Number Theory

Number theory is concerned with divisibility, prime numbers, congruences, and pattern in whole numbers and integers. It is known as the “Queen of Mathematics” (Gauss). Number theory plays a central role in modern applications such as cryptography, coding theory, computer security, music, authenticators, error codes, and more.

Divisibility

We will say that a divides b, denoted $a \mid b$, if and only if there exists an integer d such that $a \cdot d = b$. If a does not divide b, then we will write $a \nmid b$.

$$2 \mid 6, \quad -5 \mid 50, \quad 4 \nmid 2$$

- If $a \mid b$ and $b \mid c$, then $a \mid c$.

  Proof. Suppose $a \mid b$ and $b \mid c$. By definition, $b = m \cdot a$ and $c = n \cdot b$.

  $$\begin{aligned} c &= n \cdot b \\ c &= n \cdot (m \cdot a) \\ c &= (n \cdot m) \cdot a \quad \text{let } x = n \cdot m,\ n \in \mathbb{Z} \\ c &= x \cdot a \end{aligned}$$

  By definition, $a \mid c$. □

- If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
- If $a \mid b$ and $a \mid c$, then $a \mid (m \cdot b + n \cdot c)$ for any integers m and n
- If $d \mid a$, then $d \mid (c \cdot a)$ for any integer c

Example

Is it possible to have 100 coins, made up of p pennies, d dimes, and q quarters, be worth exactly, \$5.00?

First, assume there is a solution. Then we have:

$$p + d + q = 100$$

$$p + 10 \cdot d + 25 \cdot q = 500$$

Subtracting these equations gives us:

$$(p + 10 \cdot d + 25 \cdot q) - (p + d + q) = 500 - 100$$

$$9 \cdot d + 24 \cdot q = 400$$

Since $3 \mid 9$ and $3 \mid 24$, we have that:

$$3 \mid (9 \cdot d + 24 \cdot q)$$

That is, $3 \mid 400$, but $3 \nmid 400$. This is a contradiction. Having \$5.00 with 100 pennies, dimes and quarters is impossible.

Greatest Common Divisor (GCD)

We say that d is the greatest common divisor of a and b, $d = (a, b) = \gcd(a, b)$ if and only if $d \mid a$ and $d \mid b$, and if $c \mid a$ and $c \mid b$, then $c \leq d$.

$$(2, 6) = 2, \quad (3, 4) = 1, \quad (7, 0) = 7$$

If $(a, b) = 1$, then we will say that a and b are relatively prime.

Theorem : (1.1)

If $(a, b) = d$, then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof. Suppose that $d = (a, b)$ and that $c = \left(\frac{a}{d}, \frac{b}{d}\right)$. Then, there exists integers q and r such that:

$$c \cdot q = \frac{a}{d} \quad \text{and} \quad c \cdot r = \frac{b}{d}$$

By rearranging these equations, we have that:

$$(c \cdot d) \cdot q = a \quad \text{and} \quad (c \cdot d) \cdot r = b$$

This shows that cd is a common divisor of a and b, so

$$1 \leq cd \leq (a, b) = d$$

Since d is positive, this gives $c = 1$ as desired. □

Theorem : Division Algorithm (1.2)

Given positive integers a and b, $b \neq 0$, there exists unique integers q and r, with $0 \leq r < b$, such that:

$$a = b \cdot q + r$$

Proof. Consider the set of integers:

$$\{a, a - b, a - 2b, a - 3b, \dots\}$$

From this set, let $r = a - qb$ be the smallest non-negative integer. It remains to show that q and r and unique. Suppose that there are integers q_1 and r_1 such that:

$$a = bq + r = bq_1 + r_1$$

By subtracting the two equations, we have that:

$$b\,(q - q_1) + (r - r_1) = 0$$

Since $b \mid 0$ and $b \mid (b\,(q - q_1))$, we have that $b \mid (r - r_1)$. However, $-b < r - r_1 < b$, therefore, we have that $r = r_1$. Substituting this into $0 = b\,(q - q_1) + (r - r_1)$ gives us that $q = q_1$. Therefore, q and r are unique. □

The Euclidean Algorithm

Lemma : (1.3)

If $a = bq + r$, then $(a, b) = (b, r)$.

Proof. Let $d = (a, b)$, that is $d \mid a$ and $d \mid b$. From the equation $a = bq + r$, it follows that $d \mid r$. Thus, d is a common divisor of b and r.

Suppose c is any common divisor of b and r. We know that $c \mid b$ and $c \mid r$, so it follows from $a = bq + r$ that $c \mid a$. Thus, c is a common divisor of a and b, and hence $c \leq d$. Therefore, by definition, d is the greatest common divisor of b and r.

So, we have that $(a, b) = d = (b, r)$ as desired. □

Example

Find the greatest common divisor of 70 and 21.

By the Division Algorithm, we have that:

$$70 = 3 \cdot 21 + 7$$

Therefore, by Lemma 1.3,

$$(70, 21) = (21, 7) = 7$$

Theorem : The Euclidean Algorithm

If a and b are positive integers, $b \neq 0$ and

$$\begin{aligned} a &= bq + r, & 0 &\leq r < b \\ b &= rq_1 + r_1, & 0 &\leq r_1 < r \\ r &= r_1q_2 + r_2 & 0 &\leq r_2 < r_1 \\ &\vdots \end{aligned}$$

Then for k large enough, say $k = t$, we have that $r_{t-1} = r_tq_{t+1}$ and $(a, b) = r_t$.

Proof. The sequence of non-negative integers must end

$$b > r > r_1 > r_2 > \cdots \geq 0$$

Eventually, one of the remainders will be zero, suppose it is r_{t+1}. Then we have that $r_{t-1} = r_tq_{t+1}$. Applying Lemma 1.3 repeatedly, we have

$$(a, b) = (b, r) = (r, r_1) = (r_1, r_2) = \cdots = (r_{t-1}, r_t) = r_t$$

If either a or b is negative, we can use that

$$(a, b) = (-a, b) = (a, -b) = (-a, -b)$$

□

Example

Apply the Euclidean Algorithm to calculate $(662, 414)$.

By applying the Division Algorithm, we have that

$$\begin{aligned} 662 &= 1 \cdot 414 + 248 \\ 414 &= 1 \cdot 248 + 166 \\ 248 &= 1 \cdot 166 + 82 \\ 166 &= 2 \cdot 82 + 2 \\ 82 &= 41 \cdot 2 \end{aligned}$$

Thus, by the Euclidean Algorithm, we have that $(662, 414) = 2$.

Example

Apply the Euclidean Algorithm to calculate $(343, 280)$.

By applying the Division Algorithm, we have that

$$\begin{aligned} 343 &= 1 \cdot 280 + 63 \\ 280 &= 4 \cdot 63 + 28 \\ 63 &= 2 \cdot 28 + 7 \\ 28 &= 4 \cdot 7 \end{aligned}$$

Thus, by the Euclidean Algorithm, we have that $(343, 280) = 7$.

Theorem : (1.4)

If $(a, b) = d$, then there are integers x and y such that

$$ax + by = d$$

Example

Find integers x and y such that $343x + 280y = 7$.

By working the Euclidean Algorithm backwards, we have that

$$\begin{aligned} 7 &= 63 - 2 \cdot 28 \\ 7 &= 63 - 2 \cdot (280 - 4 \cdot 63) \\ 7 &= 9 \cdot 63 - 2 \cdot 280 \\ 7 &= 9 \cdot (343 - 1 \cdot 280) - 2 \cdot 280 \\ 7 &= 9 \cdot 343 - 11 \cdot 280 \end{aligned}$$

Therefore, the integers are $x = 9$, and $y = -11$.

Corollary : (1.1)

If $d \mid (ab)$ and $(d, a) = 1$, then $d \mid b$.

Proof. From Theorem 1.4, we have that there are integers x and y such that

$$dx + ay = 1$$

$$d\,(bx) + (ab)\,y = b$$

Since $d \mid (bx)$ and since $d \mid (ab)$ by assumption, we have that $d \mid b$. □

Corollary : (1.2)

Let $(a, b) = d$, and suppose that $c \mid a$ and $c \mid b$, then $c \mid d$.

Proof. From Theorem 4, we have that there are integers x and y such that

$$ax + by = d$$

Since $c \mid (ax)$ and $c \mid (by)$, we have that $c \mid d$. □

Corollary : (1.3)

If $a \mid m$, $b \mid m$, and $(a, b) = 1$, then $(ab) \mid m$.

Proof. There is an integer q such that $m = bq$. Since $a \mid m$ and $(a, b) = 1$, Corollary 1.1 says that $a \mid q$. Therefore, there is an integer r such that $q = ar$. Thus, we have that $m = bq = bar$. This shows $(ab) \mid m$. □

Prime Numbers

A prime number is an integer that is greater than 1 and has no positive divisors other than 1 and itself.

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad \ldots$$

An integer that is greater than 1 but is not prime is called composite.

$$4, \quad 15, \quad 77, \quad 120, \quad \ldots$$

We call 1 neither a prime nor a composite number. Including it among primes would make the statement of the Fundamental Theorem of Arithmetic inconvenient. Therefore, we call 1 a unit. The primes can be used to build the entire system of positive integers. The first two lemmas will show that every positive integer can be written as a product of primes. Later, we will prove the uniqueness of the representation.

Lemma : (2.1)

Every integer $n > 1$ is divisible by a prime number.

Proof. The set of divisors of n that are greater than 1 and less than n is either empty or non-empty.

If it is empty, then n is a prime number and thus has a prime divisor.

If it is nonempty, then the least integer principle says that it has a smallest element, call it d. If d had a divisor greater than 1 and less than d, then so would n. But this is impossible because d was the smallest such divisor. (Suppose $c \mid d$ and $1 < c < d$. $c \mid d$ and $d \mid n$, so $c \mid n$, but $c < d$).

Therefore, d is prime, and n has a prime divisor, namely d. In both cases, n is divisible by a prime number. $\square$

Lemma : (2.2)

Every integer $n > 1$ can be written as a product of primes.

Proof. From Lemma 2.1, we know that there is a prime p_1 such that $p_1 \mid n$. By the definition of divides, we get that $n = p_1 n_1$, where $1 \leq n_1 < n$.

If $n_1 = 1$, then $n = p_1$ is an expression as a product of primes.

If $n > 1$, then from Lemma 2.1, there is a prime that divides n_1. By applying Lemma 2.1 repeatedly, we will find some n_i equal to 1 because the sequence of n_i is strictly decreasing but larger than 1. $n > n_1 > n_2 > \cdots \geq 1$. For some k, we will have $n_k = 1$, in which case, $n = p_1 p_2 \ldots p_k$ is an expression of n as a product of primes. $\square$

Example

Write the prime decompositions for 60 and 960.

$$\begin{aligned} 60 &= 30 \cdot 2 \\ &= 15 \cdot 2 \cdot 2 \\ &= 5 \cdot 3 \cdot 2 \cdot 2 \end{aligned}$$

$$\begin{aligned} 960 &= 480 \cdot 2 \\ &= 240 \cdot 2 \cdot 2 \\ &= 120 \cdot 2 \cdot 2 \cdot 2 \\ &= 60 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \\ &= 5 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \end{aligned}$$

Theorem

There are infinitely many primes.

Proof. Suppose there are finitely many primes. Denote them by:

$$p_1, p_2, \ldots, p_r$$

Consider the integer

$$n = p_1 p_2 \ldots p_r + 1$$

From Lemma 2.1, we have that n is divisible by a prime, and since there are only finitely many primes, it must be one of $p_1, p_2, \ldots, p_r$. Suppose that it is p_k. Then, since $p_k \mid n$ and $p_k \mid p_1 p_2 \ldots p_r$, we get that $p_k \mid 1$, a contradiction. □

Lemma : (2.5)

If $p \mid (ab)$, then $p \mid a$ or $p \mid b$.

Proof. Since p is prime, either $(p, a) = p$ or $(p, a) = 1$. In the first case, $p \mid a$ and we are done. In the second case, by Corollary 1.1, $p \mid b$, and we are done. □

Lemma : (2.6)

If $p \mid (a_1 a_2 \ldots a_k)$, then $p \mid a_i$ for some i, $i = 1, 2, \ldots, k$.

Proof. If $k = 1$, then Lemma 2.6 is true by inspection. If $k = 2$, then Lemma 2.5 shows that Lemma 2.6 is true.

Suppose that Lemma 2.6 is true for $k = r$. Suppose that $p \mid (a_1 a_2 \ldots a_{r+1})$, that is, $p \mid (a_1 a_2 \ldots a_r)\, a_{r+1}$. Then, Lemma 2.5 gives us that $p \mid a_{r+1}$ or $p \mid (a_1 a_2 \ldots a_r)$.

In the first case, $p \mid a_{r+1}$. In the second case, by the induction step, $p \mid a_i$ for some $1 \leq i \leq r$. In either case, $p \mid a_i$ for some i, $i = 1, 2, \ldots, r + 1$.

Therefore, if $p \mid (a_1 a_2 \ldots a_k)$, then $p \mid a_i$ for some i, $i = 1, 2, \ldots, k$. □

Lemma : (2.7)

If $q_1, q_2, \ldots, q_n$ are primes, and $p \mid (q_1 q_2 \ldots q_k)$, then $p = q_k$ for some k.

Proof. From Lemma 2.7, we know that $p \mid q_k$ for some k. However, the only divisors of q_k are q_k and 1. Also, p is not 1 since p is a prime. Therefore, we have that $p = q_k$. □

Theorem : Fundamental Theorem of Arithmetic

Any positive integer can be written as a product of primes in one and only one way.

Proof. From Lemma 2.2, any integer $n > 1$ can be written as a product of primes. Suppose that there are two representations

$$n = p_1 p_2 \ldots p_m \quad \text{and} \quad n = q_1 q_2 \ldots q_r$$

We must show that the same primes appear in each product and that they appear the same number of times. Since $p_1 \mid n$, we have that $p_1 \mid (q_1 q_2 \ldots q_r)$. From Lemma 2.7, it follows that $p_1 = q_i$ for some i. If we divide by the common factor we have that

$$p_2 p_3 \ldots p_m = q_1 q_2 \ldots q_{t-1} q_{t+1} \ldots q_r$$

Applying Lemma 2.7 repeatedly, we find that each p is a q. Similarly, by interchanging p and q, we find that each q is a p.

Therefore, $p_1, p_2, \ldots, p_m$ are a rearrangement of $q_1, q_2, \ldots, q_r$, and the two factorizations differ only in the order of the factors. □

Diophantine Equations

Equations where we look for solutions in a restricted class of numbers are called Diophantine equations.

$$x^2 + y^2 = z^2, \qquad x^4 + y^4 = z^4$$

These equations have infinitely many solutions in the reals, but the second equation has no nontrivial integer solutions.

We will consider the linear Diophantine equation,

$$ax + by = c, \quad a, b, c \in \mathbb{Z}$$

We want solutions where $x, y \in \mathbb{Z}$.

Example

Are there any solutions in the integers to the equation:

$$7x + 21y = 6$$

Suppose that there is a solution. Since $7 \mid 7x$ and $7 \mid 21y$, if there is a solution, $7 \mid 6$. This is a contradiction since $7 \nmid 6$. Therefore, this has no solutions in $\mathbb{Z}$.

Lemma : (3.1)

If x_0, y_0 is a solution of $ax + by = c$, then for any integer t,

$$\begin{aligned} x &= x_0 + bt \\ y &= y_0 - at \end{aligned}$$

is also a solution.

