Thus $\binom{n}{r} = {}_nP_r/{}_rP_r$, followed by the desired result.

Corollary The product of any n consecutive positive integers is divisible by $n!$.

Proof:

$$ \frac{N(N-1)\cdots(N-n+1)}{n!} = \binom{n}{r} \in \mathbb{Z} $$

4 Congruence, Residue Systems

Sections 4.1, 4.2

4.1 Congruence

Congruence Let a, b, n be integers. If $n \mid (a-b)$, a is ***congruent*** to b modulo n, denoted by $a \equiv b \pmod{n}$.

Note that n can be 0, and $m \equiv n \pmod{0}$ if and only if $m = n$.

Theorem 4.1

Let a, b, c, n be integers, the following statements hold:

1. Reflexive: $a \equiv a \pmod{n}$.
2. Symmetric: if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
3. Transitive: if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

In other words, congruence modulo n is an equivalence relation.

Proof (1) $(a-a)/n = 0 \in \mathbb{Z}$.

(2) Since $(a-b)/n \in \mathbb{Z}$, we have $(b-a)/n = -(a-b)/n \in \mathbb{Z}$.

(3) Since $(a-b)/n, (b-c)/n \in \mathbb{Z}$, we have $(a-c)/n = (a-b)/n + (b-c)/n \in \mathbb{Z}$.

Q.E.D.

Theorem 4.2

Suppose $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$$a \pm b \equiv a' \pm b' \pmod{n}, \qquad ab \equiv a'b' \pmod{n}$$

Proof Since $(a-a')/n, (b-b')/n \in \mathbb{Z}$, so are

$$\frac{(a \pm b) - (a' \pm b')}{n} = \frac{a-a'}{n} \pm \frac{b-b'}{n} \quad \text{and} \quad \frac{ab - a'b'}{n} = a\frac{b-b'}{n} + b'\frac{a-a'}{n}$$

Q.E.D.

Theorem 4.3 (Cancellation Law)

If $ab \equiv ab' \pmod{n}$ and if $\gcd(a, n) = 1$, then $b \equiv b' \pmod{n}$.

Proof Since $n \mid a(b-b')$ by congruence and a, n are relatively prime, $n \mid (b-b')$ (2.3), followed by $b \equiv b' \pmod{n}$.

Q.E.D.

4.2 Residue System

Residue If $a, b \in \mathbb{Z}$ and $a \equiv b \pmod{n}$, then b is a ***residue*** of a modulo n.

Note that it is not necessary that $0 \leq b < n$.

Complete Residue System A set of integers $\{r_1, \cdots, r_s\}$ is called a ***complete residue system*** modulo n if

1. $r_i \not\equiv r_j \pmod{n}$ for all $i \neq j$, and
2. for all $m \in \mathbb{Z}$, there exists an r_i such that $m \equiv r_i \pmod{n}$.

Corollary 4.1 Let n be a positive integer, then $\{0, 1, \cdots, n-1\}$ is a complete residue system modulo n.

Proof: Condition (1): If $i \equiv j \pmod{n}$ for some $0 \leq i, j \leq m-1$, then $m \mid (i-j)$. Since $|i-j| \leq m-1$, so $i = j$.

Condition (2): For all $m \in \mathbb{Z}$, by Euclid's Division Lemma, $m = qn + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < n$ thus $r \in S$. Since $m - r = qn$, $m \equiv r \pmod{n}$ for some r. ■

Theorem 4.4

If s different integers $r_1, \cdots, r_s$ form a complete residue system modulo n, then $s = n$.

Proof Let $S = \{r_1, \cdots, r_s\}$ ve a complete residue system modulo n. For each r_i, there exists $k_i \in \{0, 1, \cdots, m-1\}$ such that $r_i \equiv k_i \pmod{n}$ by Euclid's Division Lemma. If $k_i = k_j$, $r_i \equiv k_i \equiv k_j \equiv r_j \pmod{m}$. Therefore, $r_i \not\equiv r_j \pmod{n}$ whenever $i \neq j$, namely k_i is unique. Therefore, we deduce $s \leq m$. Without loss of generality, we can show $m \leq s$. Hence $s = m$.

Q.E.D.

Reduced Residue System A set of integers $\{r_1, \cdots, r_s\}$ is called a ***reduced residue system*** modulo n if

1. $\gcd(r_i, n) = 1$ for all $1 \leq i \leq s$,
2. $r_i \not\equiv r_j \pmod{n}$ for all $i \neq j$, and
3. for all $m \in \mathbb{Z}$ such that m is relatively prime to n, there corresponds an r_i such that $m \equiv r_i \pmod{n}$.

Proposition Suppose S is a complete residue system modulo n. Then $\{r \in S \mid \gcd(r, n) = 1\}$ is a reduced residue system modulo n.

Sketch of the Proof: The first two conditions are clearly met. Let $m \in \mathbb{Z}$ be coprime to n. Since S is a complete residue system modulo n, there exists a unique $x \in S$ such that $m \equiv x \pmod{n}$. Note that since $x \equiv m \pmod{n}$, $\gcd(x, n) = \gcd(m, n) = 1$, so $x \in \{r \in S \mid \gcd(r, n) = 1\}$. ■

Euler ϕ-function The ***Euler ϕ-function*** $\phi(m)$ is defined to be the number of positive integers less than or equal to m that are relatively prime to m.

Theorem 4.5

If s integers $r_1, \cdots, r_s$ form a reduced residue system modulo m, then $s = \phi(m)$.

Proof Denote $S = \{n \in \mathbb{Z} \,|\, 0 \leq n \leq m-1, \gcd(n, m) = 1\}$. Let $\{r_1, \cdots, r_s\}$ be a reduced residue system modulo m. For any r_i, since $\gcd(r_i, m) = 1$, there exists unique $s_i \in S$ such that $r_i \equiv s_i \pmod{m}$. If $r_i \neq s_j$, we can show that $s_i \neq s_j$ (we use the same argument as used in Theorem 4.4). Thus $s \leq \phi(m)$, similarly $\phi(m) \leq s$. Hence $s = \phi(m)$.

Q.E.D.

5 Solving Congruences

Sections 5.1 - 5.4

5.1 Linear Congruence

5.1.1 Solving Linear Congruences

Problem: Let a, c be non-zero integers and b be an integer. Determine all integer x such that $ax \equiv b \pmod{c}$.

Remark: Equivalently, there exists $y \in \mathbb{Z}$ such that $ax - b = cy$. Therefore, the congruence equation has a solution if and only if $\gcd(a, c) \mid c$. Now assume $d = \gcd(a, c) \mid b$ and let x_0 be a solution to the congruence. Then $a(x - x_0) \equiv 0 \pmod{c} \;\Leftrightarrow\; c \mid a(x - x_0) \;\Leftrightarrow\; \frac{c}{d} \mid \frac{a}{d}(x - x_0)$, followed by

$$x = x_0 + \frac{c}{d}t = x_0 + \frac{c}{\gcd(a, c)}t$$

where $t \in \mathbb{Z}$.

