Chapter 3

Congruences

A congruence is nothing more than a statement about divisibility. The theory of congruences was introduced by Carl Friedreich Gauss. Gauss contributed to the basic ideas of congruences and proved several theorems related to this theory. We start by introducing congruences and their properties. We proceed to prove theorems about the residue system in connection with the Euler ϕ-function. We then present solutions to linear congruences which will serve as an introduction to the Chinese remainder theorem. We present finally important congruence theorems derived by Wilson, Fermat and Euler.

3.1 Introduction to congruences

As we mentioned in the introduction, the theory of congruences was developed by Gauss at the beginning of the nineteenth century.

Definition 12. *Let m be a positive integer. We say that a is congruent to b modulo m if $m \mid (a-b)$ where a and b are integers, i.e. if $a = b + km$ where $k \in \mathbb{Z}$.*

If a is congruent to b modulo m, we write $a \equiv b(mod\, m)$.

Example 24. $19 \equiv 5(mod\, 7)$. *Similarly* $2k+1 \equiv 1(mod\, 2)$ *which means every odd number is congruent to 1 modulo 2.*

There are many common properties between equations and congruences. Some properties are listed in the following theorem.

Theorem 21. *Let* a, b, c *and* d *denote integers. Let* m *be a positive integers. Then:*

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

2. *If* $a \equiv b(mod\, m)$ *and* $b \equiv c(mod\, m)$*, then* $a \equiv c(mod\, m)$*.*

3. *If* $a \equiv b(mod\, m)$*, then* $a + c \equiv b + c(mod\, m)$*.*

4. *If* $a \equiv b(mod\, m)$*, then* $a - c \equiv b - c(mod\, m)$*.*

5. *If* $a \equiv b(mod\, m)$*, then* $ac \equiv bc(mod\, m)$*.*

6. *If* $a \equiv b(mod\, m)$*, then* $ac \equiv bc(mod\, mc)$*, for* $c > 0$.

7. *If* $a \equiv b(mod\, m)$ *and* $c \equiv d(mod\, m)$ *then* $a + c \equiv (b + d)(mod\, m)$*.*

8. *If* $a \equiv b(mod\, m)$ *and* $c \equiv d(mod\, m)$ *then* $a - c \equiv (b - d)(mod\, m)$*.*

9. *If* $a \equiv b(mod\, m)$ *and* $c \equiv d(mod\, m)$ *then* $ac \equiv bd(mod\, m)$*.*

Proof.

1. If $a \equiv b(mod\ m)$, then $m \mid (a-b)$. Thus there exists integer k such that $a - b = mk$, this implies $b - a = m(-k)$ and thus $m \mid (b-a)$. Consequently $b \equiv a(mod\, m)$.

2. Since $a \equiv b(mod\ m)$, then $m \mid (a-b)$. Also, $b \equiv c(mod\ m)$, then $m \mid (b-c)$. As a result, there exit two integers k and l such that $a = b+mk$ and $b = c+ml$, which imply that $a = c+m(k+l)$ giving that $a = c(mod\, m)$.

3. Since $a \equiv b(mod\, m)$, then $m \mid (a-b)$. So if we add and subtract c we get

$$m \mid ((a+c)-(b+c))$$

and as a result

$$a+c \equiv b+c(mod\, m).$$

4. Since $a \equiv b(mod\, m)$, then $m \mid (a-b)$ so we can subtract and add c and we get

$$m \mid ((a-c)-(b-c))$$

and as a result

$$a-c \equiv b-c(mod\, m).$$

5. If $a \equiv b(mod\ m)$, then $m \mid (a-b)$. Thus there exists integer k such that $a-b=mk$ and as a result $ac-bc=m(kc)$. Thus