Proof. Supposing that $ax_0 + by_0 = c$,

$$\begin{aligned} ax + by &= a\left(x_0 + bt\right) + b\left(y_0 - at\right) \\ &= ax_0 + abt + by_0 - abt \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

Therefore, $x = x_0 + bt$ and $y = y_0 - at$ satisfy the equation. □

Example

Find the integer solutions of the equation:

$$5x + 6y = 17$$

By inspection, we see that one solution is $x = 1$, $y = 2$. From Lemma 3.1, it follows that $x = 1 + 6t$ and $y = 2 - 5t$ are also solutions, where $t \in \mathbb{Z}$.

Lemma : (3.2)

Consider the equation $ax + by = c$. If $(a, b) \mid c$, then $ax + by = c$ has a solution. If $(a, b) \nmid c$, then $ax + by = c$ has no solutions.

Proof. Suppose that there are integers x_0 and y_0 such that $ax_0 + by_0 = c$. Consider $(a, b) = d$, $d \mid a$ and $d \mid b$. Then, $d \mid (ax_0)$ and $d \mid (by_0)$ so $d \mid c$. Therefore, $(a, b) \mid c$ as wanted.

Conversely, suppose that $(a, b) \mid c$. Then, $c = m\,(a, b)$ for some m. From Theorem 1.4, we know that there are integers r and s such that:

$$\begin{aligned} ar + bs &= (a, b) \\ a\,(rm) + b\,(sm) &= m\,(a, b) \\ a\,(rm) + b\,(sm) &= c \end{aligned}$$

Therefore, $x = rm$ and $y = sm$ is a solution. □

Example

Which of the following Linear Diophantine equations has no solutions?

$$14x + 34y = 90$$

$$14x + 36y = 93$$

---

1. $14x + 34y = 90$
$$(14, 34) = 2$$
$$2 \mid 90$$
By Lemma 3.2, this has solutions.
2. $14x + 36y = 93$
$$(14, 36) = 2$$
$$2 \nmid 93$$
By Lemma 3.2, this has no solutions.

Lemma : (3.3)

Consider the equation:

$$ax + by = c$$

Suppose that $(a, b) = 1$ and (x_0, y_0) is a solution, then:

$$x = x_0 + bt, \quad y = y_0 - at$$

provides all of the solutions.

Proof. Consider $ax + by = c$. Suppose $(a, b) = 1$, we have $1 \mid c$, therefore, there exists a solution (x_0, y_0).

Suppose that (r, s) is a solution, then show

$$r = x_0 + bt, \quad s = y_0 - at$$

Consider the equations:

$$\begin{aligned} ax_0 + by_0 &= c \\ ar + bs &= c \end{aligned}$$

Then,

$$\begin{aligned} ax_0 + by_0 - (ar + bs) &= c - c \\ a(x_0 - r) + b(y_0 - s) &= 0 \end{aligned}$$

$a \mid a(x_0 - r)$ and $a \mid 0$, so $a \mid b(y_0 - s)$. Since $(a, b) = 1$, Corollary 1.1 tells us $a \mid (y_0 - s)$.

$$\begin{aligned} y_0 - s &= at \\ s &= y_0 - at \end{aligned}$$

Now, substitute this back into the equation above.

$$\begin{aligned} a(x_0 - r) + b(y_0 - s) &= 0 \\ a(x_0 - r) + b(y_0 - (y_0 - at)) &= 0 \\ a(x_0 - r) + b(at) &= 0 \\ (x_0 - r) + bt &= 0 \\ x_0 + bt &= r \end{aligned}$$

So we have that:

$$s = y_0 - at, \quad r = x_0 + bt$$

□

Theorem : (3.1)

Consider $ax + by = c$, if $(a, b) \mid c$, then there are infinitely many solutions of the form

$$x = x_0 + \frac{bt}{(a, b)}, \quad y = y_0 - \frac{at}{(a, b)}$$

Where x_0, y_0 is any solution, and $t \in \mathbb{Z}$.

Example

Find all integer solutions of $2x + 6y = 20$.

Notice that $x = 1$ and $y = 3$ is a particular solution. The greatest common divisor is $(2, 6) = 2$. By Theorem 3.1, the general solution is given by:

$$x = 1 + \frac{6}{2}t = 1 + 3t, \quad y = 3 - \frac{2}{2}t = 3 - t$$

Example

Find all integer solutions of $14x + 21y = 196$.

Notice that $x = 14$ and $y = 0$ is a particular solution. The greatest common divisor is $(14, 21) = 7$. By Theorem 3.1, the general solution is given by:

$$x = 14 + \frac{21}{7}t = 14 + 3t, \quad y = 0 - \frac{14}{7}t = -2t$$

Congruences and Linear Congruences

We say that a and b are congruent to each other modulo m,

$$a \equiv b \mod m$$

if $m \mid (a-b)$.

For example,

$$\begin{aligned} -2 &\equiv 5 \mod 7 &\quad -2-5 &= -7, \quad 7 \mid -7 \\ 10 &\equiv 6 \mod 6 &\quad 10-6 &= 4, \quad 4 \mid 4 \\ 10 &\equiv 2 \mod 4 &\quad 10-2 &= 8, \quad 4 \mid 8 \end{aligned}$$

Theorem : (4.1)

If $a \equiv b \mod m$, then there exists k such that $a = b + km$.

Proof. By definition, $m \mid (a-b)$. Then, $a - b = mk$ by divisibility. Therefore, $a = mk + b$. □

Theorem : (4.2)

There is a unique r, call this the least residue modulo m.

$$a \equiv r \mod m$$

$$r \in \{0, 1, 2, \ldots, m-2, m-1\}$$

Proof. By the division theorem with a, m, there are unique integers k and r such that:

$$a = km + r, \quad 0 \leq r < m$$

Thus, $a \equiv r \mod m$ by the previous theorem. □

Example

What is the residue of:

$$44 \mod 3, \qquad 44 \mod 4, \qquad 44 \mod 5$$

In the first case, $44 \equiv 2 \mod 3$

In the second case, $44 \equiv 0 \mod 3$

In the third case, $44 \equiv 4 \mod 5$.

Theorem : (4.3)

$a \equiv b \mod m$ if and only if they have the same remainder when divided by m.

Proof. Suppose a and b have the same remainder when divided by m.

$$a = q_1 m + r \qquad b = q_2 m + r$$

By the division algorithm,

$$\begin{aligned} a - b &= (q_1 m + r) - (q_2 m + r) \\ &= q_1 m - q_2 m \\ &= m\,(q_1 - q_2) \end{aligned}$$

Thus, $m \mid (a-b)$ by definition. Then, $a \equiv b \mod m$ by definition.

Now, suppose that $a \equiv b \mod m$. Then, $a \equiv b \equiv r \mod m$, where r is the least residue modulo m. Then, from Theorem 4.1, we have that:

$$a = q_1 m + r \quad \text{and} \quad b = q_2 m + r$$

For some integers q_1 and q_2, since $0 \leq r < m$. Thus, a and b have the same remainder when divided by m. □

Lemma : (4.1)

For integers a, b, c, d, we have that:

- $a \equiv a \mod m$
- If $a \equiv b \mod m$, then $b \equiv a \mod m$
- If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$
- If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a + c \equiv b + d \mod m$
- If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$

Theorem : (4.4)

This is listed as a lemma in the in-person notes.

Suppose $ab \equiv ac \mod m$, then if $(a, m) = 1$, then $b \equiv c \mod m$.

Proof. By the definition of congruence, $m \mid (ac - bc)$ or $m \mid c\,(a-b)$. From Theorem 1.5, this means that $m \mid (a-b)$ since $(m, c) = 1$. Therefore, by the definition of congruence, $a \equiv b \mod m$. □

Example

a) What values of x satisfy $2x \equiv 4 \mod 7$.
b) What values of x satisfy $2x \equiv 1 \mod 7$.

---

a) Since $(2, 7) = 1$, Theorem 4.4 gives us that $x \equiv 2 \mod 7$.
b) Note that $2x \equiv 1 \equiv 8 \mod 7$. Since $(2, 7) = 1$, Theorem 4.4 gives us that $x \equiv 4 \mod 7$.

Theorem : (4.5)

This is listed as a lemma in the in-person notes.

If $ac \equiv bc \mod m$ and $(c, m) = d$, then $a \equiv b \mod \frac{m}{d}$.

Proof. If $ac = bc \mod m$, then $m \mid c\,(a - b)$ and $\frac{m}{d} \mid \left(\frac{c}{d}\right)(a - b)$. Since we know that $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$, Theorem 1.5 gives us that $\frac{m}{d} \mid (a - b)$. Therefore, by the definition of congruence, $a \equiv b \mod \frac{m}{d}$ □

Example

Which x will satisfy $3x \equiv 15 \mod 9$?

By Theorem 4.5, we have that

$$\begin{aligned} 3x &\equiv 15 \mod 9 \\ x &\equiv 5 \mod 3 \\ x &\equiv 2 \mod 3 \end{aligned}$$

Linear Congruences

A linear congruence is of the form

$$ax \equiv b \mod m$$

This has a solution if and only if there are integers x and k such that

$$ax = b + km$$

$$\Leftrightarrow ax - km = b$$

These can be viewed as Diophantine equations.

If one integer satisfies $ax \equiv b \mod m$, then there are infinitely many.

The table below shows $5x \equiv 4 \mod 7$ has a solution of $x = 5$.

x	0	1	2	3	4	5	6
$5x$	0	5	3	1	6	4	2

Let $r \in \mathbb{Z}$, $y = x + rm$. Suppose $ax \equiv b \mod m$

$$\begin{aligned} ay &\equiv a(x + rm) \mod m \\ &\equiv ax + arm \mod m \\ &\equiv ax \mod m \\ &\equiv b \mod m \end{aligned}$$

The solutions of linear congruences are the solutions that are the least residues modulo m. Therefore, the only solution to $5x \equiv 4 \mod 7$ is $x = 5$.

The linear congruence $ax \equiv b \mod m$, may have no solutions, exactly one solution, or many solutions.

- $2x \equiv 1 \mod 5$ is satisfied by $x = 3$
- $2x \equiv 1 \mod 8$ has no solutions
- $2x \equiv 4 \mod 6$ has two solutions, $x = 2$, and $x = 5$.

Lemma : (5.1)

If $(a, m) \nmid b$, then $ax \equiv b \mod m$ has no solutions.

Proof. By contraposition, suppose there is a solution. Suppose that $ax \equiv b \mod m$. By the definition of congruence, $m \mid (ax - b)$. By divisibility, $ax - b = km$. Consider (a, m). $(a, m) \mid ax$, and $(a, m) \mid km$, thus, $(a, m) \mid b$. □

Lemma : (5.2)

If $(a, m) = 1$, then $ax \equiv b \mod m$ has exactly one solution.

Proof. Suppose that $(a, m) = 1$, we know there exists r and s such that:

$$ar + ms = 1$$

$$arb + msb = b$$

$$arb \mod m \equiv b \mod m$$

Let $x = rb$, then $ax \equiv b \mod m$.

Suppose p and q are solutions.

$$ap \equiv b \mod m \qquad aq \equiv b \mod m$$

$$ap \equiv aq \mod m$$

Since $(a, m) = 1$,

$$p \equiv q \mod m, \quad 0 \leq p < m, \quad 0 \leq q < m$$

$$m \mid (p - q) \qquad -m < p - q < m$$

Thus, $p = q$, so they are the same solution. Thus, the solution is unique. □

Example

How many solutions does each congruence have?
a) $3x \equiv 1 \mod 10$
b) $4x \equiv 1 \mod 10$
c) $5x \equiv 1 \mod 10$
d) $7x \equiv 1 \mod 10$

---

a) Since $(3, 10) = 1$, $3x \equiv 1 \mod 10$ has exactly one solution
b) Since $(4, 10) = 2$, and $2 \nmid 1$, $4x \equiv 1 \mod 10$ has no solutions
c) Since $(5, 10) = 5$, and $5 \nmid 1$, $5x \equiv 1 \mod 10$ has no solutions
d) Since $(7, 10) = 1$, $7x \equiv 1 \mod 10$ has exactly one solution.

Example

What is the solution of $14x \equiv 27 \mod 31$?

$(14, 31) = 1$, so there is one solution.

$$\begin{aligned} 14x &\equiv 27 \mod 31 \\ 7 \cdot 2 \cdot x &\equiv 27 \mod 31 \\ 7 \cdot 2 \cdot x &\equiv 58 \mod 31 \\ 7 \cdot x &\equiv 29 \mod 31 \\ 7 \cdot x &\equiv 60 \mod 31 \\ 7 \cdot x &\equiv 91 \mod 31 \\ x &\equiv 13 \mod 31 \end{aligned}$$

The equation $ax + by = c$ implies the two congruences:

$$ax \equiv c \mod b \quad \text{and} \quad by \equiv c \mod a$$

We can choose one equation, solve for the variable, and then substitute the result into the original equation to get all the solutions.

Example

Find all integer solutions of:

$$9x + 16y = 35$$

$$\begin{aligned} ax &\equiv c \mod b \\ 9x &\equiv 35 \mod 16 \\ 9x &\equiv 3 \mod 16 \\ 3x &\equiv 1 \mod 16 \\ 3x &\equiv 17 \mod 16 \\ 3x &\equiv 33 \mod 16 \\ x &\equiv 11 \mod 16 \end{aligned}$$

$$x = 11 + 16t$$

$$\begin{aligned} 9x + 16y &= 35 \\ 9\left(11 + 16t\right) + 16y &= 35 \\ 99 + 144t + 16y &= 35 \\ 16y &= -64 - 144t \\ y &= -4 - 9t \end{aligned}$$

Here, $(11, -4)$ is a particular solution.

Example

Find all integer solutions of:

$$9x + 10y = 11$$

$$\begin{aligned} by &\equiv c \mod a \\ 10y &\equiv 11 \mod 9 \\ 10y &\equiv 2 \mod 9 \\ 5y &\equiv 1 \mod 9 \\ 5y &\equiv 10 \mod 9 \\ y &\equiv 2 \mod 9 \end{aligned}$$

$$y = 2 + 9t$$

$$\begin{aligned} 9x + 10y &= 11 \\ 9x + 10\left(2 + 9t\right) &= 11 \\ 9x + 20 + 90t &= 11 \\ 9x &= -9 - 90t \\ x &= -1 - 10t \end{aligned}$$

Here, $(-1, 2)$ is a particular solution.

Linear Congruences

Lemma : (5.3)

Let $d = (a, m)$. If $d \mid b$, then $ax \equiv b \mod m$ has d solutions.

Proof. Suppose $(a, m) = d$ and $d \mid b$. Thus, $\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$. Note that $\left(\frac{a}{b}, \frac{m}{d}\right) = 1$ so this second congruence has a unique solution r.

Let r be a solution of the first / second congruence. Let s be a solution of $ax \equiv b \mod m$.

$$\begin{aligned} as &\equiv ar \mod m \\ s &\equiv r \mod \frac{m}{d} \qquad \text{from Theorem 4.5} \end{aligned}$$

By the definition of congruence, $\frac{m}{d} \mid (s - r)$. $s - r = k\left(\frac{m}{d}\right)$, so $s = r + k\left(\frac{m}{d}\right), 0 \le k \le d - 1$. We also have that $r < \frac{m}{d}$ from the second congruence equation.

$$\begin{aligned} s &= r + k\left(\frac{m}{d}\right) \\ &< \frac{m}{d} + (d-1)\left(\frac{m}{d}\right) \\ &= \frac{m}{d} + m - \frac{m}{d} \\ s &< m \end{aligned}$$

So, $s = r + k\left(\frac{m}{d}\right), 0 \le k \le d - 1$ are all of the solutions of the original equation. □

Example

Find all the solutions of $5x \equiv 10 \mod 15$.

