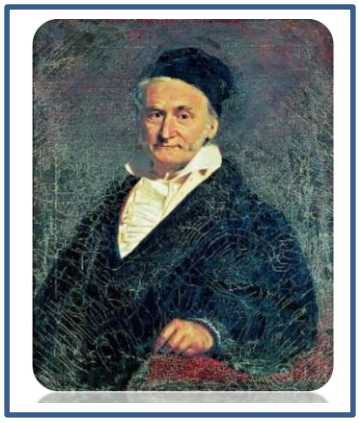
CHAPTER Three

Congruences



Mathematics is the most beautiful and most powerful creation of the human spirit

Johann Carl Friedrich Gauss, a German(1777 –1855).

1. Congruences

A Congruence is nothing more than a statement about divisibility. The theory of congruences was introduced and developed by Carl Friedreich Gauss at the beginning of the nineteenth century. Gauss often referred to as the "Prince of Mathematicians", He introduced many of the basic concepts and notations used in the theory of congruences, such as modular arithmetic and the ≡ symbol, and he established the field's terminology. Moreover, he 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.

1.1. Introduction to Congruences

Congruences have a wide range of applications in number theory and mathematics as a whole. They are crucial for solving diophantine equations, understanding the properties of prime numbers, and exploring the divisibility of integers. Additionally, congruences play a vital role in areas such as cryptography, computer science, and algebraic number theory.

Definition 1 Let m be a positive integer. We say that $\boldsymbol{a}$ is congruent to $\boldsymbol{b}$ 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 $a \equiv b (\mathrm{mod}\ m)$.

Example $24.19 \equiv 5 (\mathrm{mod}\ 7)$.

Similarly $2k + 1 \equiv 1 (\mathrm{mod}\ 2)$ 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 1 Let a, b, c and d denote integers. Let m be a positive integers. Then:

1. If $a \equiv b (\text{mod } m)$, then $b \equiv a (\text{mod } m)$.
2. If $a \equiv b (\text{mod } m)$, and $b \equiv c (\text{mod } m)$, then $a \equiv c (\text{mod } m)$.
3. If $a \equiv b (\text{mod } m)$, then $a + c \equiv b + c (\text{mod } m)$.
4. If $a \equiv b (\text{mod } m)$, then $a - c \equiv b - c (\text{mod } m)$.
5. If $a \equiv b (\text{mod } m)$, then $ac \equiv bc (\text{mod } m)$.
6. If $a \equiv b (\text{mod } m)$, then $ac \equiv bc (\text{mod } mc)$, for $c > 0$.
7. If $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$ then $a + c \equiv (b + d) (\text{mod } m)$.
8. If $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$ then $a - c \equiv (b - d) (\text{mod } m)$.
9. If $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$ then $ac \equiv bd (\text{mod } m)$.

Proof.

(1) If $a \equiv b (\text{mod } m)$, 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 $b \equiv a (\text{mod } m)$.

(2) Since $a \equiv b (\text{mod } m)$, then $m \mid (a - b)$. Also, $b \equiv c (\text{mod } m)$, 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 $a \equiv c (\text{mod } m)$.

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

$m \mid ((a + c) - (b + c))$, and as a result $a + c \equiv b + c (\text{mod } m)$.

(4) Since $a \equiv b(\text{mod}m)$, 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 $a-c \equiv b-c(\text{mod}m)$.

(5) If $a \equiv b(\text{mod}m)$, 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 $ac \equiv bc(\text{mod}\, m)$.

(6) If $a \equiv b(\text{mod}m)$, 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 $ac \equiv bc(\text{mod}\, mc)$.

Example 1 Because $14 \equiv 8(\text{mod}6)$ then $8 \equiv 14(\text{mod}6)$.

Because $22 \equiv 10(\text{mod}6)$ and $10 \equiv 4(\text{mod}6)$. Notice that $22 \equiv 4(\text{mod}6)$.

Because $50 \equiv 20(\text{mod}15)$, then $50+5 = 55 \equiv 20+5 = 25(\text{mod}15)$.

Because $50 \equiv 20(\text{mod}15)$, then $50-5 = 45 \equiv 20-5 = 15(\text{mod}15)$.