Note that the integers $x_0, x_0 + c/d, \cdots, x_0 + (c/d)(d-1)$ are mutually incongruent modulo c because the distance of any two of them is less than $|b|$. Moreover, $x_0 + (b/d)t$ is congruent to one of these integers. In fact, if $t = qd + r$ where $q, r \in \mathbb{Z}$ and $0 \le r < d$, then $x_0 + (c/d)t \equiv x_0 + (c/d)r \pmod{c}$. Therefore, the congruence equation has d mutually incongruent solutions.

Theorem 5.1

Let a, c be non-zero integers, let c be an integer, and denote $d = \gcd(a, c)$. Then the congruence

$$ax \equiv b \pmod{c}$$

has a solution if and only if $d \mid b$. If $d \mid b$, then the equation has d mutually incongruent solutions.

Finding a Solution To find a solution of the linear congruence $ax \equiv b \pmod{c}$, we can

- Euclidean algorithm on a, c, and back substitution
- Exhaust $x = 0, \pm 1, \pm 2, \cdots$
- Use the properties of congruence to simplify the congruence. For instance, $a \equiv a - c \pmod{c}$, divisibility, etc.

5.1.2 Inverse

If a, c are relatively prime, then all the solutions of $ax \equiv b \pmod{c}$ are congruence modulo c. In this case, we say a solution n of a congruence is ***unique*** modulo c.

Inverse If $a\bar{a} \equiv 1 \pmod{c}$, then $\bar{a}$ is called the ***inverse*** of a modulo c.

Finding the Inverse Performing Euclidean algorithm on a and m will yield $ax + my = 1$ for some $x, y \in \mathbb{Z}$. Since $m \mid my$, $ax \equiv 1 \pmod{m}$, so $\bar{a} = x$ is the desired inverse.

Corollary 5.1

If $\gcd(a, c) = 1$, then a has an unique inverse modulo c.

Proof Theorem 5.1 implies that $an \equiv 1 \pmod{c}$ has a solution n, and it is unique.

5.2 The Theorems of Euler, Fermat, and Wilson

Theorem 5.2 (Euler's Theorem)

If $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof Let $\{r_1, \cdots, r_{\phi(m)}\}$ be a reduced residue system modulo m. We can show that $\{ar_1, \cdots, ar_{\phi(m)}\}$ is also a reduced residue system modulo m:

1. Given $\gcd(a, m) = 1$, so $\gcd(ar_i, m) = 1$ for all i.
2. If for some $i \neq j$, $ar_i \equiv ar_j \pmod{m}$, then since $\gcd(a, m) = 1$, $r_i \equiv r_j \pmod{m}$ by cancellation law (Theorem 4.3), contradicting that $\{r_1, \cdots, r_{\phi(m)}\}$ is a reduced residue system. Hence $r_i \not\equiv r_j \pmod{m}$ whenever $i \neq j$.
3. Let $\bar{a}$ be an inverse of a modulo m. For any $n \in \mathbb{Z}$ such that $\gcd(n, m) = 1$, there exists an r_i such that $\bar{a}n \equiv r_i \pmod{m}$, since $\bar{a}n$ is relatively prime to m and $\{r_1, \cdots, r_{\phi(m)}\}$ is a reduced residue system. Thus, $n \equiv a \cdot \bar{a}n \equiv ar_i \pmod{m}$ for some i.

Therefore, there is a bijection $f : \{r_1, \cdots, r_{\phi(m)}\} \to \{ar_1, \cdots, ar_{\phi(m)}\}$ such that $f(r_i) \equiv r_i \pmod{m}$ for all i. Thus,

$$\prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} ar_i \equiv a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i \pmod{m}$$

Note that $\gcd(\prod_{i=1}^{\phi(m)} r_i, m) = 1$ since $\prod_{i=1}^{\phi(m)} r_i$ is a product of integers that are relatively prime to m. By the cancellation law,

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Q.E.D.

Corollary 5.2 (Fermat's Little Theorem)

If p is a prime, then $n^p \equiv n \pmod{p}$.

Proof If $p \nmid n$, by Euler's theorem, since $\phi(p) = p - 1$, we have $n^{p-1} \equiv 1 \pmod{p}$ and thus $n^p \equiv n \pmod{p}$. If $p \mid n$, $n^p \equiv 0 \equiv n \pmod{p}$.

Q.E.D.

Theorem 5.3 (Wilson's Theorem)

Let $m > 1$ be an integer. Then the congruence $(m-1)! \equiv -1 \pmod{m}$ holds if and only if m is a prime.

Proof Suppose m is a prime. For any integer $1 \leq a < m$, since $\gcd(a, m) = 1$, there exists an inverse of a modulo m, namely an unique $1 \leq \bar{a} < m$ such that $a\bar{a} \equiv 1 \pmod{n}$. Note that if $a = \bar{a}$, $a^2 \equiv 1 \pmod{m}$.

In this case, $m \mid (a-1)(a+1)$, and since m is a prime, we have $a = 1$ or $a = m-1$. Therefore, for each $1 < a < m-1$, we can pair it with its inverse modulo m, thus, $\prod_{a=2}^{m-2} a \equiv 1 \pmod{m}$. Then,

$$(m-1)! \equiv (m-1) \cdot \left(\prod_{a=2}^{m-2} a \right) \cdot 1 \equiv m-1 \equiv -1 \pmod{m}$$

Conversely, suppose m is not a prime. Then there exists an a $(1 < a < m)$ such that $a \mid m$. If $(m-1)! \equiv -1 \pmod{m}$, then $a \mid (m-1)! + 1$. However, $a \mid (m-1)!$, thus $a \mid 1$, resulting in a contradiction. Hence $(m-1)! \not\equiv -1 \pmod{m}$.

Q.E.D.

5.3 The Chinese Remainder Theorem

Theorem 5.4

Suppose $m_1, \cdots, m_s$ be pairwise relatively prime nonzero integers. Let $M = m_1 m_2 \cdots m_s$, and suppose that $a_1, \cdots, a_s$ are integers such that $\gcd(a_i, m_i) = 1$ for each i. The the system of s congruences

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \qquad \vdots \\ a_s x \equiv b_s \pmod{m_s} \end{cases}$$

has a simultaneous solution that is unique modulo M.

Remark The condition, $m_1, \cdots, m_s$ are pairwise relatively prime integers, is natural. If m_i, m_j are not relatively prime, we can reduce each congruence into multiple congruences in the form of $ax \equiv b \pmod{p_i^{e_i}}$ where p_i's are distinct primes.

Proof (Existence) For each $1 \le i \le s$, we can find a solution $x = x_i$ for

$$\begin{cases} a_i x_i \equiv b_i \pmod{m_i} \\ a_j x_j \equiv 0 \pmod{m_j} \ \forall\, j \ne i \end{cases} \tag{5.3.1}$$

and then $x = \sum_{i=1}^{s} x_i$ is a solution to the system of congruences [since for all i, $a_i \sum_{i=1}^{s} x_i \equiv a_i x_i + 0 \equiv b_i \pmod{m_i}$]. Since $\gcd(a_j, m_j) = 1$ and m_j's are pairwise coprime, so (5.4.1) is equivalent to

$$\begin{cases} a_i x_i \equiv b_i \pmod{m_i} \\ \quad x_i \equiv 0 \pmod{M/m_i} \end{cases} \tag{5.3.2}$$

Let $n_i := M/m_i$. By the second congruence in (5.3.2), $x_i = n_i k_i$ for some $k_i \in \mathbb{Z}$. Since $\gcd(a_i n_i, m_i) = 1$, the congruence

$$a_i n_i k_i \equiv b_i \pmod{m_i}$$

has a solution, followed by (5.3.2) has a solution.