$(5, 15) = 5$ and $5 \mid 10$, so there should be 5 equations.

$$x \equiv 5 \mod 3$$

So, the 5 solutions are: $x = 2, x = 5, x = 8, x = 11, x = 14$.

Example

Find all the solutions of $9x \equiv 15 \mod 24$.

$(9, 24) = 3$ and $3 \mid 15$, so there should be 3 solutions.

$$\begin{aligned} 3x &\equiv 5 \mod 8 \\ 3x &\equiv 13 \mod 8 \\ 3x &\equiv 21 \mod 8 \\ x &\equiv 7 \mod 8 \end{aligned}$$

So, the 3 solutions are: $x = 7, x = 15, x = 23$.

Example

Find x such that $x \equiv 1 \mod 3$, $x \equiv 2 \mod 5$, and $x \equiv 3 \mod 7$.

The first congruence gives $x = 1 + 3k_1$, now plug this into the second congruence.

$$\begin{aligned} x &\equiv 2 \mod 5 \\ 1 + 3k_1 &\equiv 2 \mod 5 \\ 3k_1 &\equiv 1 \mod 5 \\ 3k_1 &\equiv 6 \mod 5 \\ k_1 &\equiv 2 \mod 5 \end{aligned}$$

This congruence gives $k_1 = 2 + 5k_2$.

$$\begin{aligned} x &= 1 + 3k_1 \\ &= 1 + 3\left(2 + 5k_2\right) \\ &= 1 + 6 + 15k_2 \\ &= 7 + 15k_2 \end{aligned}$$

Plugging this into the third congruence gives:

$$\begin{aligned} x &\equiv 3 \mod 7 \\ 7 + 15k_2 &\equiv 3 \mod 7 \\ 15k_2 &\equiv 3 \mod 7 \\ 5k_2 &\equiv 1 \mod 7 \\ 5k_2 &\equiv 8 \mod 7 \\ 5k_2 &\equiv 15 \mod 7 \\ k_2 &\equiv 3 \mod 7 \end{aligned}$$

This congruence gives us $k_2 = 3 + 7k_3$.

$$\begin{aligned} x &= 7 + 15k_2 \\ &= 7 + 15\left(3 + 7k_3\right) \\ &= 7 + 45 + 105k_3 \\ &= 52 + 105k_3 \end{aligned}$$

This means, $x \equiv 52 \mod 105$, and that $x = 52$ is the unique solution.

Theorem : The Chinese Remainder Theorem

The linear congruence system

$$x \equiv a_1 \mod m_1, \qquad x \equiv a_2 \mod m_2, \quad \dots \quad , x = a_n \mod m_n$$

has a unique solution modulo $m_1 \times m_2 \times \cdots \times m_n$ if for each (m_i, m_j), where $i \neq j$, $(m_i, m_j) = 1$.

Proof. The result is trivial when $n = 1$. If $n = 2$, then

$$x \equiv a_1 \mod m_1 \quad \text{and} \quad x \equiv a_2 \mod m_2$$

where m_1 and m_2 are relatively prime. From the first congruence, we have that $x = a_1 + k_1 m_1$

$$\begin{aligned} x &\equiv a_2 \mod m_2 \\ a_1 + k_1 m_1 &\equiv a_2 \mod m_2 \\ k_1 m_1 &\equiv a_2 - a_1 \mod m_2 \end{aligned}$$

k_1 is the variable, and since (m_1, m_2), there is a unique solution we will call t. Note, $k_1 = t + k_2 m_2$

$$\begin{aligned} x &= a_1 + k_1 m_1 \\ &= a_1 + (t + k_2 m_2)(m_1) \\ &= a_1 + t m_1 + k_2 m_2 m_1 \\ &\equiv a_1 + t m_1 \mod m_1 m_2 \end{aligned}$$

satisfies both equations.

Suppose the result holds for $n - 1$ equations:

$$x \equiv a_1 \mod m_1 \quad \dots \quad x \equiv a_{n-1} \mod m_{n-1}$$

Has a solution $x \equiv s \mod m_1 \times \cdots \times m_{n-1}$. Now suppose you have another congruence, $x \equiv a_n \mod m_n$. This creates a system of two congruences which we already proved has a unique solution modulo $(m_1 \times \cdots \times m_{n-1}) \cdot (m_n)$.

Now, for uniqueness. Suppose r and s are solutions.

$$r \equiv s \mod m_1, \quad \dots, \quad r \equiv s m_k$$

$$\begin{gathered} r - s \equiv 0 \mod m_1 \quad \dots, \quad r - s \equiv 0 \mod m_k \\ m_1 \mid (r - s), \quad m_2 \mid (r - s), \quad \dots, \quad m_k \mid (r - s) \end{gathered}$$

Thus, $m_1 \times m_2 \times \cdots \times m_k \mid (r - s)$ since $(m_i, m_j), i \neq k$

$$0 \leq r < m_1 \times m_2 \times \cdots \times m_k, \quad 0 \leq s < m_1 \times m_2 \times \cdots \times m_k$$

$$\begin{gathered} -m_1 \times m_2 \times \cdots \times m_k < r - s < m_1 \times m_2 \times \cdots \times m_k \\ r - s = 0 \Rightarrow r = s \end{gathered}$$

□

The Chinese Remainder Theorem is very efficient for computers. It is helpful in error correcting codes, signal processing, RSA algorithms, etc.

Fermat's Theorem

Lemma : (6.1)

If $(a, m) = 1$, then the least residues of

$$a, \quad 2a, \quad 3a, \quad \ldots, \quad (m-1)\,a \mod m$$

are given by

$$1, \quad 2, \quad 3, \quad \ldots, \quad m-1$$

in some order

Proof. Note that none of the $m-1$ numbers are congruent to $0 \mod m$

$$a, \quad 2a, \quad 3a, \quad \ldots, \quad (m-1)\,a \mod m$$

Hence, each of them is congruent ($\mod m$) to one of the numbers in

$$1, \quad 2, \quad 3, \quad \ldots, \quad m-1$$

Suppose that two of the integers are congruent modulo m

$$ra \equiv sa \mod m$$

Since $(a, n) = 1$, Theorem 4.4 gives us that

$$r \equiv s \mod m$$

Therefore, since r and s are least residues, it follows that $r = s$ □

Theorem : Fermat's Theorem (Little Theorem)

If p is a prime, and $(a, p) = 1$, then

$$a^{p-1} \equiv 1 \mod p$$

Proof. Lemma 6.1 says that if $(a, p) = 1$, then the least residues of

$$a, \quad 2a, \quad 3a, \quad \ldots, \quad (p-1)\,a \mod p$$

are a permutation of the set

$$1, \quad 2, \quad 3, \quad \ldots, \quad p-1$$

Hence, their products are congruent modulo p

$$a \times 2a \times 3a \times \cdots \times (p-1)\,a \equiv 1 \times 2 \times 3 \times \cdots \times (p-1) \mod p$$
$$a^{p-1}\,(p-1)! \equiv (p-1)! \mod p$$

Since p and $(p-1)!$ are relatively prime, the last congruence gives

$$a^{p-1} \equiv 1 \mod p$$

□

Example

Verify that $3^{16} \equiv 1 \mod 17$.

Note that we have the following components of 3^{16}

$$\begin{aligned} 3^3 &\equiv 27 \equiv 10 \mod 17 \\ 3^6 &\equiv \left(3^3\right)^2 \equiv 100 \equiv -2 \mod 17 \\ 3^{12} &\equiv \left(3^6\right)^2 \equiv 4 \mod 17 \end{aligned}$$

Therefore, for the second congruence, we have that

$$\begin{aligned} 3^{16} &\equiv 3^{12} \cdot 3^3 \cdot 3 \\ &\equiv 4 \cdot 10 \cdot 3 \\ &\equiv 1 \mod 17 \end{aligned}$$

Multiplicative Modular Inverses, denoted by a', $\bar{a}$ modulo m, is one such that

$$a \cdot a' \equiv 1 \mod m$$

In general, 1 and $(p-1)$ are there own inverses modulo p

Example

Find all multiplicative modular inverses modulo 7.

A table showing all a and their respective a' is shown below

a	1	2	3	4	5	6
a'	1	4	5	2	3	6

Example

Find all multiplicative modular inverses modulo 6.

A table showing all a and their respective a' is shown below

a	1	2	3	4	5
a'	1	DNE	DNE	DNE	5

Wilson's Theorem

Lemma : (6.2)

$$x^2 \equiv 1 \mod p$$

has exactly 2 solutions, 1 and $p-1$.

Proof. Let r be any solution of $x^2 \equiv 1 \mod p$. Then, it follows that $r^2 - 1 \equiv 0 \mod p$. Thus, by definition of congruence,

$$p \mid \left(r^2 - 1\right) \quad \text{so} \quad p \mid (r-1)(r+1)$$

Hence, $r + 1 \equiv 0 \mod p$, or $r - 1 \equiv 0 \mod p$. Since r is a least residue modulo p, we get that $r = p - 1$ or $r = 1$. □

Definition : Modular Multiplicative Inverse

The modular multiplicative inverse of an integer a is an integer a' such that

$$aa' \equiv 1 \mod m$$

If $(a, p) = 1$, we know that $ax \equiv 1 \mod p$ has exactly one solution. Thus, the inverses exist for each non-zero element.

Lemma : (6.3)

Let p be an odd prime, and let a' be the solution of $ax \equiv 1 \mod p$, for $a = 1, 2, \dots, p-1$. Then, $a' \equiv b' \mod p$ if and only if $a \equiv b \mod p$. Furthermore, $a \equiv a' \mod p$ if and only if $a = 1$ or $a = p - 1$.

Proof. Suppose that $a' \equiv b' \mod p$. Then, it follows that

$$b \equiv aa'b \equiv ab'b \equiv a \mod p$$

Conversely, suppose $a \equiv b \mod p$. Then it follows that

$$b' \equiv baa' \equiv b'ba \equiv a' \mod p$$

If $a = 1$ or $a = p - 1$, then

$$1 \cdot 1 \equiv 1 \mod p \quad \text{and} \quad (p-1)\cdot(p-1) \equiv 1 \mod p$$

Conversely, if $a \equiv a' \mod p$, then it follows that

$$1 \equiv aa' \mod p \equiv a^2 \mod p$$

From Lemma 6.2, this implies that $a = 1$ or $a = p - 1$ □

Theorem : Wilson's Theorem

p is a prime if and only if

$$(p-1)! \equiv -1 \mod p$$

Proof. From Lemma 6.3, we know that we can separate the numbers

$$2, \quad 3, \quad \ldots, \quad p-2$$

Into $(p-3)/2$ pairs such that each pair consists of an integer a and its associated multiplicative inverse a'. The product of the two integers in each pair is congruent to 1 modulo p, so it follows that

$$2 \times 3 \times \cdots \times (p-2) \equiv 1 \mod p$$

Therefore, it follows that

$$(p-1)! \equiv 1 \times 2 \times \cdots \times (p-2) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \mod p$$

Suppose that $n = ab$ for some integers a and b, with $a < n$. If $(n-1)! \equiv -1 \mod n$, then we have that

$$n \mid ((n-1)! + 1)$$

Since $a \mid n$, we also have that

$$a \mid ((n-1)! + 1)$$

Since $a \leq n-1$, one of the factors of $(n-1)!$ is a itself. This gives that $a \mid (n-1)!$ However, this implies that $a \mid 1$. The only positive divisors of n are 1 and n, and therefore n is a prime. □

Positive Divisors

Definition

Let n be a positive integer. Then, $d(n)$ is the number of positive divisors of n, including 1 and n. Also, $\sigma(n)$ is the sum of the positive divisors of n. That is,

$$d(n) = \sum_{d|n} 1 \quad \text{and} \quad \sigma(n) = \sum_{d|n} d$$

(Note $\sum_{d|n}$ means the sum over the positive divisors of n)

Notice that when p is prime, $d(p^n) = n + 1$, since the positive divisors of p^n are $1, p, p^2, \ldots, p^n$.

Theorem : (7.1)

If $p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ is the prime-power decomposition of n, then we have that

$$d(n) = d\left(p_1^{e_1}\right) \times d\left(p_2^{e_2}\right) \times \cdots \times d\left(p_k^{e_k}\right)$$

Proof. Consider the set

$$D = \left\{ p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k} : 0 \leq f_i \leq e_i \right\}$$

Notice that D is exactly the set of divisors of n. If $d \mid n$, then $d \in D$ (left as an exercise to show). By the unique factorization theorem, $d(n) = |D|$.

$$\begin{aligned} d(n) &= |D| \\ &= (e_1 + 1) \times (e_2 + 1) \times \cdots \times (e_r + 1) \\ &= d(p_1^{e_1}) \times d(p_2^{e_2}) \times \cdots \times d(p_r^{e_r}) \end{aligned}$$

□

Example

Calculate $d(540)$ and $d(6300)$.

$$\begin{aligned} 540 &= 2^2 \cdot 3^3 \cdot 5 \\ d(540) &= d(2^2) \cdot d(3^3) \cdot d(5) \\ &= 3 \cdot 4 \cdot 2 \\ d(540) &= 24 \end{aligned}$$

$$\begin{aligned} 6300 &= 2^2 \cdot 3^2 \cdot 5^2 \cdot 7 \\ d(6300) &= d(2^2) \cdot d(3^2) \cdot d(5^2) \cdot d(7) \\ &= 3 \cdot 3 \cdot 3 \cdot 2 \\ &= 54 \end{aligned}$$

Now, notice that $\sigma(p^n) = 1 + p + \cdots + p^n$ for all primes p. This is because the only factors of p^n are $1, p, \ldots, p^n$.

Lemma : (7.1)

If p and q are different primes, then

$$\sigma\left(p^e q^f\right) = \sigma\left(p^e\right) \cdot \sigma\left(q^f\right)$$

Proof. The divisors of $p^e q^f$ are given by

$$\begin{array}{ccccc} 1, & p, & p^2, & \ldots, & p^e \\ q, & pq, & p^2q, & \ldots, & p^eq \\ & & \vdots & & \\ q^f, & pq^f, & p^2q^f, & \ldots, & p^eq^f \end{array}$$

If we add across each row, we get that

$$\begin{aligned} \sigma\left(p^e q^f\right) &= \left(1 + p + \cdots + p^e\right) + \cdots + q^f\left(1 + p + \cdots + p^e\right) \\ &= \left(1 + p + \cdots + p^e\right)\left(1 + q + \cdots + q^f\right) \\ &= \sigma\left(p^e\right)\sigma\left(q^f\right) \end{aligned}$$

$\square$

Theorem : (7.2)

If $p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ is a prime-power decomposition of n, then

$$\sigma(n) = \sigma\left(p_1^{e_1}\right)\sigma\left(p_2^{e_2}\right)\ldots\sigma\left(p_k^{e_k}\right)$$

Proof. By Lemma 7.1, the theorem is true for $k = 2$. To prove by induction, suppose that the theorem is true for $k = r - 1$. We will show that this implies the theorem is true for $k = r$. Let

$$n = p_1^{e_1} p_2^{e_2} \ldots p_{r-1}^{e_{r-1}} p_r^{e_r} = N p_r^{e_r}, \qquad \text{let } N = p_1^{e_1} p_2^{e_2} \ldots p_{r-1}^{e_{r-1}}$$

Let $1, d_1, \ldots, d_t$ denote all the divisors of N, since $(N, p_r) = 1$, all the divisors of n are given by

$$\begin{array}{ccccc} 1, & d_1, & d_2, & \ldots, & d_t \\ p_r, & d_1p_r, & d_2p_r, & \ldots, & d_tp_r \\ & & \vdots & & \\ p_r^{e_r}, & d_1p_r^{e_r}, & d_2p_r^{e_r}, & \ldots, & d_tp_r^{e_r} \end{array}$$

Summing across the rows, we get that

$$\sigma(n) = \left(1 + d_1 + \cdots + d_t\right)\left(1 + p_r + \cdots + p_r^{e_r}\right) = \sigma(N)\,\sigma\left(p_r^{e_r}\right)$$

From the induction hypothesis, we get that

$$\sigma(n) = \sigma\left(p_1^{e_1}\right)\sigma\left(p_2^{e_2}\right)\ldots\sigma\left(p_{r-1}^{e_{r-1}}\right)\sigma\left(p_r^{e_r}\right)$$

$\square$

Example

Calculate $\sigma(540)$.

$$\begin{aligned} 540 &= 2^2 \cdot 3^3 \cdot 5 \\ \sigma(540) &= \sigma\left(2^2\right) \cdot \sigma\left(3^3\right) \cdot \sigma(5) \\ &= (1+2+4) \cdot (1+3+9+27) \cdot (1+5) \\ &= 7 \cdot 40 \cdot 6 \\ &= 1680 \end{aligned}$$

Definition : Multiplicative Functions

A function f, defined for the positive integers, is said to be multiplicative if and only if

$$(m, n) = 1 \quad \text{implies} \quad f(mn) = f(m) f(n)$$

Multiplicative Functions

Theorem : (7.3)

The function d is multiplicative.