$$m \mid (ac-bc)$$

and hence

$$ac \equiv bc(mod\, m).$$

6. If $a \equiv b(mod\ m)$, then $m \mid (a-b)$. Thus there exists integer k such that $a-b=mk$ and as a result

$$ac-bc=mc(k).$$

Thus

$$mc \mid (ac-bc)$$

and hence

$$ac \equiv bc(mod\, mc).$$

7. Since $a \equiv b(mod\ m)$, then $m \mid (a-b)$. Also, $c \equiv d(mod\ m)$, then $m \mid (c-d)$. As a result, there exits two integers k and l such that $a-b = mk$ and $c-d = ml$. Note that

$$(a-b)+(c-d) = (a+c)-(b+d) = m(k+l).$$

As a result,

$$m \mid ((a+c)-(b+d)),$$

hence

$$a+c \equiv b+d(mod\, m).$$

8. If $a = b+mk$ and $c = d+ml$ where k and l are integers, then

$$(a-b)-(c-d) = (a-c)-(b-d) = m(k-l).$$

As a result,

$$m \mid ((a-c)-(b-d)),$$

hence

$$a-c \equiv b-d(mod\, m).$$

9. There exit two integers k and l such that $a-b = mk$ and $c-d = ml$ and thus $ca-cb = m(ck)$ and $bc-bd = m(bl)$. Note that

$$(ca-cb)+(bc-bd) = ac-bd = m(kc-lb).$$

As a result,

$$m \mid (ac-bd),$$

hence

$$ac \equiv bd(mod\, m).$$

□

Examples 1. 1. *Because* $14 \equiv 8(mod\, 6)$ *then* $8 \equiv 14(mod\, 6)$.

2. *Because* $22 \equiv 10(mod\, 6)$ *and* $10 \equiv 4(mod\, 6)$. *Notice that* $22 \equiv 4(mod\, 6)$.

3. *Because* $50 \equiv 20(mod\, 15)$*, then* $50 + 5 = 55 \equiv 20 + 5 = 25(mod\, 15)$.

4. *Because* $50 \equiv 20(mod\, 15)$*, then* $50 - 5 = 45 \equiv 20 - 5 = 15(mod\, 15)$.

5. *Because* $19 \equiv 16(mod 3)$*, then* $2(19) = 38 \equiv 2(16) = 32(mod\, 3)$.

6. *Because* $19 \equiv 16(mod 3)$*, then* $2(19) = 38 \equiv 2(16) = 32(mod\, 2(3) = 6)$.

7. *Because* $19 \equiv 3(mod\, 8)$ *and* $17 \equiv 9(mod\, 8)$*, then* $19 + 17 = 36 \equiv 3 + 9 = 12(mod\, 8)$.

8. *Because* $19 \equiv 3(mod\, 8)$ *and* $17 \equiv 9(mod\, 8)$*, then* $19 - 17 = 2 \equiv 3 - 9 = -6(mod\, 8)$.

9. *Because* $19 \equiv 3(mod\, 8)$ *and* $17 \equiv 9(mod\, 8)$*, then* $19(17) = 323 \equiv 3(9) = 27(mod\, 8)$.

We now present a theorem that will show one difference between equations and congruences. In equations, if we divide both sides of the equation by a non-zero number, equality holds. While in congruences, it is not necessarily true. In other words, dividing both sides of the congruence by the same integer doesn't preserve the congruence.

Theorem 22. 1. *If* a, b, c *and* m *are integers such that* $m > 0$*,* $d = (m, c)$ *and* $ac \equiv bc(mod\ m)$*, then* $a \equiv b(mod\ m/d)$.

2. *If* $(m, c) = 1$ *then* $a = b(mod\ m)$ *if* $ac \equiv bc(mod\ m)$.

Proof. Part 2 follows immediately from Part 1. For Part 1, if $ac \equiv bc(mod\ m)$, then

$$m \mid (ac - bc) = c(a - b).$$

Hence there exists k such that $c(a-b)=mk$. Dividing both sides by d, we get $(c/d)(a-b)=k(m/d)$. Since $(m/d,c/d)=1$, it follows that $m/d \mid (a-b)$. Hence $a \equiv b(mod\, m/d)$. □

Example 25. $38 \equiv 10(mod\, 7)$. *Since* $(2,7)=1$ *then* $19 \equiv 5(mod\, 7)$.