(Uniqueness) Suppose $x = z_1$, $x = z_2$ are both solutions to the system, the for all i,

$$a_i(z_2 - z_1) \equiv 0 \pmod{m_i}.$$

Since $\gcd(a_i, m_i) = 1$, $m_i \,|\, (z_2 - z_1)$ for all i; and because m_i's are pairwise coprime, so $M \,|\, (z_2 - z_1)$.

Q.E.D.

5.4 Polynomial Congruences

Theorem 5.5

If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ $(a_n \neq 0)$ is a polynomial of degree n with integral coefficients. If p is a prime such that $p \nmid a_n$, then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n mutually incongruent solutions modulo p.

Proof We shall use induction on the degree n. If $n = 0$, the $f(x) = a_0 \neq 0$, so the congruence has no solution since $p \nmid a_n$. If $n = 1$, the congruence becomes $a_1 x \equiv -a_0 \pmod{p}$, which has a unique solution.

For $n \geq 1$, suppose the statement holds for all polynomials of degree n. Suppose $f(x)$ is a degree $n+1$ polynomial. If $f(x) \equiv 0 \pmod{p}$ has no solution, then we are done. Otherwise, let $x = x_0$ be a solution, then $f(x) - f(x_0) \equiv 0 \pmod{p}$, so

$$g(x) \cdot (x - x_0) \equiv 0 \pmod{p}$$

where

$$g(x) = a_n \cdot \frac{x^n - x_0^n}{x - x_0} + a_{n-1} \cdot \frac{x^{n-1} - x_0^{n-1}}{x - x_0} + \cdots + a_1$$

is a polynomial with integral coefficients of degree $n-1$ and its coefficient of x^{n-1} is a^n. By the inductive hypothesis, $g(x) \equiv 0 \pmod{p}$ has at most n mutually incongruent solutions. Hence $f(x)$ has at most $n+1$ incongruent solutions.

Q.E.D.

6 Arithmetic Function

6.1 Euler's Totient Function

Convention: All the integers are going to be considered and assumed to be positive.

Proposition

Suppose p is a prime and n is a positive integer then $\phi(p^n) = p^n - p^{n-1}$.

Proof An integer is coprime to p^n if and only if it is not a multiple of p. Then $\phi(p^n) = |\{1, \cdots, p^n\} \setminus \{p, 2p, \cdots, p^n\}| = p^n - p^{n-1}$.

Q.E.D.

Theorem 6.1

$\sum_{d|n} \phi(d) = n$.

Proof For each $d \,|\, n$, denote

$$T_d(n) := \{k \in \mathbb{Z} \mid 1 \leq k \leq n,\ \gcd(k, n) = d\}$$

then $\sum_{d|n} |T_d(n)| = n$ (because T_d is a partition). We want to show that $|T_d(n)| = \phi(n/d)$. In fact, for $1 \leq k \leq n$, $\gcd(k, n) = d$ iff $k = dq$ for some $1 \leq q \leq n/d$ where $\gcd(q, n/d) = 1$. Note that $|\{q \mid \gcd(q, n/d) = 1\}| = \phi(n/d)$, so $|T_d(n)| = \phi(n/d)$. It follows that

$$\sum_{d|n} \phi(d) = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} |T_d(n)| = n$$

Q.E.D.

Theorem

Let $m, n \in \mathbb{Z}_{\geq 1}$ be coprime. Then $\phi(mn) = \phi(m)\phi(n)$

Proof Let $\{r_1, \cdots, r_{\phi(m)}\}$, $\{s_1, \cdots, s_{\phi(n)}\}$ be reduced residue systems modulo m, n, respectively. It suffices to show that $\{nr_i + ms_j \mid 1 \leq i \leq \phi(m), 1 \leq j \leq \phi(n)\}$ form a reduced residue system modulo mn.

1. We want to show $\gcd(nr_i + ms_j) = 1$. If p is a prime such that $p \mid \gcd(nr_i + ms_j, mn)$, then $p \mid mn$. Without loss of generality, suppose $p \mid m$, then $p \nmid n$ since m and n are coprime. Note that $p \mid (nr_i + ms_j)$ implies $p \mid nr_i$, thus $p \mid r_i$. Then $p \mid \gcd(m, r_i)$, contradiction. Therefore, $\gcd(nr_i + ms_j) = 1$ for all i, j.
2. We want to show that $nr_i + ms_j \not\equiv nr_k + ms_l \pmod{mn}$ whenever $(i, j) \neq (k, l)$. In fact, if $nr_i + ms_j \equiv nr_k + ms_l \pmod{mn}$, $n(r_i - r_k) + m(s_j - s_l) \equiv 0 \pmod{mn}$. In particular, $m \mid n(r_i - r_k) + m(s_j - s_l)$, so $m \mid n(r_i - r_k)$. Since $\gcd(m, n) = 1$, $m \mid (r_i - r_k)$ thus $r_i \equiv r_k \pmod{m}$, contradiction. Therefore, $nr_i + ms_j \not\equiv nr_k + ms_l \pmod{mn}$ whenever $(i, j) \neq (k, l)$.
3. We want to show that for all $t \in \mathbb{Z}$ such that $\gcd(t, mn) = 1$, there exists (i, j) such that $r \equiv nr_i + ms_j \pmod{mn}$. Since $\gcd(m, n) = 1$, there exists an inverse $\bar{n}$ of n modulo m. Since $\gcd(t, m) = 1$, $\gcd(\bar{n}t, m) = 1$. There exists $\bar{n}t \equiv r_i \pmod{m}$ thus $t \equiv nr_i \pmod{m}$ for some r_i by reduced residue

system. Without loss of generality, $t \equiv ms_j \pmod{n}$. Now we have $t \equiv nr_i + ms_j \pmod{m}$ and $t \equiv nr_i + ms_j \pmod{n}$. Given that $\gcd(m, n) = 1$, $t \equiv nr_i + ms_j \pmod{mn}$.

Then $\phi(mn) = |\{nr_i + ms_j \mid 1 \leq i \leq \phi(m), 1 \leq j \leq \phi(n)\}| = \phi(m)\phi(n)$.

Q.E.D.

Theorem 6.2

$\phi(n) = n \prod_{p \mid n} \left(1 - \dfrac{1}{p}\right)$ where p are primes.

Proof For $n = 1$, $\phi(1) = 1$. For $n \geq 2$, let $n = \prod_{i=1}^{k} p_i^{n_i}$ where p_i's are pairwise distinct primes and n_i's are positive integers. By the previous theorem and the proposition,

$$\phi(n) = \prod_{i=1}^{k} \phi(p_i^{n_i}) = \prod_{i=1}^{k} p_i^{n_i} - p_i^{n_i - 1} = \prod_{i=1}^{k} p_i^{n_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Q.E.D.

6.2 Divisors

d(n), σ(n) For $n \in \mathbb{Z}_{\geq 1}$, denote by $d(n)$ the number of positive divisors of n and denote by $\sigma(n)$ the sum of these divisors.