Proof. Let m and n be relatively prime. Then, no prime that divides m can divide n and vice versa. Thus, if

$$m = p_1^{e_1} \dots p_k^{e_k} \quad \text{and} \quad n = q_1^{f_1} \dots q_r^{f_r}$$

are the prime power decompositions of m and n, then $p_i \neq q_j$. Then, the prime power decomposition of mn is given by

$$mn = p_1^{e_1} \dots p_k^{e_k} q_1^{f_1} \dots q_r^{f_r}$$

Applying Theorem 7.1, we have that

$$\begin{aligned} d(mn) &= d\left(p_1^{e_1} \dots p_k^{e_k} q_1^{f_1} \dots q_r^{f_r}\right) \\ &= d\left(p_1^{e_1}\right) \dots d\left(p_k^{e_k}\right) d\left(q_1^{f_1}\right) d\left(q_r^{f_r}\right) \\ &= d\left(p_1^{e_1} \dots p_k^{e_k}\right) d\left(q_1^{f_1} \dots q_r^{f_r}\right) \\ &= d(m)\, d(n) \end{aligned}$$

□

Theorem : (7.4)

The function σ is multiplicative.

Proof. Let m and n be relatively prime. Then, no prime that divides m can divide n and vice versa. Thus, if

$$m = p_1^{e_1} \dots p_k^{e_k} \quad \text{and} \quad n = q_1^{f_1} \dots q_r^{f_r}$$

are the prime power decompositions of m and n, then $p_i \neq q_j$. Then, the prime power decomposition of mn is given by

$$mn = p_1^{e_1} \dots p_k^{e_k} q_1^{f_1} \dots q_r^{f_r}$$

Applying Theorem 7.2, we have that

$$\begin{aligned} \sigma(mn) &= \sigma\left(p_1^{e_1} \dots p_k^{e_k} q_1^{f_1} \dots q_r^{f_r}\right) \\ &= \sigma\left(p_1^{e_1}\right) \dots \sigma\left(p_k^{e_k}\right) \sigma\left(q_1^{f_1}\right) \sigma\left(q_r^{f_r}\right) \\ &= \sigma\left(p_1^{e_1} \dots p_k^{e_k}\right) \sigma\left(q_1^{f_1} \dots q_r^{f_r}\right) \\ &= \sigma(m)\, \sigma(n) \end{aligned}$$

□

Theorem : (7.5)

If f is a multiplicative function and the prime power decomposition of n is $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, then

$$f(n) = f\left(p_1^{e_1}\right) f\left(p_2^{e_2}\right) \dots f\left(p_k^{e_k}\right)$$

Proof. Base case: $k = 1$: $f(n) = f\left(p_1^{e_1}\right)$. Assume the theorem is true for $k = r$. Now consider $k = r = 1$. Since $\left(p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}, p_{r+1}^{e_{r+1}}\right) = 1$, we have from the definition of a multiplicative function that

$$f\left(\left(p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}\right) p_{r+1}^{e_{r+1}}\right) = f\left(p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}\right) f\left(p_{r+1}^{e_{r+1}}\right)$$

From the induction hypothesis, the first factor is

$$f\left(p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}\right) = f\left(p_1^{e_1}\right) f\left(p_2^{e_2}\right) \ldots f\left(p_r^{e_r}\right)$$

Therefore, we have that

$$f\left(p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r} p_{r+1}^{e_{r+1}}\right) = f\left(p_1^{e_1}\right) f\left(p_2^{e_2}\right) \ldots f\left(p_r^{e_r}\right) f\left(p_{r+1}^{e_{r+1}}\right)$$

□

Perfect Numbers

Definition : Perfect Numbers

A number is called perfect if and only if it is equal to the sum of its positive divisors, excluding itself. That is, a number is perfect if and only if

$$\sigma(n) = 2n$$

Example

Is 6 a perfect number? Is 12 a perfect number?

---

6 is perfect since $6 = 1 + 2 + 3$.

12 is not perfect since $12 \neq 1 + 2 + 3 + 4 + 6$

Theorem : (8.1) (Euclid)

If $2^k - 1$ is prime, then $2^{k-1}\left(2^k - 1\right)$ is perfect.

Proof. Suppose that $n = \left(2^{k-1}\right)\left(2^k - 1\right)$. Since $2^k - 1$ is prime, we know that

$$\sigma\left(2^k - 1\right) = 1 + 2^k - 1 = 2^k$$

Also, notice that 2^{k-1} and $2^k - 1$ are relatively prime. Therefore, n is perfect since

$$\begin{aligned} \sigma(n) &= \sigma\left(2^{k-1}\left(2^k - 1\right)\right) \\ &= \sigma\left(2^{k-1}\right)\sigma\left(2^k - 1\right) \\ &= \left(2^k - 1\right) 2^k \\ &= 2\left(\left(2^k - 1\right) 2^{k-1}\right) \\ &= 2n \end{aligned}$$

□

Lemma

If k is composite, then $2^k - 1$ is composite.

Proof. Suppose $k = ab$, where $a \neq 1$, $b \neq 1$. Then,

$$\begin{aligned} 2^k - 1 &= 2^{ab} - 1 \\ &= (2^a - 1)\left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1\right) \end{aligned}$$

Therefore, 2^{k-1} can be prime only when k is prime. $\square$

Theorem : (8.2) (Euler)

If n is an even perfect number, then

$$n = 2^{p-1}\left(2^p - 1\right)$$

for some prime p and $2^p - 1$ is also prime.

Proof. If n is an even perfect number, $n = 2^e m$, where m is odd and $e \geq 1$. Since $\sigma(m) > m$, we can write $\sigma(m) = m + s$, with $s > 0$. That is, s is the sum of all the divisors of m that are less than m. Therefore, substituting this into the expression for $\sigma(n) = 2n$ gives us that

$$\begin{aligned} \sigma(n) &= 2n \\ \sigma\left(2^e m\right) &= 2n \\ \sigma\left(2^e\right)\sigma(m) &= 2n \\ \left(2^{e+1} - 1\right)(m + s) &= 2^{e+1} m \\ 2^{e+1} m - m + \left(2^{e+1} - 1\right)s &= 2^{e+1} m \\ \left(2^{e+1} - 1\right)s &= m \end{aligned}$$

This means that s is a divisor of m, and $s < m$. But s is the sum of all the divisors of m that are less than m. That is, s is the sum of a group of numbers that includes s. This is only possible if the group consists of one number alone. Therefore the set of divisors of m smaller than m must contain only one element, and that element must be 1. That is, $s = 1$, and hence $m = 2^{e+1} - 1$ is prime. The only numbers of this form that are prime must have $e + 1$ prime. Hence, $m = 2^p - 1$ for some prime $p = e + 1$. Therefore we have

$$\begin{aligned} n &= 2^e m \\ &= 2^e\left(2^{e+1} - 1\right) \\ &= 2^{p-1}\left(2^p - 1\right) \end{aligned}$$

$\square$

Midterm Practice

The entirety of this lecture was spent doing the practice problems for the midterm.

Euler's Theorem

Fermat's Theorem states that if p is prime, then

$$(a, p) = 1 \quad \text{implies} \quad a^{p-1} \equiv 1 \mod p$$

Question: If $(a, m) = 1$, is there a number t such that:

$$a^t \equiv 1 \mod m$$

Let's look at some tables of powers of a modulo m, where $(a, m) = 1$.

$m = 9$

a	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1
2	4	8	7	5	1
4	7	1	4	7	1
5	7	8	4	2	1
7	4	1	8	4	1
8	1	8	1	8	1

$m = 6$

a	a^2
1	1
5	1

$m = 10$

a	a^2	a^3	a^4
1	1	1	1
3	9	7	1
7	9	3	1
9	1	9	1

Definition : Euler's ϕ Function / Euler's Totient Function

If m is a positive integer, let $\phi(m)$ denote the number of positive integers less than or equal to m and relatively prime to m.

Lemma : (9.1)

If $(a, m) = 1$ and $r_1, r_2, \ldots, r_{\phi(m)}$ are the positive integers less than m and relatively prime to m, then the least residues modulo m of

$$ar_1, \quad ar_2, \quad \ldots, \quad ar_{\phi(m)}$$

are a permutation of

$$r_1, \quad r_2, \ldots, \quad r_{\phi(m)}$$

Proof. To show they are all different, suppose that for some $1 \leq i, j \leq \phi(m)$,

$$ar_i \equiv ar_j \mod m$$

Since $(a, m) = 1$, we can cancel a from both sides of the congruence

$$r_i \equiv r_j \mod m$$

Since r_i and r_j are the least residues modulo m, it follows that $r_i = r_j$.

To prove that all the numbers are relatively prime to m, suppose that p is a prime common divisor of ar_i and m for some $1 \leq i \leq \phi(m)$. Since p is prime, either $p \mid a$ or $p \mid r_i$. Thus, either p is a common divisor of a and m, or of r_i and m. But $(a, m = 1)$ and $(r_i, m) = 1$, so both cases are impossible. □

Example

Verify Lemma 9.1 if $m = 14$ and $a = 5$.

---

x	$5x$	$5x \mod 14$
1	5	5
3	15	1
5	25	11
9	45	3
11	55	13
13	65	9

Theorem : (9.1) / Euler's Theorem

If $(a, m) = 1$, then

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

Proof. From Lemma 9.1, we know that

$$r_1 r_2 \ldots r_{\phi(m)} \equiv (ar_1)(ar_2) \ldots \left(ar_{\phi(m)}\right) \mod m$$

$$r_1 r_2 \ldots r_{\phi(m)} \equiv a^{\phi(m)} r_1 r_2 \ldots r_{\phi(m)} \mod m$$

Since $(r_i, m) = 1$ for all $1 \leq i \leq \phi(m)$, we can cancel $r_1 r_2, \ldots r_{\phi(m)}$

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

□

How do we find $\phi(m)$? We will see later when we show that $\phi(m)$ is multiplicative.

Recall: Perfect numbers are n such that $\sigma(n) = 2n$. Even perfect numbers can be described as $n = 2^{p-1} \cdot (2^p - 1)$, where $2^p - 1$ is prime. We do not know if any odd perfect numbers exist, and numbers up to 10^{2200} have been checked. For even perfect numbers, we do not know if there are infinitely many Mersenne Primes, (primes of the form $2^p - 1$ where p is prime). It was originally conjectured that the only Mersenne Primes corresponded to the following values for p:

$$2, 3, 5, 7, 13, 17, 31, 67, 127, 257$$

In this list, 19, 61, 87, and 107 were missed, and 67 and 257 should not have been included. The largest Mersenne Prime currently known is:

$$2^{136279841-1} \qquad \text{This has 41,000,000+ digits}$$

Euler's Totient Function

Recall that $\phi(n)$ counts all the positive integers less than n, and relatively prime to n.

Lemma : (9.2)

For p prime, and all positive integers n,

$$\phi(p^n) = p^{n-1}(p-1)$$

Proof. The positive integers less than or equal to p^n that are not relatively prime to p^n are exactly the multiples of p.

$$1 \cdot p, \quad 2 \cdot p, \quad \ldots, \quad p^{n-1} \cdot p$$

Since there are p^n positive integers less than or equal to p^n, we have:

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

□

Lemma : (9.3)

If $(a, m) = 1$ and $a \equiv b \mod m$, then $(b, m) = 1$.

Proof. By the definition of congruence, we have that

$$a = b + km, \qquad k \in \mathbb{Z}$$

Suppose that $(b, m) = d > 1$, then $d \mid b$ and $d \mid km$, so $d \mid a$. However, this means that $(a, m) > 1$, which contradicts $(a, m) = 1$. □

Corollary : (9.1)

If the least residues modulo m of $r_1, r_2, \ldots, r_m$ are a permutation of $0, 1, \ldots, m-1$, then $r_1, r_2, \ldots r_m$ contains exactly $\phi(m)$ elements relatively prime to m.

Proof. The proof of this follows from Lemma 9.3. □

Theorem : (9.2)

The function ϕ is multiplicative.

Proof. Suppose that $(m, n) = 1$ and write the numbers from 1 to mn as

$$\begin{array}{ccccc} 1, & m+1, & 2m+1, & \ldots, & (n-1)m+1 \\ 2, & m+2, & 2m+2, & \ldots, & (n-1)m+2 \\ & & \vdots & & \\ m, & 2m, & 3m, & \ldots, & mn \end{array}$$

If $(m, r) = d > 1$, then no element in in the rth row of the array is relatively prime to mn

$$r, \quad m+r, \quad 2m+r, \quad \ldots, \quad (n-1)m+r$$

This is because if $d \mid m$ and $d \mid r$, then $d \mid (km + r)$ for any k. If $(m, r) = 1$, we claim that there are exactly $\phi(n)$ elements in the rth row of the array that are relatively prime to mn

$$r, \quad m + r, \quad 2m + r, \quad \ldots, \quad (n-1)m + r$$

If this is true, then since there are $\phi(m)$ rows, it will follow that $\phi(nm) = \phi(n)\phi(m)$ Suppose that for $0 \leq k, j < n$ that,

$$km + r \equiv jm + r \mod n$$

Then, since $(m, n) = 1$, we have that

$$\begin{aligned} km &\equiv jm \mod n \\ k &\equiv j \mod n \\ k &= j \end{aligned}$$

If $(m, r) = 1$, then Corollary 9.1 gives that there are exactly $\phi(n)$ elements in the rth row of the array that are relatively prime to n.

$$r, \quad m + r, \quad 2m + r, \quad \ldots, \quad (n-1)m + r$$

From Lemma 9.3, we have that every element in the rth row of the array is relatively prime to m. It follows that the rth row of the array contains exactly $\phi(n)$ elements relatively prime to mn. Since there are $\phi(m)$ such rows, it will follow that

$$\phi(nm) = \phi(n)\phi(m)$$

□

Theorem : (9.3)

If n has a prime power decomposition given by $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. then

$$\phi(n) = p_1^{e_1 - 1}(p_1 - 1) p_2^{e_2 - 1}(p_2 - 1) \cdots p_k^{e_k - 1}(p_k - 1)$$

Proof. Since ϕ is multiplicative by Theorem 9.2, Theorem 7.5 gives us that

$$\phi(n) = \phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_k^{e_k})$$

Applying Lemma 9.2, gives us the desired result

$$\phi(n) = p_1^{e_1 - 1}(p_1 - 1) p_2^{e_2 - 1}(p_2 - 1) \cdots p_k^{e_k - 1}(p_k - 1)$$

□

Example

Calculate $\phi(2700)$.