The following theorem combines several congruences of two numbers with different moduli.

Theorem 23. *If*

$$a \equiv b(mod\, m_1), a \equiv b(mod\, m_2), ..., a \equiv b(mod\, m_t)$$

where $a, b, m_1, m_2, ..., m_t$ *are integers and* $m_1, m_2, ..., m_t$ *are positive, then*

$$a \equiv b(mod\, \langle m_1, m_2, ...m_t \rangle)$$

Proof. Since $a \equiv b(mod\, m_i)$ for all $1 \leq i \leq t$. Thus $m_i \mid (a-b)$. As a result,

$$\langle m_1, m_2, ..., m_t \rangle \mid (a-b)$$

(prove this as an exercise). Thus

$$a \equiv b(mod\, \langle m_1, m_2, ...m_t \rangle).$$

□

Exercises

1. Determine whether 3 and 99 are congruent modulo 7 or not.

2. Show that if x is an odd integer, then $x^2 \equiv 1(mod\, 8)$

3. Show that if a, b, m and n are integers such that m and n are positive, $n \mid m$ and $a \equiv b(mod\, m)$, then $a \equiv b(mod\, n)$.

4. Show that if $a_i \equiv b_i(mod\, m)$ for $i = 1, 2, ..., n$, where m is a positive integer and a_i, b_i are integers for $j = 1, 2, ..., n$, then $\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i(mod\, m)$

5. For which n does the expression $1 + 2 + ... + (n-1) \equiv 0(mod\, n)$ holds.

3.2 Residue Systems and Euler's ϕ-Function

3.2.1 Residue Systems

Suppose m is a positive integer. Given two integers a and b, we see that by the division algorithm that $a = bm + r$ where $0 \leq r < m$. We call r the least non-negative residue of a modulo m. As a result, we see that any integer is congruent to one of the integers $0, 1, 2, ..., m - 1$ modulo m.

Definition 13. *A complete residue system modulo m is a set of integers such that every integer is congruent modulo m to exactly one integer of the set.*

The easiest complete residue system modulo m is the set of integers $0, 1, 2, ..., m-1$. Every integer is congruent to one of these integers modulo m.

Example 26. *The set of integers $\{0, 1, 2, 3, 4\}$ form a complete residue system modulo 5. Another complete residue system modulo 5 could be $6, 7, 8, 9, 10$.*

Definition 14. *A reduced residue system modulo m is a set of integers r_i such that $(r_i, m) = 1$ for all i and $r_i \neq r_j (mod\, m)$ if $i \neq j$.*

Notice that, a reduced residue system modulo m can be obtained by deleting all the elements of the complete residue system set that are not relatively prime to m.

Example 27. *The set of integers $\{1, 5\}$ is a reduced residue system modulo 6.*

The following lemma will help determine a complete residue system modulo any positive integer m.

Lemma 10. *A set of m incongruent integers modulo m forms a complete residue system modulo m.*

Proof. We will prove this lemma by contradiction. Suppose that the set of m integers does not form a complete residue system modulo m. Then we can find at least one integer a that is not congruent to any element in this set. Hence non of the elements of this set is actually congruent to the remainder when a is divided by m. Thus dividing by m yields to at most $m-1$ remainders. Therefore by the pigeonhole principle, at least two integers in the set that have the same remainder modulo m. This is a contradiction since the set of integers is formed of m integers that are incongruent modulo m. □

Theorem 24. *If $a_1, a_2, ..., a_m$ is a complete residue system modulo m, and if k is a positive integer with $(k,m)=1$, then*

$$ka_1+b, ka_2+b, ..., ka_m+b$$

is another complete residue system modulo m for any integer b.