Proposition

If p is a prime and $n \in \mathbb{Z}_{\geq 1}$, then $d(p^n) = n + 1$ and $\sigma(p^n) = (p^{n+1} - 1)/(p - 1)$.

Sketch of the Proof The divisors of p^n are $1, p, 2p, \cdots, p^n$. Clearly $d(p^n) = n + 1$, and $\sigma(p^n)$ follows from geometric series.

Corollary 6.1

Let $m, n \in \mathbb{Z}_{\geq 1}$ be coprime. Then $d(mn) = d(m)d(n)$ and $\sigma(mn) = \sigma(m)\sigma(n)$.

Sketch of the Proof Since $\gcd(m, n) = 1$, a positive divisor of mn can be written as the product of a positive divisor of m and a positive divisor of n in a unique way (prime factorization). Therefore,

$$d(mn) = \sum_{d \mid mn} 1 = \left(\sum_{d_1 \mid m} 1\right)\left(\sum_{d_2 \mid n} 1\right) = d(m)d(n)$$

$$\sigma(mn) = \sum_{d \mid mn} d = \left(\sum_{d_1 \mid m} d_1\right)\left(\sum_{d_2 \mid n} d_2\right) = \sigma(m)\sigma(n).$$

Theorem 6.3

For $n = p_1^{r_1} \cdots p_k^{r_k}$ where p's are distinct primes and $n_i \in \mathbb{Z}$ for all i. We have

$$d(n) = (r_1+1)(r_2+1)\cdots(r_k+1)$$

$$\sigma(n) = \frac{p_1^{r_1+1}-1}{p_1-1}\cdots\frac{p_k^{r_k+1}-1}{p_k-1}$$

Remark m is a positive divisor of n if and only if $m = p_1^{r_1'} \cdots p_k^{r_k'}$ where $0 \le r_i' \le r_i$. $d(n)$ is obvious from the combinatorial view. Let $n' = p_2^{r_2} \cdots p_k^{r_k}$, note that

$$\sigma(n) = \sum_{i=0}^{r_1} \left(\sum_{1 \le r_i' \le r_i} p_i^{r_i'} \right) = \sum_{i=0}^{r_1} \sigma(n')$$

so $\sigma(n)$ follows from the induction.

Remark: Here we first prove Corollary 6.1 as a theorem, and then deduced Theorem 6.3 as the corollary.

6.3 Multiplicative Arithmetic Function

Multiplicative An ***arithmetic function*** is a map $f : \mathbb{Z}_{\ge 1} \to \mathbb{C}$. It is ***multiplicative*** if $f(mn) = f(m)f(n)$ whenever $\gcd(m,n) = 1$.

Möbius Function

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } p^2 \mid n \text{ for some prime } p \\ (-1)^r, & \text{if } p = p_1, \cdots, p_r \text{ where } p_i \text{ are distinct primes} \end{cases}$$

Theorem 6.4

$\phi(n)$, $d(n)$, $\sigma(n)$, and $\mu(n)$ are multiplicative arithmetic functions.

Proof We have already shown that $\phi(n)$, $d(n)$, and $\sigma(n)$ are multiplicative arithmetic functions. Suppose $\gcd(m,n) = 1$. We will show μ is multiplicative by cases:

1. If $m = 1$ or $n = 1$. WLOG, suppose $n = 1$, then $\mu(mn) = \mu(m) = \mu(m) \cdot 1 = \mu(m)\mu(n)$.
2. If $m, n > 1$ and any of the exponents of the prime factorization exceeds 1, then $\mu(mn) = 0 = \mu(m)\mu(n)$.
3. If $m, n > 1$ and all exponents are 1. Suppose n is the product of r primes and m is the product of s primes, then $\mu(n) = (-1)^r$ and $\mu(m) = (-1)^s$. Also, since primes are distinct (since m, n are coprime), mn is the product of $r + s$ primes, namely $\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(n)\mu(m)$.

Q.E.D.

6.4 The Möbius Inversion Formula

Theorem 6.5

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

Proof Suppose $n = 1$, $\mu(1) = 1$. Suppose $n > 1$, let $n = p_1^{n_1} \cdots p_k^{n_k}$ where p's are distinct primes and $n_i \in \mathbb{Z}_{\geq 1}$. For all positive divisors $d \mid n$, $\mu(d) \neq 0$ if and only if $d = p_1^{m_1} \cdots p_k^{m_k}$ where $m_i \in \{0, 1\}$ for all i. Incomplete!

Theorem 6.6 (Möbius Inversion Formula)

Let $f(n)$ and $g(n)$ be arithmetic functions. The following conditions are equivalent.

$$(1) \quad f(n) = \sum_{d|n} g(d) \qquad \Leftrightarrow \qquad (2) \quad g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

Proof We first assume (1), then

$$\begin{aligned} \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{dd'=n} \mu(d) f(d') = \sum_{dd'=n} \mu(d) \sum_{e|d'} g(e) \\ &= \sum_{deh=n} \mu(d) g(e) = \sum_{e|n} g(e) \sum_{d|(n/e)} \mu(d) \end{aligned}$$

where the second equality in line 1 comes from (1). By Theorem 6.5, $\sum \mu(d) = 1$ if and only if $d = 1$ and $\sum \mu(d) = 0$ otherwise. All other terms with $d \neq 1$, namely $e \neq n$, vanishes, so the summation is equal to $g(n)$. Hence

$$\sum_{d|n} \mu(d) = g(n).$$

Conversely, we assume (2), then

$$\begin{aligned} \sum_{d|n} g(d) &= \sum_{d|n} \sum_{d'|d} \mu(d') f\left(\frac{d}{d'}\right) = \sum_{dd'e=n} \mu(d') f(e) \\ &= \sum_{e|n} f(e) \sum_{d'|(n/e)} \mu(d') \end{aligned}$$

where the first equality in the first line comes from (2). Similar to the argument above, $\sum_{d'|(n/e)} \mu(d') = 1$ if and only if $n/e = 1$, i.e., $e = n$. Hence the summation is equal to $f(n)$, followed by

$$\sum_{d|n} g(d) = f(n).$$

Q.E.D.

Remark We say that $(f(n), g(n))$ is a ***Möbius pair*** if f and g satisfy the condition in the above theorem. Möbius pair is not symmetric, i.e., $(f(n), g(n))$ is a Möbius pair does not imply $(g(n), f(n))$ is a Möbius pair.

Theorem 6.8

$(n, \phi(n))$, $(d(n), 1)$, and $(\sigma(n), n)$ are all Möbius pairs.

Proof $n = \sum_{d|n} \phi(n)$ by Theorem 6.1, $d(n) = \sum_{d|n} 1$ and $\sigma(n) = \sum_{d|n} d$ by definition.

Q.E.D.

Theorem 6.7

If one of the functions in the Möbius pair $(f(n), g(n))$ is multiplicative, so is the other.