First, $2700 = 2^2 3^3 5^2$, so

$$\begin{aligned} \phi(2700) &= \phi\left(2^2\right)\phi\left(3^3\right)\phi\left(5^2\right) \\ &= 2^1(2-1) \cdot 3^2(3-1) \cdot 5^1(5-1) \\ &= 720 \end{aligned}$$

Corollary : (9.2)

If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Example

Calculate $\phi(2700)$ using the result of Corollary 9.2.

We have that $2700 = 2^2 3^3 5^2$, so

$$\begin{aligned}
\phi(2700) &= 2700\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) \\
&= 2700\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) \\
&= \frac{21600}{30} \\
&= 720
\end{aligned}$$

Arithmetic Functions

Definition : Arithmetic Functions

An arithmetic function is a function whose domain is the set of positive integers.

The function $d(n)$, $\sigma(n)$ and $\phi(n)$ are all arithmetic functions. The Möbius Inversion Formula can be used to obtain nontrivial identities among arithmetic functions from trivial identities.

Theorem : (9.5)

Let f be an arithmetic function for $n \in \mathbb{Z}$ with $n > 0$. Then, consider the following arithmetic function.

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

If f is multiplicative, then F is multiplicative.

Proof. Let m and n be relatively prime positive integers. Then, we have that

$$F(mn) = \sum_{d|mn} f(d)$$

Since $(m, n) = 1$, each divisor d of mn can be written uniquely as $d_1 d_2$, where $d_1, d_2 > 0$, $d_1 \mid m$, $d_2 \mid n$, and $(d_1, d_2) = 1$. Each product $d_1 d_2$ corresponds to a divisor d of mn, so we have that

$$\begin{aligned} F(mn) &= \sum_{d_1|m, d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m, d_2|n} f(d_1) f(d_2) \\ &= \sum_{d_1} f(d_1) \sum_{d_1} f(d_2) \\ &= F(m) F(n) \end{aligned}$$

□

Theorem : Gauss' Theorem

Let $n \in \mathbb{Z}$ with $n > 0$. Then

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

Proof. By Theorem 9.2 and Theorem 9.5, the following arithmetic function is multiplicative.

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

Therefore, by Theorem 7.5, the arithmetic function F is completely determined by its values at powers of prime numbers. If p is a prime number and $a \in \mathbb{Z}$ with $a > 0$, then

$$\begin{aligned} F(p^a) &= \sum_{d \mid n} \phi(d) \\ &= \phi(1) + \phi(p) + \phi\left(p^2\right) + \cdots + \phi(p^a) \\ &= 1 + (p-1) + \left(p^2 - p\right) + \cdots + (p^a - p^{a_1}) \\ &= p^a \end{aligned}$$

Therefore, if the prime decomposition of n is $n = p_1^{e_1} \dots p_r^{e_r}$, then by Theorem 7.5, we have that

$$\begin{aligned} F(n) &= F\left(p_1^{e_1}\right) F\left(p_2^{e_2}\right) \dots F\left(p_r^{e_r}\right) \\ &= p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} \\ &= n \end{aligned}$$

□

Example

Verify that Gauss' Theorem holds for $n = 12$.

The divisors of 12 are 1, 2, 3, 4, 6, and 12. For each divisor, we evaluate Euler's totient function.

$$\begin{aligned} &\phi(1) = 1, \quad \phi(2) = 1, \quad \phi(3) = 2, \\ &\phi(4) = 2, \quad \phi(6) = 2, \quad \phi(12) = 4 \end{aligned}$$

Therefore, we have that

$$\begin{aligned} \sum_{d \mid 14} \phi(d) &= \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) \\ &= 1 + 1 + 2 + 2 + 2 + 4 \\ &= 12 \end{aligned}$$

The Möbius Function

Definition : The Möbius μ Function

If $n \in \mathbb{Z}$ with $n > 0$, then the Möbius μ-function, denoted $\mu(n)$, is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 \mid n \text{ with } p \text{ prime} \\ (-1)^r & \text{if } n = p_1 p_2 \dots p_r \text{ with } p_1, \dots, p_r \text{ distinct primes} \end{cases}$$

Consider the first few values of the Möbius μ-function.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0

Theorem : (9.6)

The Möbius μ-function is multiplicative.

Proof. Let m and n be relatively prime positive integers. If $m = 1$, then by definition of μ, we have that $\mu(m) = 1$. Thus,

$$\begin{aligned}\mu(mn) &= \mu(1n) \\ &= 1 \times \mu(n) \\ &= \mu(m)\mu(n)\end{aligned}$$

If m is divisible by the square of a prime number, then mn is divisible by the square of a prime number. Therefore, by the definition of μ, we would have that $\mu(m) = 0$ and $\mu(mn) = 0$.

$$\begin{aligned}\mu(mn) &= 0 \\ &= 0 \times \mu(n) \\ &= \mu(m)\mu(n)\end{aligned}$$

Assume that $m = p_1 \dots p_r$ and that $n = q_1 \dots q_t$, where all the prime numbers are distinct. Then, by the definition of μ, we have that

$$\begin{aligned}\mu(mn) &= \mu(p_1 \dots p_r q_1 \dots q_t) \\ &= (-1)^{r+t} \\ &= (-1)^r (-1)^t \\ &= \mu(m)\mu(n)\end{aligned}$$

□

Corollary : (9.7)

Let $n \in \mathbb{Z}$ with $n > 0$. Then

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

Proof. By Theorem 9.5 and Theorem 9.6, the following arithmetic function is multiplicative.

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

Therefore, by Theorem 7.5, the arithmetic function F is completely determined by its values at powers of prime powers. If p is a prime number and $a \in \mathbb{Z}$ with $a > 0$, then

$$\begin{aligned}F(p^a) &= \sum_{d|n} \mu(d) \\ &= \mu(1) + \mu(p) + \mu\left(p^2\right) + \cdots + \mu(p^a) \\ &= 1 - 1 + 0 + \cdots + 0 \\ &= 0\end{aligned}$$

Therefore, if the prime decomposition of n is $n = p_1^{e_1} \dots p_r^{e_r}$, then by Theorem 7.5, we have that

$$\begin{aligned}F(n) &= F\left(p_1^{e_1}\right) F\left(p_2^{e_2}\right) \dots F\left(p_r^{e_r}\right) \\ &= 0 \cdot 0 \cdot \ldots \cdot 0 \\ &= 0\end{aligned}$$

If $n = 1$, then $F(n) = \mu(1) = 1$. $\square$

Example

Verify that Corollary 9.7 holds for $n = 12$.

The divisors of 12 are 1, 2, 3, 4, 6, and 12. For each divisor, we evaluate the Möbius μ-function

$$\begin{aligned} &\mu(1) = 1, \quad \mu(2) = -1, \quad \mu(3) = -1, \\ &\mu(4) = 0, \quad \mu(6) = 1, \quad \mu(12) = 0 \end{aligned}$$

Therefore, we have that

$$\begin{aligned} \sum_{d \mid 14} \mu(d) &= \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12) \\ &= 1 - 1 - 1 + 0 + 1 + 0 \\ &= 0 \end{aligned}$$

Möbius Inversion Formula

Theorem : Möbius Inversion Formula

Let f and g be arithmetic functions. Then

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

If and only if

$$g(n) = \sum_{d \mid n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) f(d)$$

Proof. Assume that $f(n) = \sum_{d \mid n} g(d)$. Then

$$\begin{aligned}
\sum_{d \mid n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d \mid n} \left(\mu(d) \sum_{c \mid \frac{n}{d}} g(c) \right) \\
&= \sum_{c \mid n} \left(g(c) \sum_{d \mid \frac{n}{c}} \mu(d) \right)
\end{aligned}$$

By Corollary 9.7, the summation inside the parentheses is 0 unless

$$\frac{n}{c} = 1 \quad \text{or equivalently} \quad n = c$$

The only contribution of the outer summation is when $c = n$ giving

$$\sum_{d} \mu(d) f\left(\frac{n}{d}\right) = g(n)$$

Assume that $g(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) f(d)$. Then

$$\begin{aligned}
\sum_{d \mid n} g(d) &= \sum_{d \mid n} \left(\sum_{c \mid d} \mu\left(\frac{d}{c}\right) f(c) \right) \\
&= \sum_{c \mid n} \left(f(c) \sum_{d \mid c} \mu\left(\frac{d}{c}\right) \right) \\
&= \sum_{c \mid n} \left(f(c) \sum_{m \mid \frac{n}{c}} \mu(m) \right)
\end{aligned}$$

By Corollary 9.7, the summation inside the parentheses is 0 unless

$$\frac{n}{c} = 1 \quad \text{or equivalently} \quad n = c$$

The only contribution of the outer summation is when $c = n$ giving

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

$\square$

Example

Let $g(n) = n$ for all $n \in \mathbb{Z}$ with $n > 0$. By Gauss' Theorem, we have

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

Apply the Möbius Inversion Formula to obtain a nontrivial identity.

Applying the Möbius Inversion Formula gives us:

$$\begin{aligned}\phi(n) &= \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d)\, \frac{n}{d} \\ &= \sum_{d|n} \mu\left(\frac{n}{d}\right) d\end{aligned}$$

Example

Verify for $n = 12$ that

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

The divisors of 12 are 1, 2, 3, 4, 6, and 12. Therefore we have that:

$$\begin{aligned}\sum_{d|n} \mu\left(\frac{n}{d}\right) d &= \mu(12) \cdot 1 + \mu(6) \cdot 2 + \mu(4) \cdot 3 + \mu(3) \cdot 4 + \mu(2) \cdot 6 + \mu(1) \cdot 12 \\ &= 0 \cdot 1 + 1 \cdot 2 + 0 \cdot 3 - 1 \cdot 4 - 1 \cdot 6 + 1 \cdot 12 \\ &= 4 \\ &= \phi(12)\end{aligned}$$

Example

Let $v(n) = 1$ for all $n \in \mathbb{Z}$ with $n > 0$, We have that

$$d(n) \sum_{d \mid n} v(d)$$

Apply the Möbius Inversion Formula to obtain a nontrivial identity.

By the Möbius Inversion Formula, we obtain the nontrivial identity

$$\begin{aligned} 1 &= \sum_{d \mid n} \mu(d)\, d\left(\frac{n}{d}\right) \\ &= \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d(d) \end{aligned}$$

Example

Verify for $n = 12$ that

$$1 = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d(d)$$

The divisors of 12 are 1, 2, 3, 4, 6, and 12. Therefore we have that

$$\begin{aligned} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d(d) &= \mu(12) \cdot 1 + \mu(6) \cdot 2 + \mu(4) \cdot 2 + \mu(3) \cdot 3 + \mu(2) \cdot 4 + \mu(1) \cdot 6 \\ &= 0 \cdot 1 + 1 \cdot 2 + 0 \cdot 2 - 1 \cdot 3 - 1 \cdot 4 + 1 \cdot 6 \\ &= 1 \end{aligned}$$

Example

Let $g(n) = n$ for all $n \in \mathbb{Z}$ with $n > 0$. By definition of $\sigma(n)$ we have

$$\sigma(n) = \sum_{d \mid n} g(d)$$

Apply the Möbius Inversion Formula to obtain a nontrivial identity.

By the Möbius Inversion Formula, we obtain the nontrivial identity

$$\begin{aligned} n &= \sum_{d} \mu(d)\, \sigma\left(\frac{n}{d}\right) \\ &= \sum_{d} \mu\left(\frac{n}{d}\right) \sigma(d) \end{aligned}$$

Example

Verify for $n = 12$ that

$$n = \sum_d \mu(d)\,\sigma\left(\frac{n}{d}\right)$$

The divisors of 12 are 1, 2, 3, 4, 6, and 12. Therefore we have that

$$\begin{aligned}\sum_d \mu\left(\frac{n}{d}\right)\sigma(d) &= \mu(12)\cdot 1 + \mu(6)\cdot 3 + \mu(4)\cdot 4 + \mu(3)\cdot 7 + \mu(2)\cdot 12 + \mu(1)\cdot 28 \\ &= 0\cdot 1 + 1\cdot 3 + 0\cdot 4 - 1\cdot 7 - 1\cdot 12 + 1\cdot 28 \\ &= 12\end{aligned}$$

Example

Let $\mathbb{F}_q$ be the finite field with q elements and let $f(n)$ be the number of monic irreducible polynomials of degree n. Apply the Möbius inversion formula to count the number of irreducible polynomials of degree n that exist over $\mathbb{F}_q$ if the following polynomial has q^n distinct roots.

$$X^{q^n} - X \in \mathbb{F}_q[X]$$

Each degree n polynomial can be decomposed according to the degrees of its irreducible factors, so

$$\sum_{d|n} df(d) = q^n$$

By the Möbius Inversion Formula, we obtain the nontrivial identity

$$f(n) = \frac{1}{n}\sum_{d|n}\mu(d)\,q^{n/d}$$

If $q = 5$ and $n = 2$, then the number of irreducible polynomials is given by

$$f(2) = \frac{1}{2}\sum_{d|2}\mu(d)\cdot 5^{2/d} = \frac{1}{2}\left(5^2 - 5\right) = 10$$

The list of these polynomials are

$$x^2+x+1,\quad x^2+4x+1,\quad x^2+2,\quad x^2+x+2,\quad x^2+4x+2,$$

$$x^2+3,\quad x^2+2x+3,\quad x^2+3x+3,\quad x^2+2x+4,\quad x^2+3x+4$$

Definition : The Riemann Hypothesis

Conjecture: All non-trivial zeros of the Riemann zeta function $\zeta(s)$ lie on the critical line $\mathrm{Re}(s) = \frac{1}{2}$.

The Riemann Hypothesis is equivalent to a strong bound on the partial sums of the Möbius function.

$$M(x) = \sum_{n \leq x} \mu(n) = O^{\left(x^{\frac{1}{2}+\epsilon}\right)}$$

Definition : Mertens Conjecture

Conjecture: For all $x > 1$, we have that

$$|M(x)| = \sqrt{x}$$

This was disproved by Odlyzko and Riele in 1985. However, no explicit counterexample is known.

Definition : Chowla Conjecture

Conjecture: For any distinct positive integers $k_1, \ldots, k_n$,

$$\sum_{n} \mu(n + k_1)\,\mu(n + k_2) \ldots \mu(n + k_n) = o(x)$$

This conjecture states that values of $\mu(n)$ behave pseudo randomly and are asymptotically uncorrelated.

Orders of Elements

In Euler's Theorem, we saw that if $(a, m) = 1$, then there is a positive integer $\phi(m)$ such that

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

If $(a, m) = 1$, then the least residues are all relatively prime elements to m.

$$a, \qquad a^2, \qquad a^3, \qquad \ldots$$

There are $\phi(m)$ least residues $\mod m$ that are relatively prime to m and infinitely many powers of a. It follows that there are positive integers j and k with $j \neq k$ such that

$$a^j \equiv a^k \mod m$$

The smaller power of a in the last congruence may be canceled.

$$a^{j-k} \equiv 1 \mod m \qquad \text{or} \qquad a^{k-j} \equiv 1 \mod m$$

Thus, if $(a, m) = 1$, then there is a positive integer t such that

$$a^t \equiv 1 \mod m$$

Notice that for any positive integer k

$$\begin{aligned} a^{t+k\cdot\phi(m)} &\equiv a^t \left(a^k\right)^{\phi(m)} \mod m \\ &\equiv a^t \mod m \\ &\equiv 1 \mod m \end{aligned}$$

Definition : Order

The order of a modulo m is the smallest positive integer t such that

$$a^t \equiv 1 \mod m$$

Example

Find the orders of the least residues modulo 11.