Proof. Let us prove first that no two elements of the set $\{ka_1+b, ka_2+b, ..., ka_m+b\}$ are congruent modulo m. Suppose there exists i and j such that

$$ka_i+b \equiv ka_j+b(mod\, m).$$

Thus we get that

$$ka_i \equiv ka_j(mod\, m).$$

Now since $(k,m)=1$, we get

$$a_i \equiv a_j(mod\, m)$$

But for $i \neq j$, a_i is inequivalent to a_j modulo m. Thus $i=j$. Now notice that there are m inequivalent integers modulo m and thus by Lemma 10, the set form a complete residue system modulo m. □

3.2.2 Euler's ϕ-Function

We now present a function that counts the number of positive integers less than a given integer that are relatively prime to that given integer. This function is called Euler ϕ-function. We will discuss the properties of Euler ϕ-function in details in chapter 5. It will be sufficient for our purposes in this chapter to the notation.

Definition 15. *The Euler ϕ-function of a positive integer n, denoted by $\phi(n)$ counts the number of positive integers less than n that are relatively prime to n.*

Example 28. *Since 1 and 3 are the only two integers that are relatively prime to 4 and less than 4, then $\phi(4) = 2$. Also, 1,2,...,6 are the integers that are relatively prime to 7 that are less than 7, thus $\phi(7) = 6$.*

Now we can say that the number of elements in a reduced residue system modulo n is $\phi(n)$.

Theorem 25. *If $a_1, a_2, ..., a_{\phi(n)}$ is a reduced residue system modulo n and $(k, n) = 1$, then $ka_1, ka_2, ..., ka_{\phi(n)}$ is a reduced residue system modulo n.*

Proof. The proof proceeds exactly in the same way as that of Theorem 24. □

Exercises

1. Give a reduced residue system modulo 12.
2. Give a complete residue system modulo 13 consisting only of odd integers.
3. Find $\phi(8)$ and $\phi(101)$.

3.3 Linear Congruences

Because congruences are analogous to equations, it is natural to ask about solutions of linear equations. In this section, we will be discussing linear congruences of one variable and their solutions. We start by defining linear congruences.

Definition 16. *A congruence of the form $ax \equiv b(mod\, m)$ where x is an unknown integer is called a linear congruence in one variable.*

It is important to know that if x_0 is a solution for a linear congruence, then all integers x_i such that $x_i \equiv x_0(mod\ m)$ are solutions of the linear congruence. Notice also that $ax \equiv b(mod\, m)$ is equivalent to a linear Diophantine equation i.e. there exists y such that $ax - my = b$. We now prove theorems about the solutions of linear congruences.

Theorem 26. *Let a, b and m be integers such that $m > 0$ and let $c = (a, m)$. If c does not divide b, then the congruence $ax \equiv b(mod\ m)$ has no solutions. If $c \mid b$, then*

$$ax \equiv b(mod\, m)$$

has exactly c incongruent solutions modulo m.

Proof. As we mentioned earlier, $ax \equiv b(mod\ m)$ is equivalent to $ax - my = b$. By Theorem 19 on Diophantine equations, we know that if c does not divide b, then the equation, $ax - my = b$ has no solutions. Notice also that if $c \mid b$, then there are infinitely many solutions whose variable x is given by

$$x = x_0 + (m/c)t$$

Thus the above values of x are solutions of the congruence $ax \equiv b(mod\, m)$. Now we have to determine the number of incongruent solutions that we have. Suppose that two solutions are congruent, i.e.

$$x_0 + (m/c)t_1 \equiv x_0 + (m/c)t_2(mod\, m).$$

Thus we get

$$(m/c)t_1 \equiv (m/c)t_2(mod\, m).$$

Now notice that $(m, m/c) = m/c$ and thus

$$t_1 \equiv t_2(mod\ c).$$

Thus we get a set of incongruent solutions given by $x = x_0 + (m/c)t$, where t is taken modulo c. □