Proof Suppose f is multiplicative and $\gcd(m, n) = 1$.

$$\begin{aligned} g(mn) &= \sum_{d|mn} \mu(d) f\left(\frac{mn}{d}\right) = \sum_{e|m} \sum_{h|n} \mu(eh) f\left(\frac{mn}{eh}\right) \\ &= \sum_{e|m} \sum_{h|n} \mu(e)\mu(h) f\left(\frac{m}{e}\right) f\left(\frac{n}{h}\right) \\ &= \left[\sum_{e|m} \mu(e) f\left(\frac{m}{e}\right)\right] \left[\sum_{h|n} \mu(h) f\left(\frac{n}{h}\right)\right] \\ &= g(m)g(n) \end{aligned}$$

Hence g is multiplicative. The proof of the other direction is similar.

7 Primitive Roots

7.1 Properties of Reduced residue Systems

Multiplicative Order Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. Suppose $\gcd(a, m) = 1$, the (multiplicative) ***order*** of a modulo m is the smallest positive integer d such that $a^d \equiv 1 \pmod{m}$.

Theorem 7.2

If d is the order of a modulo m, and $a^n \equiv 1 \pmod{m}$ for some positive integer n, then $d \mid n$.

Proof By Euclid's division lemma, there exists $q \in \mathbb{Z}_{\geq 0}$ and $0 \leq r < d$ such that $n = qd + r$. Then,

$$1 \equiv a^n = (a^d)^q \cdot a^r \equiv a^r \pmod{m}.$$

Since d is the smallest positive integer such that $a^d \equiv 1 \pmod{m}$, $r = 0$, thus $n = qd$.

Q.E.D.

Corollary

If d is the order of a modulo m, then $d \mid \phi(m)$.

Primitive Root If $\phi(m)$ is the order of a modulo m, then a is called a ***primitive root*** modulo m.

Theorem 7.3

If a is a primitive root modulo m, then $a, a^2, a^{\phi(m)}$ are mutually incongruent and form a reduced residue system modulo m.

Sketch of Proof Assume there exist $1 \leq i < j \leq \phi(m)$ such that $a^i \equiv a^j \pmod{m}$. Then $m \mid a^i(a^{j-i} - 1)$, so $m \mid (a^{j-i} - 1)$ since m and a^i are coprime, followed by $a^{j-i} \equiv 1 \pmod{m}$. Note that $j - i < \phi(m)$, this contradicts that a is primitive root of m, so $a, a^2, \cdots, a^{\phi(m)}$ are mutually incongruent.

All conditions for reduced residue system are satisfied: (1) holds because $\gcd(a^i, m) = 1$ for all i since $\gcd(a, m) = 1$; (2) holds because $a, \cdots, a^{\phi(m)}$ are mutually incongruent; (3) is automatically satisfied by $|\{a, a^2, \cdots, a^{\phi(m)}\}| = \phi(m)$. Hence $a, a^2, \cdots, a^{\phi(m)}$ is a reduced residue system.

Theorem 7.4

If h is the order of a modulo m and k is a positive integer such that $\gcd(k, h) = d$, then h/d is the order of a^k modulo m.

Proof Denote by j the order of a^k modulo m. Let $k = k'd$, $h = h'd$, then $\gcd(k', h') = 1$. We need to show $j = h'$.

Since $a^h \equiv 1 \pmod m$,

$$(a^k)^{h'} = a^{k'd \cdot h'} = (a^h)^{k'} \equiv 1 \pmod m$$

so $j \mid h'$ (Theorem 7.2). Note that by the definition of j, $a^{kj} \equiv 1 \pmod m$, so $h \mid kj$, namely $h' \mid k'j$. Note that $\gcd(h', k') = 1$, we have $h' \mid j$ (Theorem 2.3). Hence $h/d = h' = j$ is the order of a^k modulo m.

Q.E.D.

Corollary 7.1

If a is a primitive root modulo m, then a^r is a primitive root modulo m if and only if $\gcd(r, \phi(m)) = 1$.

Proof The order of a modulo m is $\phi(m)$, while the order of a^r modulo m is $\phi(m)/\gcd(r, \phi(m))$ (Theorem 7.4), which equals $\phi(m)$ if and only if $\gcd(r, \phi(m)) = 1$. Therefore, a^r is a primitive root if and only if $\gcd(r, \phi(m)) = 1$.

Q.E.D.

Theorem 7.5

If there exists a primitive root modulo m, then there are exactly $\phi(\phi(m))$ mutually incongruent primitive roots modulo m.

Proof Suppose a is a primitive root modulo m, then $\{a, a^2, \cdots, a^{\phi(m)}\}$ is a reduced residue system modulo m. a^r is a primitive root if and only if $\gcd(r, \phi(m)) = 1$ (Corollary 7.1), so there are exactly $\phi(\phi(m))$ primitive roots by the definition of ϕ-function.

Q.E.D.

7.2 Primitive Roots Modulo p

Theorem 7.6

For each prime p there exist primitive roots modulo p.

Proof For each $d \mid p-1$, denote by $N(d)$ the number of elements in $\{1, \cdots, p-1\}$ whose order modulo m equals d (we want to prove $N(p-1) \geq 1$). Clearly by the definition of N, $p - 1 = \sum_{d \mid p-1} N(d)$.

Lemma 7.6.1 $N(d) = 0$ or $N(d) = \phi(d)$ for all $d \mid p-1$.

By Lemma 7.6.1, we see that $N(d) \leq \phi(d)$, followed by

$$p - 1 = \sum_{d \mid p-1} N(d) \leq \sum_{d \mid p-1} \phi(d) = p - 1,$$

where the last equality holds by Theorem 6.1. Therefore, $N(d) = \phi(d)$ for all $d \mid p-1$. In particular, $N(p-1) = \phi(p-1) \geq 1$.

Proof of Lemma 7.6.1 If $N(d) > 0$, let a be of order d. Then $a, a^2, \cdots, a^d$ are mutually incongruent solutions of $x^d \equiv 1 \pmod m$, and they are all of the mutually incongruent solutions since the congruence has at most d solutions (Theorem 5.5). The order of a^h modulo m is d if and only $\gcd(h, d) = 1$ (Corollary 7.1), thus there are exactly $\phi(d)$ elements. It implies that $N(d) = \phi(d)$.

Q.E.D.

8 Prime Numbers

π For $x \in \mathbb{R}_{>0}$, denote by $\pi(x)$ the number of primes less than or equal to x.

Theorem 8.1

$\lim_{x\to\infty} \pi(x) = +\infty$; that is, there exist infinitely many primes.

Proof Assume for the sake of contradiction there are only finitely many primes, $p_1, \cdots, p_n$. Let $M = p_1 \cdots p_n + 1$. Clearly $p_i \nmid M$ for all i, so we deduce that M has no prime factorization, contradicting the fundamental theorem of arithmetic. Hence there are infinitely many primes.

Q.E.D.

Notation: For $x \in \mathbb{R}$, denote by $[x]$ the largest integer less than or equal to x.

Prime Number Theorem

$$\lim_{x\to+\infty} \frac{\pi(x)}{x/\log x} = 1$$

Theorem 8.2

(Lemma of Theorem 8.4) If k is a positive integer,

$$\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{k}{x}$$

Proof Suppose $[x] = qk + r$, where $0 \leq r < k$. Consider the partition

$$\{1, \cdots, [x]\} = \{1, \cdots, k\} \cup \{k+1, \cdots, 2k\} \cup \cdots \cup \{kq+1, \cdots, kq+r\}.$$

Among $\{1, \cdots, k\}$, there are at most k primes. Among $\{mk+1, \cdots, (m+1)k\}$ (where $1 < k < q$), there are at most $\phi(k)$ primes, since only the number coprime to k can be a prime and we know $\gcd(ik+j, k) = \gcd(j, k)$ for all i, j. Similarly, among $\{kq+1, \cdots, kq+r\}$, there are at most $\phi(k)$ primes. Consequently,

$$\pi(x) \leq k + q\phi(k) \leq k + \frac{x}{k}\phi(k)$$

Hence,

$$\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{k}{x}$$

Q.E.D.