Because $19 \equiv 16(\text{mod}3)$, then $2(19) = 38 \equiv 2(16) = 32(\text{mod}3)$.

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

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

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

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

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 nonzero 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 2 If a, b, c and m are integers such that $m > 0, d = (m, c)$ and $ac \equiv bc(\text{mod } m)$, then $a \equiv b(\text{mod } \frac{m}{d})$, if $(m, c) = 1$ and $ac \equiv bc(\text{mod } m)$ then $a = b(\text{mod } m)$.

Proof. For **part 1**, if $ac \equiv bc(\text{mod } m)$, 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 $a \equiv b(\text{mod } m/d)$.

P**art 2** follows immediately from Part 1.

Example $238 \equiv 10(\text{mod}7)$. Since $(2,7) = 1$ then $19 \equiv 5(\text{mod}7)$.

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

Theorem 3 If $a \equiv b(\text{mod } m_1), a \equiv b(\text{mod } m_2), \dots, a \equiv b(\text{mod } m_t)$,

where $a, b, m_1, m_2, \dots, m_t$ are integers and $m_1, m_2, \dots, m_t$ are positive, then

$a \equiv b(\text{mod}\langle m_1, m_2, \dots m_t\rangle)$.

2. Exercises

1. Determine whether 3 and 99 are congruent modulo 7 or not.
2. Show that if x is an odd integer, then $x^2 \equiv 1(\text{mod}8)$

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

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

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

3. 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 nonnegative residue of a modulo m. As a result, we see that any integer is congruent to one of the integers $0,1,2, \dots, m-1$ modulo m.

Definition 2 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 $0,1,2, \dots, m-1$. Every integer is congruent to one of these integers modulo m.

Example 3 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 3 A reduced residue system modulo m is a set of integers r_i such that $(r_i, m) = 1$ for all i and $r_i \neq r_j(\text{mod} m)$ 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 4 The set of integers $\{1,5\}$ is a reduced residue system modulo 6 .

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

Lemma 1 A set of m incongruent integers modulo m forms a complete residue system modulo m.

Theorem 4 If $a_1, a_2, \dots, a_m$ is a complete residue system modulo m, and if k is a positive integer with $(k, m) = 1$, then

$$ka_1 + b, ka_2 + b, \dots, ka_m + b$$

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

4. Euler's Phi- Function


LEONARDO EULER (1707-1783)

Leonhard Euler **(1707–1783)** was born in Basel, **Switzerland**. At the age of 13 he enrolled at the University of Basel, and in **1723**, received his **Master of Philosophy** with a dissertation that compared the philosophies of Descartes and Newton. At this time, he was receiving Saturday afternoon lessons from Johann Bernoulli, who quickly discovered his new pupil's incredible talent for mathematics.

He was a pioneering Swiss mathematician and physicist. He made important discoveries in fields as diverse as infinitesimal calculus and graph theory. He also introduced much of the modern mathematical terminology and notation, particularly for mathematical analysis, such as the notion of a mathematical function. He is also renowned for his work in mechanics, fluid dynamics, optics, astronomy, and music theory.

Euler is considered to be the pre-eminent mathematician of the 18th century and one of the greatest mathematicians to have ever lived. He is also one of the most prolific mathematicians; his collected works fill 60–80 quarto volumes.

Definition For $\boldsymbol{n \geq 1}$, let $\boldsymbol{\varphi(n)}$ denote the number of positive integers not exceeding n that are relatively prime to $\boldsymbol{n}$. The function $\boldsymbol{\varphi(n)}$ is called Euler's phi-function.

As an illustration of the definition, we find that $\boldsymbol{\varphi(30) = 8}$; for, among the positive integers that do not exceed 30, there are eight that are relatively prime to 30; specifically, 1, 7, 11, 13, 17, 19, 23, 29.

Similarly, for the first few positive integers, we may check that

n	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4

Notice that if $\boldsymbol{p}$ is a prime number then every integer less than $\boldsymbol{p}$ is relatively prime to $\boldsymbol{p}$. So for prime numbers we have the formula

$\boldsymbol{\varphi(p) = p - 1}$ if and only if $\boldsymbol{p}$ is prime.