---

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1
3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1
7	5	2	3	10	4	6	9	8	1
8	9	6	4	10	3	2	5	7	1
9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1

The residue 1 has order 1, the residue 10 has order 2, the residues, 3, 4, 5, and 9 have order 5, the residues 2, 6, 7, and 8 have order 10.

Theorem : (10.1)

Suppose that $(a, m) = 1$ and a has order t modulo m. Then, $a^n \equiv 1 \mod m$ if and only if n is a multiple of t.

Proof. Suppose that $n = tq$ for some integer q. Then

$$\begin{aligned} a^n &\equiv a^{tq} \mod m \\ &\equiv \left(a^t\right)^q \mod m \\ &\equiv 1^q \mod m \\ &\equiv 1 \mod m \end{aligned}$$

Conversely, suppose that $a^n \equiv 1 \mod m$. Since t is the smallest positive integer such that $a^t \equiv 1 \mod m$, we have that $n \geq t$. We can divide n by t to get $n = tq + r$ with $q \geq 1$ and $0 \leq r < t$. Therefore, we have that

$$\begin{aligned} 1 &\equiv a^n \mod m \\ &\equiv a^{tq+r} \mod m \\ &\equiv \left(a^t\right)^q a^r \mod m \\ &\equiv a^r \mod m \end{aligned}$$

Since t is the smallest positive integer such that $a^t \equiv 1 \mod m$, $a^r \equiv 1 \mod m$ with $0 \leq r < t$ is only possible $r = 0$. Thus $n = tq$. □

Theorem : (10.2)

If $(a, m) = 1$ and a has order t modulo m, then $t \mid \phi(m)$.

Proof. From Euler's Theorem, we know that

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

From Theorem 10.1, $\phi(m)$ is a multiple of t, therefore

$$t \mid \phi(m)$$

□

Example

What order can an integer have modulo 9? Find an example of each possible order.

By Theorem 10.2, the possible orders are the divisors of $\phi(9) = 6$. Therefore, the possible orders are 1, 2, 3, and 6.

a	Order of a
1	1
8	2
4	3
2	6

Theorem : (10.3)

If p and q are odd primes and $q \mid a^p - 1$, then $q \mid a - 1$ or $q = 2kp + 1$ for some integer k.

Proof. Since $q \mid a^p - 1$, we have that $a^p \equiv 1 \mod q$. Thus, by Theorem 10.1, the order of a modulo q is a divisor of p. That is, a has order 1 or order p. If the order of a is 1, then $a^1 \equiv 1 \mod q$, therefore $q \mid a - 1$.

If the order of a if p, then by Theorem 10.2, $p \mid \phi(q)$. That is, $p \mid (q-1)$. Therefore, $q - 1 = rp$ for some integer r. Since p and q are odd, r must be even, thus $q = 2kp + 1$ for some k. □

Corollary : (10.1)

Any divisor of $2^p - 1$ is of the form $2kp + 1$.

Example

What is the smallest possible prime divisor of $2^{19} - 1$?

By Corollary 10.1, the divisors are of the form $38k + 1$.

k	$38k+1$	Prime
1	39	No
2	77	No
3	115	No
4	153	No
5	191	Yes

Therefore, the smallest possible prime divisor is 191.

Primitive Roots

Theorem : (10.4)

If the order of a modulo m is t, then $a^r \equiv a^s \mod m$ if and only if $r \equiv s \mod t$.

Proof. Suppose that $a^r \equiv a^s \mod m$ and that $r \geq s$ without loss of generality. Thus, $a^{r-s} \equiv 1 \mod m$. From Theorem 10.1, we have that $r - s$ is a multiple of t. By the definition of a modulo, this gives us that $r \equiv s \mod t$.

To prove the converse, suppose that $r \equiv \mod t$. Then $r = s + kt$ for some integer k, and

$$\begin{aligned} a^r &\equiv a^{s+kt} \mod m \\ &\equiv a^s \left(a^t\right)^k \mod m \\ &\equiv a^s \mod m \end{aligned}$$

□

Definition : Primitive Roots

If a is the least residue and the order of a modulo m is $\phi(m)$, we will say that a is a primitive root of m.

Theorem : (10.5)

If g is a primitive root of m, then the least residues of

$$g, \qquad g^2, \qquad \ldots, \qquad g^{\phi(m)}$$

are a permutation of the $\phi(m)$ positive integers less than m and relatively prime to m.

Proof. Since $(g, m) = 1$¡ each power of g is relatively prime to m. No two powers have the same least residue, because if $g^j \equiv g^k \mod m$, then Theorem 10.4 would give that

$$j \equiv k \mod \phi(m)$$

If $j \not\equiv k \mod \phi(m)$, then $g^j \not\equiv g^k \mod m$. □

Example

Show that 3 is a primitive root of 7.

Since 7 is prime, all elements modulo 7 are relatively prime to 7

$$\begin{aligned}3^1 &\equiv 3 \mod 7,\\ 3^2 &\equiv 2 \mod 7,\\ 3^3 &\equiv 6 \mod 7,\\ 3^4 &\equiv 4 \mod 7,\\ 3^5 &\equiv 5 \mod 7,\\ 3^6 &\equiv 1 \mod 7\end{aligned}$$

Therefore, 3 is a primitive root of 7.

Not every integer has a primitive roots. For example, 8 does not. We will show that each prime has a primitive root. If a has order t modulo m, then any power of a will have an order no larger than t, because for any k,

$$\begin{aligned}\left(a^k\right)^t &\equiv \left(a^t\right)^k \mod m\\ &\equiv 1 \mod m\end{aligned}$$

Lemma : (10.1)

Suppose that a has order t modulo m. Then a^k has order t modulo m if and only if $(k,t)=1$.

Proof. Suppose that $(k,t)=1$ and denote the order of a^k by s.

$$\begin{aligned}1 &\equiv \left(a^t\right)^k \mod m\\ &\equiv \left(a^k\right)^t \mod m\end{aligned}$$

Therefore, by Theorem 10.1, it follows that $s \mid t$. Since s is the order of a^k, we have that

$$\begin{aligned}1 &\equiv \left(a^k\right)^s \mod m\\ &\equiv a^{ks} \mod m\end{aligned}$$

Therefore, by Theorem 10.1, it follows that $t \mid ks$. Since $(k,t)=1$, it follows that $t \mid s$. However, since $s \mid t$, this implies that $s=t$. Therefore, a^k has order $s=t$ as desired.

Suppose that a and a^k have order t, where $(k,t)=r$. Then,

$$\begin{aligned}1 &\equiv a^t \mod m\\ &\equiv \left(a^t\right)^{k/r} \mod m\\ &\equiv \left(a^k\right)^{t/r} \mod m\end{aligned}$$

Theorem 10.1 gives $t \mid r$ is a multiple of t which implies that $r=1$. $\square$

Corollary : (10.2)

Suppose that g is a primitive root of p. Then the least residue of g^k is a primitive root of p if and only if $(k, p-1) = 1$.

Example

Find all primitive roots of 10.

First, we have that $\phi(10) = 4$, so a primitive root will have order 4.

$$\begin{aligned} 3^2 &= 9 \mod m \\ 3^3 &= 7 \mod m \\ 3^4 &= 1 \mod m \end{aligned}$$

Therefore, by Lemma 10.1, the primitive roots of 10 are:

$$3^1 \equiv 3 \mod 10, \qquad 3^3 \equiv 7 \mod 10$$

Primitive Roots

Lemma : (10.2)

If f is a polynomial of degree n, then

$$f(x) \equiv 0 \mod p$$

has at most n solutions

Proof. Let $f(n)$ be a polynomial of degree n

$$f(n) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

For $n = 1$, the polynomial has one solution since $(a_1, p) = 1$

$$a_1 x + a_0 \equiv 0 \mod p$$

Suppose that the lemma is true for polynomials of degree $n-1$. Let $f(n)$ be a polynomial of degree n. Either $f(x) \equiv 0 \mod p$ has no solutions, or it has at least one. If $f(x) \equiv 0 \mod p$ has no solutions, then it has at most n solutions. In the second case, suppose that r is a solution, that is $f(r) \equiv 0 \mod p$. Then, because $x - r$ is a factor of $x^t - r^t$ for $t = 0, 1, \ldots, n$, we have

$$\begin{aligned} f(x) &\equiv f(x) - f(r) \\ &\equiv a_n (x^n - r^n) + a_{n-1} \left(x^{n-1} - r^{n-1}\right) + \cdots + a_1 (x - r) \\ &\equiv (x - r) g(x) \mod p \end{aligned}$$

Where $g(x)$ is of degree $n - 1$. Suppose that s is also a solution of $f(x) \equiv 0 \mod p$. Then,

$$f(s) = (s - r) g(s) \equiv 0 \mod p$$

Since p is a prime, it follows that $s \equiv r \mod p$ or $g(s) \equiv 0 \mod p$. From the induction assumption, the second congruence has at most $n - 1$ solutions, so in total there are at most n solutions. □

Note that Lemma 10.2 is not true if the modulus is not prime. For example, the polynomial equation

$$x^2 + x \equiv 0 \mod 6$$

Has the solutions $x = 0, 2, 3$, and 5

Lemma : (10.3)

If $d \mid p - 1$, then $x^d \equiv 1 \mod p$ has exactly d solutions.

Proof. From Fermat's Theorem, we have that the congruence

$$x^{p-1} \equiv 1 \mod p$$

has exactly $p - 1$ solutions, which are

$$1, \quad 2, \quad \ldots, \quad p - 1$$

However, notice that we have

$$\begin{aligned} x^{p-1} - 1 &= \left(x^d - 1\right)\left(x^{p-1-d} + x^{p-1-2d} + \cdots + 1\right) \\ &= \left(x^d - 1\right) h\left(x\right) \end{aligned}$$

From Lemma 10.2, $h(x) \equiv 0 \mod p$ has at most $p-1-d$ solutions. Hence $x^d \equiv 1 \mod p$ has at least d solutions. By Lemma 10.2, $x^d \equiv 1 \mod p$ also has at most d solutions. Therefore, we see that $x^d \equiv 1 \mod p$ has exactly d solutions. □

Theorem : (10.6)

Every prime p has $\phi(p-1)$ primitive roots.

Proof. Theorem 10.2 says that each of the integers

$$1, \quad 2, \quad \ldots, \quad p-1$$

has an order that is a divisor of $p-1$. For each divisor t of $p-1$, let $\psi(t)$ denote the number of integer that have order t. This can be restated as

$$\sum_{t|p-1} \psi(t) = p-1$$

From Theorem 9.4, we have that

$$\sum_{t|p-1} \psi(t) = \sum_{t|p-1} \phi(t)$$

If we can show that $\psi(t) \leq \phi(t)$ for each t, it will follow from

$$\sum_{t|p-1} \psi(t) = \sum_{t|p-1} \phi(t)$$

that $\psi(t) = \phi(t)$ for each t. In particular, the number of primitive roots of p will be

$$\psi(p-1) = \phi(p-1)$$

If $\psi(t) = 0$, then $\psi(t) < \phi(t)$ and we are done. If $\psi(t) \neq 0$, then there is an integer with order t, call it a. By Lemma 10.3, $x^t \equiv 1 \mod p$ has exactly t solutions. Furthermore, the integers $a, a^2, \ldots, a^t$ satisfy the congruence. By Theorem 10.4, no two powers have the same least residue. Therefore, they give all the solutions to $x^t \equiv 1 \mod p$. From Lemma 10.1, the numbers in $a, a^2, \ldots, a^t$ that have order t are those powers of a^k with $(k, t) = 1$. There are $\phi(t)$ such numbers k. Hence $\psi(t) = \phi(t)$ in this case. That is, there are $\phi(p-1)$ primitive roots. □

Theorem 10.6 does not actually help us to find a primitive root. We do not have an efficient way to find primitive roots, since they behave pseudo-randomly. They can also be composite, for example, 6 is the smallest for 41.

Theorem

The only positive integers with primitive roots are 1, 2, 4, p^e, and $2p^e$, where p is an odd prime.

Quadratic Congruences

It is natural to look at quadratic congruences

$$Ax^2 + Bx + C \equiv 0 \mod m$$

In this section, we will restrict the modulo to an odd prime p

$$Ax^2 + Bx + C \equiv 0 \mod p$$

We know that there is an integer A' such that $AA' \equiv 1 \mod p$. Therefore, the congruence can be rewritten as

$$\begin{aligned} Ax^2 + Bx + C &\equiv 0 \mod p \\ x^2 + A'Bx + A'C &\equiv 0 \mod p \end{aligned}$$

If $A'B$ is even, then we can complete the square to get

$$\begin{aligned} 0 &\equiv x^2 + A'Bx + A'C \mod p \\ 0 &\equiv x^2 + A'Bx + \left(\frac{A'B}{2}\right)^2 - \left(\frac{A'B}{2}\right)^2 + A'C \mod p \\ \left(x + \frac{A'B}{2}\right)^2 &\equiv \left(\frac{A'B}{2}\right)^2 - A'C \mod p \end{aligned}$$

If $A'B$ i odd, change it to $A'B + p$ and then complete the square

$$\begin{aligned} 0 &\equiv x^2 + (A'Bx + p) + A'C \mod p \\ 0 &\equiv x^2 + (A'Bx + p) + \left(\frac{A'B + p}{2}\right)^2 - \left(\frac{A'B + p}{2}\right)^2 + A'C \mod p \\ \left(x + \frac{A'B + p}{2}\right)^2 &\equiv \left(\frac{A'B + p}{2}\right)^2 - A'C \mod p \end{aligned}$$

In either case, we have replaced

$$Ax^2 + Bx + C \equiv 0 \mod p$$

With an equivalent quadratic congruence of the form

$$y^2 \equiv a \mod p$$

Example

Find all the solutions of the congruence $2x^2 + 3x + 1 \equiv 0 \mod 5$.

The multiplicative inverse of 2 modulo 5 is 3. Thus,

$$\begin{aligned} 0 &\equiv 2x^2 + 3x + 1 \mod 5 \\ &\equiv x^2 + 4x + 3 \mod 5 \\ &\equiv x^2 + 4x + 4 - 4 + 3 \mod 5 \\ &\equiv (x+2)^2 - 1 \mod 5 \\ (x+2)^2 &\equiv 1 \mod 5 \end{aligned}$$

By inspection, we see that $x = 2$ and $x = 4$ are solutions.

Such quadratic congruences do not always have solutions

$$\begin{aligned}
0^2 &\equiv 0 \mod 5 \\
1^2 &\equiv 1 \mod 5 \\
2^2 &\equiv 4 \mod 5 \\
3^2 &\equiv 4 \mod 5 \\
4^2 &\equiv 1 \mod 5
\end{aligned}$$

Therefore, there is no solution for $x^2 \equiv 2 \mod 5$ or $x^2 \equiv 3 \mod 5$

Theorem : (11.1)

Suppose that p is an odd prime. If $p \nmid a$, then $x^2 \equiv a \mod p$ has exactly two solutions or has no solutions.

Proof. Suppose that the congruence has a solution, call the solution r. Then, notice that $p - r$ is also a solution since

$$\begin{aligned}
(p-r)^2 &\equiv p^2 - 2pr + r^2 \mod p \\
&\equiv r^2 \mod p \\
&\equiv 1 \mod p
\end{aligned}$$

If s is any solution, then $r^2 \equiv s^2 \mod p$. Therefore,

$$p \mid (r-s)(r+s)$$

Since p is prime, either $p \mid (r-s)$ or $p \mid (r+s)$. In the first case, this gives that $s \equiv r \mod p$, so $s = r$. In the second case, this gives that $s \equiv p - r \mod p$, so $s = p - r$. $\square$

Example

Find all solutions of the congruence $x^2 \equiv 1 \mod 8$.