Theorem 8.3

(Lemma of Theorem 8.4) If $M > 1$ and $p_1, \cdots, p_s$ are all primes less than or equal to M, then

$$\sum_{n=1}^{M} \frac{1}{n} < \frac{1}{\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)}$$

Proof By the geometric series, for each p,

$$\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots,$$

so we express the right hand side of the inequality as

$$\frac{1}{\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right)} = \prod_{i=1}^{s}\left(1+\frac{1}{p_i}+\frac{1}{p_i^2}+\cdots\right) = \sum_{\mathbf{m}\in\{\mathbb{Z}_{>0}\}^s} \frac{1}{p_1^{m_1}\cdots p_s^{m_s}} = \sum_{n\in\Lambda}\frac{1}{n} < \sum_{n\le M}\frac{1}{n}$$

where Λ is the set of positive integers whose prime factors are $p_1, \cdots, p_s$. Note that the last inequality holds because the prime factors of n are less or equal to M, that is $p_1, \cdots, p_s$, for all $n \le M$.

Q.E.D.

Theorem 8.4

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 0$$

Proof For any $\varepsilon > 0$. Since $\sum_{n=1}^{\infty} 1/n$ diverges, there exists M such that $\sum_{n=1}^{M} 1/n > 2/\varepsilon$. Let $p_1, \cdots, p_s$ be primes less than M, and let $k = p_1 \cdots p_s$. Therefore,

$$\frac{\pi(x)}{x} \le \frac{\phi(k)}{k} + \frac{k}{x} = \frac{k\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right)}{k} + \frac{k}{x} < \left(\sum_{n=1}^{M}\frac{1}{n}\right)^{-1} + \frac{k}{x}.$$

where the first inequality holds by Theorem 6.2 and the second inequality holds by Theorem 8.3. For $x > 2k/\varepsilon$,

$$\frac{\pi(x)}{x} < \left(\frac{2}{\varepsilon}\right)^{-1} + \frac{k}{2k/\varepsilon} = \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Since $\pi(x)/x \ge 0$ for $x \ge 0$, we conclude that $\lim_{x\to\infty} \dfrac{\pi(x)}{x} = 0$.

Q.E.D.

Theorem 8.6

If p is a prime, then $\sum_{j=1}^{\infty}\left[\dfrac{n}{p^j}\right]$ is the exponent of p appearing in the prime factorization of $n!$.

Proof If $p > n$, the statement is trivial. Suppose $p \le n$. For $j > 0$, there are $[n/p^j]$ integers divisible by p a j-th time, namely

$$p^j, 2p^j, \cdots, \left[\frac{n}{p^j}\right]p^j.$$

After finitely many repetitions, we see the total number of time p divides numbers in $\{1, \cdots, n\}$ is precisely $\sum j = 1^{\infty}[n/p^j]$.

Q.E.D.

9 Quadratic Residues

9.1 Euler's Criterion

Quadratic Residue Let p be a prime and $a \in \mathbb{Z}$. If $p \nmid a$ and

$$x^2 \equiv a \pmod{p}$$

has a solution, then we say that a is a ***quadratic residue*** modulo p.

Corollary 9.1

Let p be an odd prime and $a \in \mathbb{Z}$ such that $p \nmid a$. Let g be a primitive root and $r \in \mathbb{Z}$ such that $g^r \equiv a \pmod{p}$. Then a is a quadratic residue modulo p if and only if r is even.

Proof ($\Leftarrow$) If r is even, then $x^2 \equiv a \pmod{p}$ has a solution $x = g^{r/2}$.

($\Rightarrow$) Suppose $x^2 \equiv a \pmod{p}$ has a solution. Since $x \equiv g^s$, $a \equiv g^r \pmod{p}$ for some $s, r \in \mathbb{Z}$ (Theorem 7.3), we have $g^r \equiv g^{2s} \pmod{p}$, i.e., $g^{r-2s} \equiv 1 \pmod{p}$. By Theorem 7.2, $(p-1) \mid (r-2s)$ since p is a primitive root. Since $p-1$ is even, $r-2s$ is even, thus r is even.

Q.E.D.

Theorem 9.1 (Euler's Criterion)

The integer a is a quadratic residue modulo p if and only if

$$a^{(p-1)/2} \equiv 1 \pmod{p}$$

Proof ($\Rightarrow$) Suppose $x^2 \equiv a \pmod{p}$ has a solution. By $p \nmid a$, $p \nmid x$, so

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$$

where the last equality holds by Euler's Theorem.

($\Leftarrow$) Suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$, and $a \equiv g^r \pmod{p}$ for some r where g is a primitive root. Then $g^{r(p-1)/2} \equiv 1 \pmod{p}$. By Theorem 7.2, $(p-1) \mid r(p-1)/2$, so $r/2 \in \mathbb{Z}$, i.e., r is even. Therefore, putting $x = g^{r/2}$ results in $x^2 \equiv g^r \equiv a \pmod{p}$, so a is a quadratic residue modulo p.

Q.E.D.

9.2 The Legendre Symbol

Legendre Symbol If p is an odd prime, then define the ***Legendre Symbol*** as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ 0 & \text{if } p \mid a \\ -1 & \text{if } p \text{ is a quadratic non-residue modulo } p \end{cases}$$

Theorem 9.2

If p is an odd prime and a and b are relatively prime to p, then

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right), \text{ if } a \equiv b \pmod p \tag{9.2.a}$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \tag{9.2.b}$$

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p \tag{9.2.c}$$

Proof (a) holds directly from the definition.

(b): If $p \mid ab$, $\left(\frac{ab}{p}\right) = 0 = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. If $p \nmid ab$, let g be a primitive root modulo p. Suppose $g^r \equiv a \pmod p$ and $g^s \equiv b \pmod p$. By the Corollary 9.1, $\left(\frac{a}{p}\right) = 1$ if and only if r is even; that is, $\left(\frac{a}{p}\right) = (-1)^r$. Similarly, $\left(\frac{b}{p}\right) = (-1)^s$, and $\left(\frac{ab}{p}\right) = (-1)^{r+s}$ because $ab \equiv g^{r+s} \pmod p$. Thus, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(c) If $p \mid a$, then $a^{(p-1)/2} \equiv 0 \equiv \left(\frac{a}{p}\right) \pmod p$. If a is a quadratic residue modulo p, $a^{(p-1)/2} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod p$ by Euler's Criterion. Otherwise, $a^{p-1} \equiv 1 \pmod p$ by Fermat's Little Theorem, thus

$$(a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1) \equiv 0 \pmod p$$

However, $a^{(p-1)/2} \not\equiv 1$ by Euler's Criterion, so $p \mid (a^{(p-1)/2} + 1)$. Therefore, $a^{(p-1)/2} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod p$.