Remark 2. *Notice that if $c = (a, m) = 1$, then there is a unique solution modulo m for the equation $ax \equiv b(mod\, m)$.*

Example 29. *Let us find all the solutions of the congruence $3x \equiv 12(mod\ 6)$. Notice that $(3, 6) = 3$ and $3 \mid 12$. Thus there are three incongruent solutions modulo 6. We use the Euclidean algorithm to find the solution of the equation $3x - 6y = 12$ as described in chapter 2. As a result, we get $x_0 = 6$. Thus the three incongruent solutions are given by $x_1 = 6(mod\ 6)$, $x_1 = 6 + 2 = 2(mod\ 6)$ and $x_2 = 6 + 4 = 4(mod\ 6)$.*

As we mentioned earlier in Remark 2, the congruence $ax \equiv b(mod\, m)$ has a unique solution if $(a, m) = 1$. This will allow us to talk about modular inverses.

Definition 17. *A solution for the congruence $ax \equiv 1(mod\, m)$ for $(a, m) = 1$ is called the modular inverse of a modulo m. We denote such a solution by $\bar{a}$.*

Example 30. *The modular inverse of 7 modulo 48 is 7. Notice that a solution for $7x \equiv 1(mod\ 48)$ is $x \equiv 7(mod\ 48)$.*

Exercises

1. Find all solutions of $3x \equiv 6(mod\ 9)$.

2. Find all solutions of $3x \equiv 2(mod\ 7)$.

3. Find an inverse modulo 13 of 2 and of 11.

4. Show that if $\bar{a}$ is the inverse of a modulo m and $\bar{b}$ is the inverse of b modulo m, then $\bar{a}\bar{b}$ is the inverse of ab modulo m.

3.4 The Chinese Remainder Theorem

In this section, we discuss the solution of a system of congruences having different moduli. An example of this kind of systems is the following; find a number that leaves a remainder of 1 when divided by 2, a remainder of 2 when divided by three and a remainder of 3 when divided by 5. This kind of question can be translated into the language of congruences. As a result, in this chapter, we present a systematic way of solving this system of congruences.

Theorem 27. *The system of congruences*

$$\begin{aligned} x &\equiv b_1 (mod\, n_1), \\ x &\equiv b_2 (mod\, n_2), \\ &. \\ &. \\ &. \\ x &\equiv b_t (mod\, n_t), \end{aligned}$$

has a unique solution modulo $N = n_1 n_2 ... n_t$ *if* $n_1, n_2, ..., n_t$ *are pairwise relatively prime positive integers.*

Proof. Let $N_k = N/n_k$. Since $(n_i, n_j) = 1$ for all $i \neq j$, then $(N_k, n_k) = 1$. Hence by Theorem 26 , we can find an inverse y_k of N_k modulo n_k such that $N_k y_k \equiv 1(mod\, n_k)$. Consider now

$$x = \sum_{i=1}^{t} b_i N_i y_i$$

Since

$$N_j \equiv 0(mod\, n_k) \text{ for all } j \neq k,$$

thus we see that

$$x \equiv b_k N_k y_k (mod\, n_k).$$

Also notice that $N_k y_k \equiv 1(mod\ n_k)$. Hence x is a solution to the system of t congruences. We have to show now that any two solutions are congruent modulo N. Suppose now that you have two solutions x_0, x_1 to the system of congruences. Then

$$x_0 \equiv x_1(mod\, n_k)$$

for all $1 \leq k \leq t$. Thus by Theorem 23, we see that

$$x_0 \equiv x_1(mod\, N).$$

Thus the solution of the system is unique modulo N. □

We now present an example that will show how the Chinese remainder theorem is used to determine the solution of a given system of congruences.