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

Theorem 5 If $a_1, a_2, \dots, a_{\varphi(n)}$ is a reduced residue system modulo n and $(k, n) = 1$, then $ka_1, ka_2, \dots, ka_{\varphi(n)}$ is a reduced residue system modulo n.

5. Exercises

1. Give a reduced residue system modulo 12 .
2. Give a complete residue system modulo 13 consisting only of odd integers.

   Find $\phi(8)$ and $\phi(101)$.

Theorem (Gauss) For any positive integer $\boldsymbol{n}$,

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

Example A simple example of what we have just said is provided by $\boldsymbol{n = 10}$.

These contain $\boldsymbol{\varphi(10) = 4}$, $\boldsymbol{\varphi(5) = 4}$, $\boldsymbol{\varphi(2) = 1}$ and $\boldsymbol{\varphi(1) = 1}$ integers respectively. Therefore

$$\boldsymbol{\sum_{d|10} \varphi(d) = \varphi(10) + \varphi(5) + \varphi(2) + \varphi(1) = 10.}$$

Theorem The function φ is a multiplicative function, i.e., if $\boldsymbol{\gcd(m, n) = 1}$, then $\boldsymbol{\varphi(m.n) = \varphi(m).\varphi(n)}$.

Theorem Let $\boldsymbol{p}$ be prime and $\boldsymbol{k > 0}$, then

$$\boldsymbol{\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right) = p^{k-1}(p-1).}$$

Proof The only numbers between $\boldsymbol{1}$ and $\boldsymbol{p^k}$ that are not relatively prime to $\boldsymbol{p^k}$ are the ones that are divisible by $\boldsymbol{p}$, and they are of the form

$\boldsymbol{p, 2p, 3p, \dots, p^{k-1}p}$. There are $\boldsymbol{\frac{p^k}{p} = p^{k-1}}$ of these. So we have that

$$\boldsymbol{\varphi(p^k) = p^k - p^{k-1}.}\blacksquare$$

Example We have

$$\boldsymbol{\varphi(9) = \varphi(3^2) = 3^2 - 3 = 6} \text{ and } \boldsymbol{\varphi(2401) = \varphi(7^4) = 7^4 - 7^3 = 2058.}$$

Theorem If the integer $\boldsymbol{n > 1}$ has the prime factorization $\boldsymbol{n = p_1^{k_1}p_2^{k_2} \dots p_r^{k_r}}$ where $\boldsymbol{p_1, p_2, \dots, p_r}$ are distinct primes, then

$$\boldsymbol{\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right).}$$

Proof Since $\boldsymbol{p_1, p_2, \dots, p_r}$ are distinct primes, then $\boldsymbol{\gcd\left(p_i^{k_i}, p_j^{k_j}\right) = 1, \text{for } i \neq j.}$

Hence, by the multiplicative formula we have

$$\boldsymbol{\varphi(n) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \dots \varphi(p_r^{k_r})}$$

Then we use the power formula to get

$$\boldsymbol{\varphi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \dots (p_r^{k_r} - p_r^{k_r-1}),}$$

or, $\boldsymbol{\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right).}$

Example We have

$$\boldsymbol{\varphi(1512) = \varphi(2^3 3^3 7) = 1512\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 432.}$$

Exercise Find all values of $\boldsymbol{n}$ that solve each of the following equations.

(1) $\boldsymbol{\varphi(n) = \frac{n}{2}}$, **(2)** $\boldsymbol{\varphi(n) = \frac{n}{3}}$, **(3)** $\boldsymbol{\varphi(n) = \frac{n}{6}}$.

5.1. 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 $ax \equiv b(\mathrm{mod} m)$ 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 $x_i \equiv x_0(\mathrm{mod}\, m)$ are solutions of the linear congruence. Notice also that $ax \equiv b(\mathrm{mod}\, m)$ 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 6 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 $ax \equiv b(\mathrm{mod}\, m)$ has no solutions. If $c \mid b$, then

$$ax \equiv b(\mathrm{mod}\, m)$$

has exactly c incongruent solutions modulo m.