Q.E.D.

9.3 The Quadratic Reciprocity Law

Least Residue If p be an odd prime, the ***least residue*** modulo p, denoted by $r(n)$, is the unique integer $x \in (-p/2, p/2]$ such that $n \equiv x \pmod p$.

Signum (Sign) We define ***signum*** of x, denoted by $\operatorname{sgn}(x)$ by $\operatorname{sgn}(x)$ equals 1 if $x > 0$, 0 if $x = 0$, and -1 if $x < 0$.

Theorem 9.3 (Gauss's Lemma)

Let $\gcd(a, p) = 1$ where p is an odd prime, let m be the number of integers in the set

$$\left\{a, 2a, \cdots, \frac{p-1}{2}a\right\}$$

whose least residues modulo p are negative. Then

$$\left(\frac{a}{p}\right) = (-1)^m$$

Proof Note that all integers in $\{a, 2a, \cdots, \frac{1}{2}(p-1)a\}$ are coprime to p. For any $n \in \{1, \cdots, (p-1)/2\}$, we have $na \equiv r(na) = \operatorname{sgn}(r(na))|r(na)| \pmod p$. Let m denotes the number of integers in the set whose least residue is negative, then $\prod \operatorname{sgn}(r(na)) = (-1)^m$. We deduce that

$$\left(\frac{p-1}{2}\right)! \cdot a^{(p-1)/2} \equiv (-1)^m \prod_{n=1}^{(p-1)/2} |r(na)| \pmod{p}$$

Note that $1 \le |r(na)| \le (p-1)/2$ for all n. For any integers $1 \le n_1 < n_2 \le (p-1)/2$, note that $p \nmid (n_1 \pm n_2)a$, so $|r(n_1 a)| \ne |r(n_2 a)|$. That is, $\{1, \cdots, (p-1)/2\} = \{|r(na)| : 1 \le n \le (p-1)/2\}$, then $\prod_{n=1}^{(p-1)/2} |r(na)| = (\frac{p-1}{2})!$. By the cancellation Law (since $(\frac{p-1}{2})!$ is coprime to p) and Theorem 9.2(c),

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

and $(\frac{a}{p}) = (-1)^m$ because both side are in $\{\pm 1\}$ and $p > 2$.

Q.E.D.

Theorem 9.5

If p is an odd prime, then

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \text{ and} \tag{9.5.a}$$

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} \tag{9.5.b}$$

Remark The theorem above is equivalent to

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases} \quad \text{and} \quad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

Proof (a) By Gauss's Lemma, with $a = -1$, we see that $m = (p-1)/2$ (since all integers in the set $\{a, 2a, \cdots, (p-1)a/2\}$ have negative least residue); this establishes (9.5.a).

(b) The number of integer in $\{2, 4, \cdots, p-1\}$ whose least residues modulo p are negative, which is denoted by m, is equal to the number of even integers in $[(p+1)/2, p-1]$. That is,

$$m = \begin{cases} 2k & \text{if } p = 8k+1 \\ 2k+1 & \text{if } p = 8k+3 \\ 2k+1 & \text{if } p = 8k+5 \\ 2k+2 & \text{if } p = 8k+7 \end{cases}$$

where $k \in \mathbb{Z}$. Note that m is even when $m \equiv \pm 1 \pmod{8}$ and m is odd when $m \equiv \pm 3 \pmod{8}$. By Gauss's Lemma,

$$\left(\frac{2}{p}\right) = (-1)^m = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

which is equivalent to the desired result.

Q.E.D.

Theorem 9.4 (Quadratic Reciprocity Law)

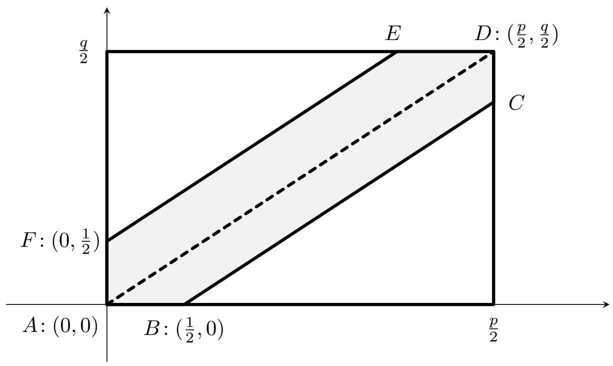
If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

That is, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless $p \equiv q \equiv 3 \pmod 4$, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Proof Let m_1, m_2 denotes the number of integers in $\{q, 2q, \cdots, \frac{1}{2}(p-1)q\}$, $\{p, 2p, \cdots, \frac{1}{2}(q-1)p\}$ with negative least residues modulo p. By Gauss's Lemma, $\left(\frac{p}{q}\right) = (-1)^{m_1}$ and $\left(\frac{q}{p}\right) = (-1)^{m_2}$. (We want to show that $m_1 + m_2$ is odd if and only if $p \equiv q \equiv 3 \pmod 4$.)

Consider the following figure, where $AD \parallel BC \parallel EF$,



It is not hard to find $C = \left(\dfrac{p}{2}, \dfrac{q(p-1)}{2p}\right)$ and $E = \left(\dfrac{p(q-1)}{2q}, \dfrac{q}{2}\right)$. The theorem results from the following two statements:

Lemma 1: m_1, m_2 are the number of lattice points in the quadrilateral $ADEF$, $ABCD$.

Lemma 2: The number of lattice points in the hexagon $ABCDEF$ is odd if and only if $p \equiv q \equiv 3 \pmod 4$.

Proof of Lemma 1: If (x, y) is a lattice point in $ADEF$, then

$$\begin{cases} y > \dfrac{q}{p}x & y < \dfrac{q}{p}x + \dfrac{1}{2} \\ y < \dfrac{q}{2} & x > 0 \end{cases} \implies \begin{cases} 0 < x < \dfrac{p}{2} \\ -\dfrac{p}{2} < xq - py < 0 \end{cases} \tag{9.1}$$

Therefore, xq has a negative least residue modulo p, so xq has a negative least residue modulo p.

Conversely, if $xq \in \{q, 2q, \cdots, \frac{1}{2}(p-1)q\}$ and xq has a negative least residue modulo p, there exists a unique $y \in \mathbb{Z}$ such that $-p/2 < xq - py < 0$. Since

$$y < \frac{q}{p}x + \frac{1}{2} \leq \frac{q(p-1)}{2p} + \frac{1}{2} < \frac{q+1}{2}$$

and $y \in \mathbb{Z}$, we have $y < q/2$. Thus we get the left hand side of (9.1), namely (x, y) is a lattice point in $ADEF$.

In this way, we establish a bijection between the set of lattice points in $ADEF$ and the set of integers in $\{q, 2q, \cdots, (p-1)q/2\}$ with negative negative least residues modulo p. ■

Proof of Lemma 2:

$$ABDCDEF : \begin{cases} 0 < x < p/2 \\ 0 < y < q/2 \\ \dfrac{q}{p}\left(x - \dfrac{1}{2}\right) < y < \dfrac{q}{p}x + \dfrac{1}{2} \end{cases} \tag{9.2}$$

In fact, if (x, y) satisfies (9.2), then $\left(\dfrac{p+1}{2} - x, \dfrac{q+1}{2} - y\right)$ satisfies (9.2) by verifying the inequalities in (9.2). This gives a pairing of lattice points in $ABCDEF$. However, $(x, y) = \left(\dfrac{p+1}{2} - x, \dfrac{q+1}{2} - y\right)$ is a lattice point if and only if $q \equiv p \equiv 3 \pmod 4$. ■

Q.E.D.