Example 31. *Solve the system*

$$\begin{aligned} x &\equiv 1(mod\, 2) \\ x &\equiv 2(mod\, 3) \\ x &\equiv 3(mod\, 5). \end{aligned}$$

We have $N = 2.3.5 = 30$. *Also*

$$N_1 = 30/2 = 15, N_2 = 30/3 = 10 \textit{and}\ \ N_3 = 30/5 = 6.$$

So we have to solve now $15y_1 \equiv 1(mod\, 2)$. *Thus*

$$y_1 \equiv 1(mod\, 2).$$

In the same way, we find that

$$y_2 \equiv 1(mod\, 3) \textit{and}\ \ y_3 \equiv 1(mod\, 5).$$

As a result, we get

$$x \equiv 1.15.1 + 2.10.1 + 3.6.1 \equiv 53 \equiv 23(mod\, 30).$$

Exercises

1. Find an integer that leaves a remainder of 2 when divided by either 3 or 5, but that is divisible by 4.

2. Find all integers that leave a remainder of 4 when divided by 11 and leaves a remainder of 3 when divided by 17.

3. Find all integers that leave a remainder of 1 when divided by 2, a remainder of 2 when divided by 3 and a remainder of 3 when divided by 5.

3.5 Theorems of Fermat, Euler, and Wilson

In this section we present three applications of congruences. The first theorem is Wilson's theorem which states that $(p-1)!+1$ is divisible by p, for p prime. Next, we present Fermat's theorem, also known as Fermat's little theorem which states that a^p and a have the same remainders when divided by p where $p \nmid a$. Finally we present Euler's theorem which is a generalization of Fermat's theorem and it states that for any positive integer m that is relatively prime to an integer a, $a^{\phi(m)} \equiv 1(mod\, m)$ where ϕ is Euler's ϕ-function. We start by proving a theorem about the inverse of integers modulo primes.

Theorem 28. *Let p be a prime. A positive integer m is its own inverse modulo p if and only if p divides $m+1$ or p divides $m-1$.*

Proof. Suppose that m is its own inverse. Thus

$$m.m \equiv 1(mod\, p).$$

Hence $p \mid m^2 - 1$. As a result,

$$p \mid (m-1) \text{or } \ p \mid (m+1).$$

We get that $m \equiv 1(mod\, p)$ or $m \equiv -1(mod\, p)$.

Conversely, suppose that

$$m \equiv 1(mod\, p)\text{or } m \equiv -1(mod\, p).$$

Thus

$$m^2 \equiv 1(mod\, p).$$

□

Theorem 29. ***Wilson's Theorem*** *If p is a prime number, then p divides $(p-1)!+1$.*

Proof. When $p = 2$, the congruence holds. Now let $p > 2$. Using Theorem 26, we see that for each $1 \leq m \leq p$, there is an inverse $1 \leq \bar{m} \leq p$ such that $m\bar{m} \equiv 1(mod\, p)$. Thus by Theorem 28, we see that the only two integers that have their own inverses are 1 and $p-1$. Hence after coupling the integers from 2 to $p-2$ each with its inverse, we get

$$2.3.....(p-2) \equiv 1(mod\, p).$$

Thus we get

$$1.2.3.....(p-2)(p-1) \equiv (p-1)(mod\, p)$$

As a result, we have $(p-1)! \equiv -1(mod\, p)$. □

Note also that the converse of Wilson's theorem also holds. The converse tells us whether an integer is prime or not.

Theorem 30. *If m is a positive integer with $m \geq 2$ such that*

$$(m-1)! + 1 \equiv 0\ (mod\, m)$$

then m is prime.