Proof. As we mentioned earlier, $ax \equiv b(\text{mod } m)$ 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 $ax \equiv b(\text{mod}m)$. Now we have to determine the number of incongruent solutions that we have. Suppose that two solutions are congruent, i.e.

$$x_0 + (m/c)t_1 \equiv x_0 + (m/c)t_2(\text{mod}m).$$

Thus we get

$$(m/c)t_1 \equiv (m/c)t_2(\text{mod}m)$$

Now notice that $(m, m/c) = m/c$ and thus $t_1 \equiv t_2(\text{mod } c)$.

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

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

Example 6 Let us find all the solutions of the congruence $3x \equiv 12(\text{mod}6)$. 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

$x = x_0 + (m/c)t$, for $t = 0,1,2$.

Hence, $x_0 = 6 = 0(\text{mod } 6)$, $x_1 = 6 + 2 = 2(\text{mod } 6)$ and $x_2 = 6 + 4 = 4(\text{mod } 6)$.

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

Definition 5 A solution for the congruence $ax \equiv 1(\text{mod}m)$ for $(a, m) = 1$ is called the modular inverse of a modulo m. We denote such a solution by $\bar{a}$.

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

Example 8 Solve the linear congruence $\mathbf{18}x \equiv \mathbf{30}\ (\boldsymbol{mod}\ \mathbf{42})$.

Because $\mathbf{gcd}(\mathbf{18}, \mathbf{42}) = \mathbf{6}$ and $\mathbf{6}$ surely divides $\mathbf{30}$, then we have exactly six solutions, which are incongruent modulo 4. We see that, one solution is found to be $\boldsymbol{x_0} = \mathbf{4}$ **(Check)**.

The six solutions are as folows

$$\boldsymbol{x \equiv 4 + \left({}^{42}/_{6}\right) t \equiv 4 + 7t(mod\ 42),\ t = 0, 1, 2, 3, 4, 5.}$$

Or, $\boldsymbol{x \equiv 4, 11, 18, 25, 32, 39\ (mod\ 42)}$**.**

Example 9 Solve the linear congruence $\mathbf{13}x \equiv \mathbf{1}\ (\boldsymbol{mod}\ \mathbf{42})$.

First we shall find **gcd(42, 13)**.

42=3(13)+3

13=4(3)+1

3=3(1)+0

Thus, **gcd(42, 13)= 1**. Therefor the equation has a unique solution.

Next, we reverse the steps to find the solution to the given equation.

3=42-3(13)

1=13-4(3)

=13-4(42)+12(13)

=13(13)-4(42)

Therefore, the solution is $\boldsymbol{x_0 = 13.}$ Or, the (multiplicative) inverse of $\boldsymbol{a = 13}$ modulo **42** is $\boldsymbol{13^{-1}(mod\ 42) = 13.}$

6. Exercises

1. Find all solutions of $3x \equiv 6(\mathrm{mod}9)$.
2. Find all solutions of $3x \equiv 2(\mathrm{mod}7)$.
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.

6.1. 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.

The Chinese Remainder Theorem (CRT) has ancient roots, dating back to ancient China around the 3rd century. Sunzi Suanjing, a Chinese mathematical text, introduced a method resembling CRT. However, the modern formulation is credited to the Chinese mathematician Qin Jiushao in the 13th century. The CRT gained prominence in the West through translations of Chinese mathematical works in the 17th century. It has since

become a fundamental concept in number theory and modular arithmetic, with applications in cryptography and computer science.

Theorem 7 (Chinese Remainder Theorem) If $n_1, n_2, \dots, n_t$ are pairwise relatively prime positive integers, then the system of linear congruences

$x \equiv b_1 (\text{mod } n_1)$, $x \equiv b_2 (\text{mod } n_2)$, …, $x \equiv b_t (\text{mod } n_t)$,

has a unique solution modulo $N = n_1 n_2 \dots n_t$ given by

$$\tilde{x} \equiv \boldsymbol{b_1 N_1 x_1 + b_2 N_2 x_2 + \cdots + b_t N_t x_t},$$

in which $\boldsymbol{N_k = \frac{N}{n_k}}$ and $\boldsymbol{x_k}$is the unique solution to the congruence

$\boldsymbol{N_k x \equiv 1 \ (mod \ n_k)}$, for $\boldsymbol{k = 1, 2, \dots, t}$.