From inspection, we see that

$$\begin{aligned}
1^2 &\equiv 1 \mod 8 \\
3^2 &\equiv 1 \mod 8 \\
5^2 &\equiv 1 \mod 8 \\
7^2 &\equiv 1 \mod 8
\end{aligned}$$

Therefore, if m is not prime, there can be more than 2 solutions (although they still come in pairs, 1 and 7, and, 3 and 5).

Suppose a is chosen from the integers $1, 2, \ldots, p-1$. Then, $x^2 \equiv a \mod p$ will have two solutions for $\frac{(p-1)}{2}$ values of a. Also, $x^2 \equiv a \mod p$ has no solutions for the other $\frac{(p-1)}{2}$ values of a.

For example, if $p = 11$, then x^2 is of the entries in the table

x	1	2	3	4	5	6	7	8	9	10
$x^2 \mod 11$	1	4	9	5	3	3	5	9	4	1

Therefore, $x^2 \equiv a \mod 11$ will have solutions for: $a \in \{1, 3, 4, 5, 9\}$.

The entries are symmetric about $\frac{p}{2}$ and the same $\frac{p-1}{2}$ least residues appear in each half. For the $\frac{p-1}{2}$ least residues in the first half, there are two solutions. For the $\frac{p-1}{2}$ least residues in the second half, there are no solutions.

Example

For what values of a does $x^2 \equiv a \mod 7$ have two solutions?

The values of a that have two solutions are:

$$\begin{aligned} 1^2 &\equiv 1 \mod 7 \\ 2^2 &\equiv 4 \mod 7 \\ 3^2 &\equiv 2 \mod 7 \end{aligned}$$

So, $a \in \{1, 2, 4\}$ have solutions.

Definition : Quadratic Residues

If $x^2 \equiv a \mod m$ has a solution, then a is called a quadratic residue modulo m.

If $x^2 \equiv a \mod m$ has no solution, then a is called a quadratic non-residue modulo m.

Theorem : Euler's Criterion (11.2)

If p is an odd prime and $p \nmid a$, then $x^2 \equiv a \mod p$ has a solution or no respectively, if

$$a^{\frac{p-1}{2}} \equiv 1 \mod p$$

or

$$a^{\frac{p-1}{2}} \equiv -1 \mod p$$

Proof. Let g be a primitive root of p, which exist by Theorem 10.6. By the definition of primitive roots, $a = g^k \mod p$ for some k. If k is even, then $x^2 \equiv a \mod p$ has a solution, which is $g^{\frac{k}{2}}$. Furthermore, by Fermat's Theorem we have that

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv \left(g^k\right)^{\frac{p-1}{2}} \mod p \\ &\equiv \left(g^{\frac{k}{2}}\right)^{p-1} \mod p \\ &\equiv 1 \mod p \end{aligned}$$

If k is odd, then by Fermat's Theorem we have that

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv \left(g^k\right)^{\frac{p-1}{2}} \mod p \\ &\equiv \left(g^{\frac{p-1}{2}}\right)^{2} \mod p \\ &\equiv (-1)^k \mod p \\ &\equiv -1 \mod p \end{aligned}$$

Also, $x^2 \equiv a \mod p$ has no solution. If it did have one, say r, then

$$\begin{aligned} 1 &\equiv r^{p-1} \mod p \\ &\equiv \left(r^2\right)^{\frac{p-1}{2}} \\ &\equiv a^{\frac{p-1}{2}} \mod p \\ &\equiv -1 \mod p \end{aligned}$$

Since p is an odd prime, $1 \equiv -1 \mod p$, which a contradiction. So this has no solutions.

$\square$

Legendre Symbol

Example

Determine if $x^2 \equiv 7 \mod 31$ has a solution.

By Euler's Criterion, we need to check $7^{\left(\frac{31-1}{2}\right)} = 7^{15} \mod 31$

$$7^2 \equiv 49 \equiv 18 \mod 31$$

$$7^4 \equiv 18^2 \equiv 324 \equiv 14 \mod 31$$
$$7^8 \equiv 14^2 \equiv 196 \equiv 10 \mod 31$$
$$7^{16} \equiv 10^2 \equiv 100 \equiv 7 \mod 31$$
$$7^{15} \equiv \frac{7^{16}}{7} \equiv \frac{7}{7} \equiv 1 \mod 31$$

Therefore, there is a solution.

Euler's Criterion tells us when $x^2 \equiv a \mod p$ has a solution, but it does not give us a way of finding the solutions. One method is to substitute $x = 1, 2, 3, \ldots$ until a solution is found. Another, sometimes more convenient method, is adding multiples of the modulus and factoring squares.

Example

Find a solution of $x^2 \equiv 7 \mod 31$.

Adding the modulus 31 repeatedly to 7, we have that

$$\begin{aligned} x^2 &\equiv 7 \mod 31 \\ &\equiv 38 \mod 31 \\ &\equiv 69 \mod 31 \\ &\equiv 100 \mod 31 \\ &\equiv 10^2 \mod 31 \end{aligned}$$

Therefore, the congruence is satisfied when $x = 10$ or $x = 21$.

Example

Find a solution of $x^2 \equiv 41 \mod 61$.

Adding the modulus 61 repeatedly to 41, we have that

$$\begin{aligned} x^2 &\equiv 41 \mod 61 \\ &\equiv 102 \mod 61 \\ &\equiv 163 \mod 61 \\ &\equiv 224 \mod 61 \\ &\equiv 4^2 \cdot 14 \mod 61 \end{aligned}$$

Adding the modulus 61 repeatedly to 14, we have that

$$\begin{aligned} 14 &\equiv 75 \mod 61 \\ &\equiv 5^2 \cdot 3 \mod 61 \end{aligned}$$

Adding the modulus 61 repeatedly to 3, we have that

$$\begin{aligned} 3 &\equiv 64 \mod 61 \\ &\equiv 8^2 \mod 61 \end{aligned}$$

Thus we have that:

$$\begin{aligned} x^2 &\equiv 41 \mod 61 \\ &\equiv 4^2 \cdot 5^2 \cdot 8^2 \mod 61 \\ &\equiv 160^2 \mod 61 \\ &\equiv 38^2 \mod 61 \end{aligned}$$

Therefore, the congruence is satisfied when $x = 38$ or $x = 23$.

Definition : The Legendre Symbol

The Legendre symbol, denoted $\left(\frac{a}{p}\right)$, where p is an odd prime and $p \nmid a$, is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue (mod } p) \\ -1 & \text{if } a \text{ is a quadratic nonresidue (mod } p) \end{cases}$$

Theorem : (11.3)

The Legendre symbol has the properties:

1. If $a \equiv b \mod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. If $p \nmid a$, then $\left(\frac{a^2}{p}\right) = 1$
3. If $p \nmid a$ and $p \nmid b$, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Proof. Suppose that $x^2 \equiv a \mod p$ has a solution. If $a \equiv b \mod p$, then $x^2 \equiv b \mod p$ also has a solution. This shows that is $\left(\frac{a}{p}\right) = 1$ and $a \equiv b \mod p$, then $\left(\frac{b}{p}\right) = 1$.

Suppose that $x^2 \equiv a \mod p$ does not have a solution. If $a \equiv b \mod p$, then $x^2 \equiv b \mod p$ does not have a solution, because if it did, then $x^2 \equiv a \mod p$ would have a solution. This shows that if $\left(\frac{a}{p}\right) = -1$ and $a \equiv b \mod p$, then $\left(\frac{b}{p}\right) = -1$.

By Euler's Criterion, we have that

$$\left(a^2\right)^{\frac{p-1}{2}} \mod p \equiv a^{p-1} \mod p \equiv 1 \mod p \qquad \text{By FLT}$$

Therefore, by the definition of the Legendre symbol, $\left(\frac{a^2}{p}\right) = 1$. In terms of Legendre symbol, Euler's criterion says that

$$\left(\frac{a}{p}\right) = 1 \quad \text{if} \quad a^{\left(\frac{p-1}{2}\right)} \equiv 1 \mod p$$

$$\left(\frac{a}{p}\right) = -1 \quad \text{if} \quad a^{\left(\frac{p-1}{2}\right)} \equiv -1 \mod p$$

Comparing the 1's and -1's, we see that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$. Therefore, we have that

$$\begin{aligned} \left(\frac{ab}{p}\right) &\equiv (ab)^{\left(\frac{p-1}{2}\right)} \mod p \\ &\equiv a^{\left(\frac{p-1}{2}\right)} b^{\left(\frac{p-1}{2}\right)} \mod p \\ &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p \end{aligned}$$

$\square$

Example

Evaluate $\left(\frac{19}{5}\right)$ and $\left(-\frac{9}{13}\right)$.

By Theorem 11.3, we have that

$$\begin{aligned}\left(\frac{19}{5}\right) &= \left(\frac{4}{5}\right) \\ &= \left(\frac{2^2}{5}\right) \\ &= 1\end{aligned}$$

By Theorem 11.3, we have that

$$\begin{aligned}\left(\frac{-9}{13}\right) &= \left(\frac{4}{13}\right) \\ &= \left(\frac{2^2}{13}\right) \\ &= 1\end{aligned}$$

Legendre Symbol Computations

The quadratic reciprocity theorem shows how $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are related. The theorem was guessed by Euler and Legendre years before it was first proved by Gauss. It's statement was arrived at by observation.

Theorem : Quadratic Reciprocity Theorem (11.4)

If p and q are odd primes and $p \equiv q \equiv 3 \mod 4$, then

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

If p and q are odd primes and $p \equiv 1 \mod 4$ or $q \equiv 1 \mod 4$, then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

Example

Determine if $x^2 \equiv 85 \mod 97$ has a solution.

From Theorem 11.3 and Theorem 11.4, we have that

$$\begin{aligned}
\left(\frac{85}{97}\right) &= \left(\frac{17 \cdot 5}{97}\right) \\
&= \left(\frac{17}{97}\right) \cdot \left(\frac{5}{97}\right) && \text{by Theorem 11.3 (C)} \\
&= \left(\frac{97}{17}\right) \cdot \left(\frac{97}{5}\right) && \text{by Theorem 11.4} \\
&= \left(\frac{12}{17}\right) \cdot \left(\frac{2}{5}\right) && \text{by Theorem 11.3 (A)} \\
&= \left(\frac{4}{17}\right) \cdot \left(\frac{3}{17}\right) \cdot \left(\frac{2}{5}\right) && \text{by Theorem 11.3 (C)} \\
&= \left(\frac{3}{17}\right) \cdot \left(\frac{2}{5}\right) && \text{by Theorem 11.3 (B)} \\
&= \left(\frac{17}{3}\right) \cdot \left(\frac{2}{5}\right) && \text{by Theorem 11.4} \\
&= \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) && \text{by Theorem 11.3 (A)} \\
&= (-1) \cdot (-1) && \text{by inspection} \\
&= 1
\end{aligned}$$

Therefore, $x^2 \equiv 85 \mod 97$ does have a solution.

Theorem : (11.5)

If p is an odd prime, then

$$\left(-\frac{1}{p}\right) = 1 \quad \text{if} \quad p \equiv 1 \mod 4$$

$$\left(-\frac{1}{p}\right) = -1 \quad \text{if} \quad p \equiv 3 \mod 4$$

Proof. If $p \equiv 1 \mod 4$, then $\frac{p-1}{2}$ is even, and Euler's Criterion gives that

$$\left(-\frac{1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p \equiv 1 \mod p$$

If $p \equiv 3 \mod 4$, then $\frac{p-1}{2}$ is odd, and Euler's Criterion gives that

$$\left(-\frac{1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p \equiv -1 \mod p$$

□

Example

Determine if $x^2 \equiv 85 \mod 97$ has a solution.

From Theorem 11.3, Theorem 11.4, and Theorem 11.5, we have that

$$\begin{aligned}
\left(\frac{85}{97}\right) &= \left(\frac{-12}{97}\right) \\
&= \left(-\frac{1}{97}\right) \cdot \left(\frac{4}{97}\right) \cdot \left(\frac{3}{97}\right) && \text{by Theorem 11.3 (C)} \\
&= 1 \cdot 1 \cdot \left(\frac{97}{3}\right) && \text{by Theorems 11.5, 11.3 (B), and 11.4} \\
&= \left(\frac{1}{3}\right) && \text{by Theorem 11.3 (A)} \\
&= 1
\end{aligned}$$

Example

Evaluate $\left(\frac{6}{7}\right)$ and $\left(\frac{2}{23}\right) \cdot \left(\frac{11}{23}\right)$.

From Theorem 11.3 and Theorem 11.5, we have that

$$\begin{aligned} \left(\frac{6}{7}\right) &= \left(\frac{-1}{7}\right) && \text{Theorem 11.3 (A)} \\ &= -1 && \text{by Theorem 11.5} \end{aligned}$$

From Theorem 11.5, we have that

$$\begin{aligned} \left(\frac{2}{23}\right) \cdot \left(\frac{11}{23}\right) &= \left(\frac{22}{23}\right) && \text{by Theorem 11.3 (C)} \\ &= \left(-\frac{1}{23}\right) && \text{by Theorem 11.3 (A)} \\ &= -1 && \text{by Theorem 11.5} \end{aligned}$$

Theorem : (11.6)

If p is an odd prime, then

$$\left(\frac{2}{p}\right) = 1 \quad \text{if} \quad p \equiv 1 \mod 8 \quad \text{or} \quad p \equiv 7 \mod 8$$

$$\left(\frac{2}{p}\right) = -1 \quad \text{if} \quad p \equiv 3 \mod 8 \quad \text{or} \quad p \equiv 5 \mod 8$$

Example

Evaluate $\left(\frac{2}{23}\right) \cdot \left(\frac{11}{23}\right)$.

From Theorem 11.5, we have that

$$\begin{aligned} \left(\frac{2}{23}\right) \cdot \left(\frac{11}{23}\right) &= -1 \cdot \left(\frac{2}{23}\right) \cdot \left(\frac{23}{11}\right) && \text{by Theorem 11.4} \\ &= -1 \cdot \left(\frac{2}{23}\right) \cdot \left(\frac{1}{11}\right) && \text{by Theorem 11.3 (A)} \\ &= -1 \cdot 1 \cdot 1 && \text{by Theorem 11.6} \\ &= -1 \end{aligned}$$

Example

Calculate $\left(\frac{1234}{4567}\right)$.

From Theorem 11.5, we have that

$$\begin{aligned}
\left(\frac{1234}{4567}\right) &= \left(\frac{2}{4567}\right) \cdot \left(\frac{617}{4567}\right) && \text{by Theorem 11.3 (C)} \\
&= 1 \cdot \left(\frac{4567}{617}\right) && \text{by Theorem 11.4 and Theorem 11.6} \\
&= \left(\frac{248}{617}\right) && \text{by Theorem 11.3 (A)} \\
&= \left(\frac{4}{617}\right) \cdot \left(\frac{2}{617}\right) \cdot \left(\frac{31}{617}\right) && \text{by Theorem 11.3 (C)} \\
&= 1 \cdot 1 \cdot \left(\frac{617}{31}\right) && \text{by Theorem 11.4 and Theorem 11.6} \\
&= \left(\frac{28}{31}\right) && \text{by Theorem 11.3 (A)} \\
&= \left(\frac{4}{31}\right) \cdot \left(\frac{7}{31}\right) && \text{by Theorem 11.3 (C)} \\
&= 1 \cdot -1 \cdot \left(\frac{31}{7}\right) && \text{by Theorem 11.3 (B) and Theorem 11.4} \\
&= -1 \cdot \left(\frac{3}{7}\right) \\
&= 1 && \text{by Theorem 11.4}
\end{aligned}$$

Example

Does $x^2 \equiv 211 \mod 159$ have a solution?