Proof. Suppose that m has a proper divisor c_1 and that

$$(m-1)!+1 \equiv 0(mod\, m).$$

That is $m = c_1 c_2$ where $1 < c_1 < m$ and $1 < c_2 < m$. Thus c_1 is a divisor of $(m-1)!$. Also, since

$$m \mid ((m-1)!+1),$$

we get

$$c_1 \mid ((m-1)!+1).$$

As a result, by Theorem 4, we get that

$$c_1 \mid ((m-1)!+1-(m-1)!),$$

which gives that $c_1 \mid 1$. This is a contradiction and hence m is prime. □

We now present Fermat's Theorem or what is also known as Fermat's Little Theorem. It states that the remainder of a^{p-1} when divided by a prime p that doesn't divide a is 1. We then state Euler's theorem which states that the remainder of $a^{\phi(m)}$ when divided by a positive integer m that is relatively prime to a is 1. We prove Euler's Theorem only because Fermat's Theorem is nothing but a special case of Euler's Theorem. This is due to the fact that for a prime number p, $\phi(p) = p-1$.

Theorem 31. ***Euler's Theorem*** *If m is a positive integer and a is an integer such that $(a, m) = 1$, then*

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

Example 32. *Note that $3^4 = 81 \equiv 1(mod\, 5)$. Also, $2^{\phi(9)} = 2^6 = 64 \equiv 1(mod\, 9)$.*

We now present the proof of Euler's theorem.

Proof. Let $k_1, k_2, ..., k_{\phi(m)}$ be a reduced residue system modulo m. By Theorem 25, the set

$$\{ak_1, ak_2, ..., ak_{\phi(m)}\}$$

also forms a reduced residue system modulo m. Thus

$$ak_1ak_2...ak_{\phi(m)} = a^{\phi(m)}k_1k_2...k_{\phi(m)} \equiv k_1k_2...k_{\phi(m)}(mod\, m).$$

Now since $(k_i, m) = 1$ for all $1 \leq i \leq \phi(m)$, we have $(k_1k_2...k_{\phi(m)}, m) = 1$. Hence by Theorem 22 we can cancel the product of k's on both sides and we get

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

□

An immediate consequence of Euler's Theorem is:

Corollary 1. ***Fermat's Theorem*** *If p is a prime and a is a positive integer with $p \nmid a$, then*

$$a^{p-1} \equiv 1(mod\, p).$$

We now present a couple of theorems that are direct consequences of Fermat's theorem. The first states Fermat's theorem in a different way. It says that the remainder of a^p when divided by p is the same as the remainder of a when divided by p. The other theorem determines the inverse of an integer a modulo p where $p \nmid a$.

Theorem 32. *If p is a prime number and a is a positive integer, then $a^p \equiv a(mod\, p)$.*

Proof. If $p \nmid a$, by Fermat's theorem we know that

$$a^{p-1} \equiv 1(mod\, p).$$

Thus, we get

$$a^p \equiv a(mod\, p).$$

Now if $p \mid a$, we have

$$a^p \equiv a \equiv 0(mod\, p).$$

□

Theorem 33. *If p is a prime number and a is an integer such that $p \nmid a$, then a^{p-2} is the inverse of a modulo p.*

Proof. If $p \nmid a$, then Fermat's theorem says that

$$a^{p-1} \equiv 1(mod\, p).$$

Hence

$$a^{p-2}a \equiv 1(mod\, p).$$

As a result, a^{p-2} is the inverse of a modulo p. □

Exercises

1. Show that 10!+1 is divisible by 11.
2. What is the remainder when 5!25! is divided by 31?
3. What is the remainder when 5^{100} is divided by 7?
4. Show that if p is an odd prime, then $2(p-3)! \equiv -1(mod\, p)$.
5. Find a reduced residue system modulo 2^m, where m is a positive integer.
6. Show that if $a_1, a_2, ..., a_{\phi(m)}$ is a reduced residue system modulo m, where m is a positive integer with $m \neq 2$, then $a_1 + a_2 + ... + a_{\phi(m)} \equiv 0(mod\, m)$.
7. Show that if a is an integer such that a is not divisible by 3 or such that a is divisible by 9, then $a^7 \equiv a(mod\, 63)$.