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 8 Solve the system of linear congruences

$x \equiv 1 (\text{mod } 2)$, $x \equiv 2 (\text{mod } 3)$, $x \equiv 3 (\text{mod } 5)$.

We have $N = 2.3.5 = 30$. Also

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

So we have to solve $15y_1 \equiv 1 (\text{mod } 2)$, $10y_2 \equiv 1 (\text{mod } 3)$, and $6y_3 \equiv 1 (\text{mod } 5)$.

Thus $y_1 \equiv 1 (\text{mod } 2)$.

In the same way, we find that $y_2 \equiv 1 (\text{mod } 3)$ and $y_3 \equiv 1 (\text{mod } 5)$

As a result, we get

$$x \equiv 1.15.1 + 2.10.1 + 3.6.1 \equiv 53 \equiv 23 (\text{mod } 30).$$

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 .

7.1. 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 $a, a^{\phi(m)} \equiv 1(\mathrm{mod} m)$ where ϕ is Euler's ϕ-function. We start by proving a theorem about the inverse of integers modulo primes.

Theorem 8 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

$$m.m \equiv 1(\mathrm{mod}\, p)$$

Hence, from the definition of congruence we have $p \mid m^2-1$.

As a result, $p \mid (m-1)$ or $p \mid (m+1)$.

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

Conversely, suppose that

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

Thus

$$m^2 \equiv 1(\text{mod } p)$$

Theorem 9 (Wilson's Theorem) $\boldsymbol{p > 1}$ is a prime, then

$\boldsymbol{(p-1)! \equiv -1\ (mod\ p).}$ **(**If p is a prime number, then p divides $(p-1)! + 1$.)

Proof When $p = 2$, the congruence holds. Suppose that $\boldsymbol{p}$ is an odd prime. We know that every number $\boldsymbol{x}$in the set $\boldsymbol{\{1, 2, \dots, p-1\}}$ has an inverse $\boldsymbol{y\ (mod\ p).}$

The only numbers which are equal to their inverses are $\boldsymbol{1}$ and $\boldsymbol{p-1.}$ The other $\boldsymbol{p-3}$ numbers in the range can be paired with their inverses, so that the product of each pair is congruent to $\boldsymbol{1\ (mod\ p).}$ Now, multiplying all these numbers together gives

$$\boldsymbol{(p-1)! = (p-1) \times (p-2) \dots 2 \times 1 \equiv (p-1).(1)^{(p-3)}.1 \equiv -1\ (mod\ p).}$$

Theorem 10 If m is a positive integer with $m \geq 2$ such that

$(m-1)! + 1 \equiv 0(\text{mod } m)$, then m is prime.

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

$$(m-1)! + 1 \equiv 0(\text{mod } m)$$

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.

Theorem 11 (Euler's Theorem) If m is a positive integer and a is an integer such that $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 (\text{mod } m)$.

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

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

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 12 If p is a prime number and a is a positive integer, then $a^p \equiv a (\text{mod } p)$

Proof. If $p \nmid a$, by Fermat's theorem we know that $a^{p-1} \equiv 1 (\text{mod } p)$.

Thus, we get $a^p \equiv a (\text{mod } p)$.

Now if $p \mid a$, we have

$$a^p \equiv a \equiv 0 (\text{mod } p)$$

Theorem 13 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 $a^{p-1} \equiv 1 (\text{mod } p)$.

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

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

8. 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 $2(p-3)! \equiv -1 (\text{mod } p)$.
5. Find a reduced residue system modulo 2^m, where m is a positive integer.
6. Show that if $a_1, a_2, \ldots, a_{\phi(m)}$ is a reduced residue system modulo m, where m is a positive integer with $m \neq 2$, then $a_1 + a_2 + \cdots + a_{\phi(m)} \equiv 0 (\text{mod } m)$.
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 $a^7 \equiv a (\text{mod } 63)$.