By the Chinese Remainder Theorem, there is a solution if and only if both of the following quadratic congruences have a solution.

$$x^2 \equiv 52 \mod 3 \equiv 1 \mod 3$$

$$x^2 \equiv 52 \mod 53 \equiv -1 \mod 53$$

By Theorem 11.4 (B), $x^2 \equiv 1 \mod 3$ has a solution. By Theorem 11.5, $x^2 \equiv -1 \mod 53$ has a solution.

Midterm Practice

The entirety of this lecture was spent doing the practice problems for the midterm.

Term Project

The entirety of this lecture was spent working on the term project.

Gauss's Lemma

Example

Determine if $x^2 \equiv 39 \mod 83$ has a solution.

By Theorem 11.3, Theorem 11.4, Theorem 11.5, and Theorem 11.6, we have that:

$$\begin{aligned}
\left(\frac{39}{83}\right) &= \left(\frac{3}{83}\right) \cdot \left(\frac{13}{83}\right) \quad \text{by Theorem 11.3 (C)} \\
&= -\left(\frac{83}{3}\right) \cdot \left(\frac{83}{13}\right) \quad \text{by Theorem 11.4} \\
&= -\left(\frac{2}{3}\right) \cdot \left(\frac{5}{13}\right) \quad \text{by Theorem 11.3 (A)} \\
&= \left(\frac{13}{5}\right) \quad \text{by Theorem 11.4 and Theorem 11.6} \\
&= \left(\frac{3}{5}\right) \text{by Theorem 11.3 (A)} \\
&= -1
\end{aligned}$$

Theorem : Gauss's Lemma (12.1)

Suppose that p is an odd prime, $(a, p) = 1$, and there are among the least residues modulo p of

$$a, \qquad 2a, \qquad 3a, \qquad \ldots, \qquad \frac{p-1}{2} \cdot a$$

Exactly g that are strictly greater than $\frac{p-1}{2}$. Then,

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

Proof. Let $r_1, r_2, \ldots, r_k$ denote the least residues of p

$$a, \qquad 2a, \qquad 3a, \qquad \ldots, \qquad \frac{p-1}{2} \cdot a$$

That are less than or equal to $\frac{p-1}{2}$. Then, let $s_1, s_2, \ldots, s_g$ denote those that are greater than $\frac{p-1}{2}$. Note that no two of the r's are congruence modulo p. Suppose that two were. Then, we would have for some k_1 and k_2 that

$$k_1 a \equiv k_2 a \mod p, \qquad 0 \leq k_1, k_2 \leq \frac{p-1}{2}$$

Since $(a, p) = 1$, it follows that $k_1 = k_2$. For the same reason, no two of the s's are congruent modulo p. Now, consider the set of numbers

$$r_1, \quad r_2, \quad \ldots, r_k, \quad p - s_1, \quad p - s_2, \quad \ldots, \quad p - s_g$$

Each integer n in the set satisfies $1 \leq n \leq \frac{p-1}{2}$ and there are $\frac{p-1}{2}$ elements in the set.

Suppose that for some i and j that we have

$$\begin{aligned} r_i &\equiv p - s_j \mod p \\ r_i + s_j &\equiv 0 \mod p \end{aligned}$$

Note that $r_i \equiv ta \mod p$ and $s_j \equiv ua \mod p$ for some t and u with

$$1 \leq t, u \leq \frac{p-1}{2}$$

Therefore, we would have that

$$\begin{aligned} (t+u)\, a &\equiv 0 \mod p \\ t + u &\equiv 0 \mod p \end{aligned}$$

This is impossible since $2 \leq t + u \leq p - 1$. Thus, all the elements in the following set are distinct

$$r_1, \quad r_2, \quad \ldots, r_k, \quad p - s_1, \quad p - s_2, \quad \ldots, \quad p - s_g$$

Consequently, the elements are a rearrangement of the elements in

$$1, \qquad 2, \qquad \ldots, \qquad \frac{p-1}{2}$$

Therefore, we have that

$$\begin{aligned} r_1 r_2 \cdots r_k \,(p - s_1) \cdots (p - s_g) &\equiv 1 \times 2 \times \cdots \times \frac{p-1}{2} \mod p \\ (-1)^g \, r_1 r_2 \cdots r_k \cdot s_1 s_2 \cdots s_g &\equiv \left(\frac{p-1}{2}\right)! \mod p \\ (-1)^g \, a^{\left(\frac{p-1}{2}\right)} \left(\frac{p-1}{2}\right)! &\equiv \left(\frac{p-1}{2}\right)! \mod p \end{aligned}$$

The common factor is relatively prime to p, thus

$$\begin{aligned} (-1)^g \, a^{\left(\frac{p-1}{2}\right)} &\equiv 1 \mod p \\ a^{\left(\frac{p-1}{2}\right)} &\equiv (-1)^g \mod p \\ \left(\frac{a}{p}\right) &\equiv (-1)^g \mod p \\ \left(\frac{a}{p}\right) &= (-1)^g \end{aligned}$$

$\square$

Example

Determine whether $x^2 \equiv 7 \mod 23$ has a solution.

We have that $\frac{p-1}{2} = \frac{23-1}{2} = 11$. The multiples of 7 are:

$$7, 14, 21, 28, 35, 42, 49, 56, 63, 70, 77$$

These have the least residues modulo 23 of

$$7, 14, 21, 5, 12, 19, 3, 10, 17, 1, 8$$

Of these, 5 (14, 21, 12, 19, 17) are strictly larger than $\frac{p-1}{2} = 11$. Then, $(-1)^5 = -1$. Therefore, by Theorem 12.1, 7 is a quadratic nonresidue modulo 23.

Quadratic Reciprocity : Part 1

Recall, we have covered Theorem 11.6, but never proven it:

Theorem : (11.6)

If p is an odd prime, then

$$\left(\frac{2}{p}\right) = 1 \quad \text{if} \quad p \equiv 1 \mod 8 \quad \text{or} \quad p \equiv 7 \mod 8$$

$$\left(\frac{2}{p}\right) = -1 \quad \text{if} \quad p \equiv 3 \mod 8 \quad \text{or} \quad p \equiv 5 \mod 8$$

Proof. By Theorem 12.1, it is sufficient to find out how many of the least residues modulo p of

$$2, \quad 4, \quad 6, \quad \dots, 2 \cdot \frac{p-1}{2}$$

Are greater than $\frac{p-1}{2}$. Since all the numbers are least residues, we only have to see how many of them are greater than $\frac{p-1}{2}$. Let the first even integer greater than $\frac{p-1}{2}$ be $2a$. Between 2 and $\frac{p-1}{2}$, there are a - 1 even integers, namely

$$2, \quad 4, \quad 6, \quad \dots, \quad 2(a-1)$$

The number of even integers from 2 to $p-1$ greater than $\frac{p-1}{2}$ is

$$g = \frac{p-1}{2} - (a-1)$$

Since $2a$ is the smallest integer greater than $\frac{p-1}{2}$, it follows that g is the largest integer less than $\frac{p+3}{4}$. Suppose that $p \equiv 1 \mod 8$. Then, $p = 1 + 8k$ for some k and

$$\frac{p+3}{4} = \frac{4+8k}{4} = 1 + 2k$$

It follows that $g = 2k$ and that $(-1)^g = 1$. From Theorem 12.1, $\left(\frac{2}{p}\right) = 1$ if $p \equiv 1 \mod 8$. Suppose that $p \equiv 3 \mod 8$. Then, $p = 3 + 8k$ for some k and

$$\frac{p+3}{4} = \frac{6+8k}{4} = \frac{3}{2} + 2k$$

It follows that $g = 2k+1$ and that $(-1)^g = -1$. From Theorem 12.1, $\left(\frac{2}{p}\right) = -1$ if $p \equiv 3 \mod 8$. Suppose that $p \equiv 5 \mod 8$. Then, $p = 5 + 8k$ for some k and

$$\frac{p+3}{4} = \frac{8+8k}{4} = 2 + 2k$$

It follows that $g = 2k+1$ and that $(-1)^g = -1$. From Theorem 12.1, $\left(\frac{2}{p}\right) = -1$ if $p \equiv 5 \mod 8$. Suppose that $p \equiv 7 \mod 8$. Then, $p = 7 + 8k$ for some k and

$$\frac{p+3}{4} = \frac{10+8k}{4} = \frac{5}{2} + 2k$$

It follows that $g = 2k+2$ and that $(-1)^g = 1$. From Theorem 12.1, $\left(\frac{2}{p}\right) = 1$ if $p \equiv 7 \mod 8$. $\square$

Lemma : (12.1)

If p and q are different odd primes, then

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

Proof. Let $S(p,q)$ and $S(q,p)$ be defined as

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

We are trying to prove that $S(p,q) + S(q,p) = \frac{(p-1)(q-1)}{4}$. $S(p,q)$ is the number of lattice points below the line $y = \frac{qx}{p}$ and above the x-axis for $x = 1, 2, \dots \frac{p-1}{2}$. $S(q,p)$ is the number of lattice points to the left of the line $y = \frac{qx}{p}$ and to the right of the y-axis. Notice that there are no lattice points on the line. If the lattice point (a,b) were on the line $y = \frac{qx}{p}$, then

$$b = \frac{qa}{p} \quad \text{or} \quad bp = qa$$

Since $p \mid qa$ and $(p,q) = 1$, it follows that $p \mid a$. However, $1 \leq a \leq \frac{p-1}{2}$, a contradiction. Each lattice point in or on the boundary of the rectangle is

$$S(p,q) + S(q,p)$$

This number is also $\frac{p-1}{2} \cdot \frac{q-1}{2}$. Therefore we have that,

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

$\square$

Quadratic Reciprocity Part 2

Theorem : (12.4)

If p and q are odd primes, then

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

Proof. Suppose that $p \equiv q \equiv 3 \mod 4$. Then $\frac{(p-1)(q-1)}{4}$ is odd and thus

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1 \quad \text{so} \quad \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

Suppose that $p \equiv 1 \mod 4$ or $p \equiv 1 \mod 4$. Then, $\frac{(p-1)(q-1)}{4}$ is even and thus

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1 \quad \text{so} \quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

As in the proof of Gauss's Lemma, take the least residues modulo p of

$$q, \quad 2q, \quad 3q, \quad \dots, \quad \frac{p-1}{2}\cdot q$$

Then, separate the least residues modulo p into two classes. Put the residues less than or equal to $\frac{p-1}{2}$ in one class and call them

$$r_1, \quad r_2, \quad \dots, \quad r_k$$

Put the least residues greater than $\frac{p-1}{2}$ in another class and call them

$$s_1, \quad s_2, \quad \dots, \quad s_g$$

The conclusion of Gauss's Lemma is that

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

To simplify notation later, define R and S as

$$R = r_1 + r_2 + \dots + r_k, \quad S = s_1 + s_2 + \dots + s_g$$

While proving Gauss's Lemma, we showed that the set of numbers

$$r_1, \quad r_2, \quad \dots, \quad r_k, \quad p - s_1, \quad p - s_2, \quad \dots, \quad p - s_g$$

Was simply a permutation of the set of numbers

$$1, \quad 2, \quad \dots, \quad \frac{p-1}{2}$$

It follows that the two sums are equivalent

$$\begin{aligned} 1 + 2 + \dots + \frac{p-1}{2} &= r_1 + r_2 + \dots + r_k + p - s_1 + p - s_2 + \dots + p - s_g \\ R + gp - S &= \frac{1}{2}\cdot\frac{p-1}{2}\cdot\frac{p+1}{2} \\ R &= \frac{p^2-1}{8} + S - gp \end{aligned}$$

The least residue modulo p of jq for $j = 1, 2, \ldots, \frac{p-1}{2}$, is the remainder when we divide jq by p. We know the quotient is $\left[\frac{jq}{p}\right]$, so if we let t_j denote the least residue modulo p of jq, we have

$$jq = \left[\frac{jq}{p}\right] p + t_j$$

If we sum these equations over j, we have

$$\begin{aligned} \sum_{j=1}^{\frac{p-1}{2}} jq &= \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jq}{p}\right] p + \sum_{j=1}^{\frac{p-1}{2}} t_j \\ q \sum_{j=1}^{\frac{p-1}{2}} j &= p \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jq}{p}\right] + \sum_{j=1}^{k} r_j + \sum_{j=1}^{g} s_j \end{aligned}$$

This gives us that

$$\begin{aligned} q \cdot \frac{p^2-1}{8} &= p \cdot S(p,q) + R + S \\ q \cdot \frac{p^2-1}{8} &= p \cdot S(p,q) + S + \frac{p^2-1}{8} + S - gp \\ (q-1) \cdot \frac{p^2-1}{8} &= p \cdot (S(p,q) - g) + 2S \end{aligned}$$

The left-hand side is even because $\frac{p^2-1}{8}$ is an integer and $q-1$ is even. The right side has $2S$ even, so it follows that $p\left(S(p,q) - g\right)$ is even. Therefore, $S(p,q) - g$ is even, and hence

$$\begin{aligned} (-1)^{S(p,q)-g} &= 1 \\ (-1)^{S(p,q)} &= (-1)^g \end{aligned}$$

Since $(-1)^g = \left(\frac{q}{p}\right)$, we get that

$$\left(\frac{p}{q}\right) = (-1)^{S(p,q)}$$

Now, we can repeat the argument with p and q interchanged to get

$$\left(\frac{p}{q}\right) = (-1)^{S(q,p)}$$

Multiplying together, we get that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)}$$

Therefore, by Lemma 12.1, we have that

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

□

Primality Testing: It is not know whether 2 is a primitive root of infinitely many primes.

Theorem : (12.3)

If p and $4p+1$ are both primes, then 2 is a primitive root modulo $4p+1$.

Proof. If $q = 4p+1$ is prime, then $\phi(q) = 4p$. Therefore, 2 has order 1, 2, p, $2p$, or $4p$, modulo q. By Euler's Criterion, we have that

$$2^{2p} \equiv 2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right) \mod q$$

However, p is odd, so $4p \equiv 4 \mod 8$, so $q \equiv 5 \mod 8$. From Theorem 11.6, 2 is a quadratic non-residue of primes congruent to 5 modulo 8. Therefore, we have that

$$2^{2p} \equiv -1 \mod q$$

Thus, the order of 2 can not be any of the divisors of $2p$. Therefore, the order of 2 is not 1, 2, p, or $2p$. Also, 2 does not have order 4 either since $2^4 \equiv 1 \mod q$ implies that $q \mid 15$, which is impossible. Thus, 2 has order $4p$ and is therefore a primitive root of $4p+1$. □

Other Extensions:

- Could you could multiple congruences simultaneously (Similar to the Chinese Remainder Theorem)?
- What about other residues (Cubic, Quartic)?

Theorem

If $p \equiv 2 \mod 3$, then all $x^3 \equiv a \mod p$ have solutions.

Proof. From Fermat's Little Theorem, we have that

$$x^p \equiv x \mod p \quad \Leftrightarrow \quad x^{p-1} \equiv 1 \mod p$$

Multiplying these gives

$$x^{2p-1} \equiv x \mod p$$

Since $p \equiv 2 \mod 3$, let $p = 3q+2$

$$x \equiv x^{2p-1} \equiv x^{2(3q+2)-1} \equiv x^{6q+3} \equiv \left(x^{2q+1}\right)^3 \mod p$$

Therefore, x is a cubic residue. □

What about for $p \equiv 1 \mod 3$? We would split it into 3 cosets (similar to how we split residues into 2 cosets for quadratics)