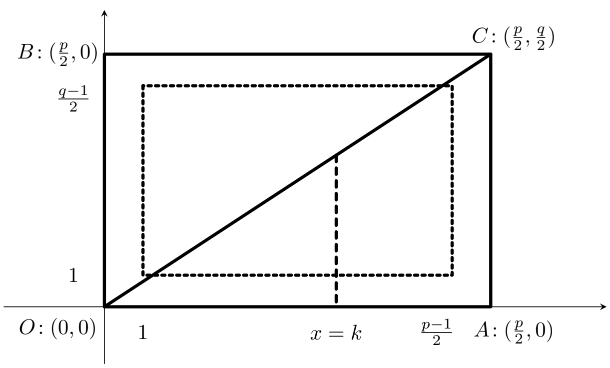
Proof (Alternative)

Lemma 1: (Corollary of Gauss's Lemma) If a is odd, then $\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2}[ka/p]}$.

By *Lemma 1*, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2}[kq/p] + \sum_{k=1}^{(q-1)/2}[kp/q]}$, thus proving

$$\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right] + \sum_{k=1}^{(q-1)/2}\left[\frac{kp}{q}\right] = \frac{p-1}{2}\frac{q-1}{2}$$

completes the proof. Consider the following figure.



Clearly, there are $\frac{p-1}{2}\frac{q-1}{2}$ lattice points inside $OACB$, and there are no lattice points on OC (proof by contradiction).

For all k s.t. $1 \le k \le \frac{p-1}{2}$, consider $x = k$ between OA and OC. It contains $[kq/p]$ lattice points, namely $(k, 1), (k, 2), \cdots, (k, [kq/p])$. Therefore, there are $\sum_{k=1}^{(p-1)/2}[kq/p]$ lattice points inside $\triangle OAC$. WLOG, there are $\sum_{k=1}^{(q-1)/2}[kp/q]$ lattice points inside $\triangle OBC$.

Hence by the number of lattice points $\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right] + \sum_{k=1}^{(q-1)/2}\left[\frac{kp}{q}\right] = \frac{p-1}{2}\frac{q-1}{2}$, and thus

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

Proof of Lemma 1: Let m denotes the number of integers with negative least residue described in Gauss's Lemma. By Euclid's Division Lemma, for all $1 \le k \le (p-1)/2$, we have $ka = pq_k + r_k$, where $q_k = [ka/p]$. Let $\sum_i a_i$ and $\sum_j b_j$ denotes the sum of r_k's whose least residue is less than, greater than $p/2$, respectively, then

$$\sum_{k=1}^{(p-1)/2} ka = p\sum_{k=1}^{(p-1)/2} q_k + \sum_{k=1}^{(p-1)/2} r_k = p\sum_{k=1}^{(p-1)/2} q_k + \sum_{i=1}^{r} a_i + \sum_{j=1}^{s} b_j$$

$$\frac{p^2-1}{8}a = \sum_{k=1}^{(p-1)/2} q_k + \sum_{i=1}^{r} a_i + \sum_{j=1}^{s}(p - b_j) - mp + 2\sum_{j=1}^{s} b_j$$

$$\frac{p^2-1}{8}a = p\sum_{k=1}^{(p-1)/2} q_k + \frac{p^2-1}{8} - mp + 2\sum_{j=1}^{s} b_j$$

where the last equality holds because $\sum_{i=1}^{r} a_i + \sum_{j=1}^{s}(p-b_j)$ is equivalent to $\sum_k |\mathrm{LR}(ka)|$ and is thus $\sum_k 1$. Taking module 2 of the above equality yields

$$\frac{p^2-1}{8} \equiv \sum_{k=1}^{(p-1)/2} q_k + \frac{p^2-1}{8} - m \pmod 2$$
$$m \equiv \sum_{k=1}^{(p-1)/2} q_k = \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] \pmod 2$$

and the result holds directly by Gauss's Lemma.

Q.E.D.

9.4 Application of Quadratic Reciprocity

Theorem 9.6

If p is an odd prime and $\gcd(a,p)=1$, then the congruence $x^2 \equiv a \pmod{p^n}$ has a solution if and only if $\left(\frac{a}{p}\right) = 1$.

Proof ($\Rightarrow$) If $x^2 \equiv a \pmod{p^n}$, then $x^2 \equiv a \pmod p$, so a is a quadratic residue, namely $\left(\frac{a}{p}\right) = 1$.

($\Leftarrow$) Suppose $\left(\frac{a}{p}\right) = 1$. We proceed by induction on n. The base case $n=1$ is trivial by the definition of Legendre symbol. Assume x_0 is a solution to $x_0^2 \equiv a \pmod{p^n}$. We want to find $k \in \mathbb{Z}$ such that

$$(x_0 + kp^n)^2 \equiv a \pmod{p^{n+1}} \tag{9.3}$$

Note that

$$(x_0+kp^n)^2 \equiv x_0^2 + 2x_0kp^n + k^2p^{2n} \equiv x_0^2 + 2x_0kp^n \pmod{p^{n+1}}$$

By inductive hypothesis, there exists $m \in \mathbb{Z}$ such that $x_0^2 - a = mp^n$. Then (9.3) is equivalent to $p^{n+1} \mid p^n(m + 2x_0k)$, namely $p \mid (m+2x_0k)$. Since $\gcd(p, 2x_0) = 1$, the linear congruence has solution. Hence the desired k exists and thus $x^2 \equiv a \pmod{p^n}$ has a solution.

Q.E.D.

9.5 Sums of Two Squares

Theorem 11.1 (Fermat)

Let p be an odd prime, there exist integers $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$.

Proof ($\Rightarrow$) For any $x \in \mathbb{Z}$, $x^2 \equiv 0$ or $1 \pmod 4$. Thus $x^2 + y^2 \equiv 0$ or 1 or $2 \pmod 4$. Since p is odd, $p = x^2 + y^2 \equiv 1 \pmod 4$.

($\Leftarrow$) Suppose $p \equiv 1 \pmod 4$. Since $\left(\frac{-1}{p}\right) = 1$, there exists $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \pmod p$. Let $k \in \mathbb{Z}_{>0}$ be integer such that $k^2 < p < (k+1)^2$ (i.e., $k = [\sqrt{q}]$). Consider integers of the form $a + bx$, where $0 \le a, b \le k$. By the pigeonhole principle, there exists two different pairs (a,b) and (a',b') such that $a + bx \equiv a' + b'x \pmod p$. Then $a - a' \equiv (b'-b)x \pmod p$, thus squaring both sides yields

$$(a-a')^2 \equiv -(b'-b)^2 \pmod{p}.$$

We have $p \mid (a-a')^2 + (b'-b)^2$. Since $0 < (a-a')^2 + (b'-b)^2 \leq 2k^2 < 2p$, then $(a-a')^2 + (b'-b)^2 = p$.

Q.E.D.