# Number Theory and Graph Theory

## Chapter 2

## Prime numbers and congruences.

By

**A. Satyanarayana Reddy**

Department of Mathematics

Shiv Nadar University

Uttar Pradesh, India

**E-mail:** satya8118@gmail.com

## Module-4: Introduction to Congruences

Objectives

- Introduction to Congruence and its properties.
- System of residues.
- Applications of congruences in divisibility.
- Fermat Little Theorem.

**Definition 1.** *Let $n$ be a positive integer and $a,b \in \mathbb{Z}$. Then $a$ and $b$ are said to be* congruent modulo *$n$ or $a$ is said to be* congruent to $b$ modulo $n$, *denoted $a \equiv b \pmod{n}$, if $n$ divides $a-b$. That is, there exists $k \in \mathbb{Z}$ such that $a-b=kn$.*

- Since 1 divides every integer. So any two integers are congruent modulo 1.
- Two integers are congruent modulo 2 if and only if either both are even or both are odd.
- Let $a \in \mathbb{Z}, n \in \mathbb{N}$. Then, by division algorithm we have $a = nq + r$, where $0 \leq r < n$. In other words, $a \equiv r \pmod{n}$. Since $r \in \{0,1,2,\ldots,n-1\}$, every integer is congruent to exactly one of the element from the set $\{0,1,2,\ldots,n-1\}$. This set is called the *set of least residues* modulo $n$.
- Fix a positive integer $m$ and let $b_1,b_2,\ldots,b_m$ be any collection of $m$ integers that are congruent to $0,1,2,\ldots,m-1$ is some order. Then, the set $\{b_1,b_2,\ldots,b_m\}$ is called a *complete system of residues* modulo $m$. It is easy to see that set of least residues is also a complete system of residues. And the set of complete system of residues is not unique. In fact, it is easy to see that any set of $m$ integers is complete system of residues if and only if no two of them are congruent modulo $m$.

**Theorem 2.** *Let $m > 1$ be a fixed positive integer and let $a, b, c \in \mathbb{Z}$. Then, the following hold:*

1. $a \equiv a \pmod{m}$.
2. *If* $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$.
3. *If* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$.
4. *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $a \pm c \equiv b \pm d \pmod{m}$ *and* $ac \equiv bd \pmod{m}$.
5. *If* $a \equiv b \pmod{m}$, *then* $a + c \equiv b + c \pmod{m}$ *and* $ac \equiv bc \pmod{m}$ *for any* $c \in \mathbb{Z}$.
6. *If* $a \equiv b \pmod{m}$, *then* $a^n \equiv b^n \pmod{m}$ *for any positive integer* $n$.
7. *If* $ac \equiv bc \pmod{m}$, *then* $a \equiv b \pmod{\frac{m}{d}}$, *where* $d = \gcd(c, m)$.
8. *If* $a \equiv b \pmod{m}$, *and* $k|m$ *then* $a \equiv b \pmod{k}$.
9. *If* $a \equiv b \pmod{m}$ *and* $c \in \mathbb{N}$, *then* $ca \equiv cb \pmod{cm}$.
10. *If* $a \equiv b \pmod{m}$ *and the integers* $a, b, m$ *are all divisible by* $d > 0$, *then* $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

*Proof.* Proof of Part 1: Since $m|0 = a - a$, $a \equiv a \pmod{m}$.

Proof of Part 2: Since $a \equiv b \pmod{m}$, so $m \mid a - b$. Hence, $a - b = mq$. Thus, $m \mid m(-q) = b - a$. Hence, $b \equiv a \pmod{m}$.

Proof of Part 3: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $m \mid a - b$ and $m \mid b - c$. Hence, by the linearity property $m \mid a - c = (a - b) + (b - c)$ and thus $a \equiv c \pmod{m}$.

Proof of Part 4: Since $a - c = a + (-c)$, it suffices to prove only the "+ case." By assumption, $m \mid a - b$ and $m \mid c - d$. Therefore, by linearity, $m \mid (a + c) - (b + d) = (a - b) + (c - d)$ and $m|c(a - b) + b(c - d) = ac - bd$. Hence

$$a + c \equiv b + d \pmod{m} \text{ and } ac \equiv bd \pmod{m}.$$

Proof of Part 5: Since $a \equiv b \pmod{m}$, $m \mid a - b$. Thus, $m \mid c(a - b)$ and $m \mid (a + c - c - b) = a - b$. Hence, $a + c \equiv b + c \pmod{m}$ and $ac \equiv bc \pmod{m}$.

Proof of Part 6: We prove $a^n \equiv b^n \pmod{m}$ by induction on $n$.

If $n = 1$, the result is true by the assumption that $a \equiv b \pmod{m}$.

Assume that the result holds for $n = k$. That is, $a^k \equiv b^k \pmod{m}$. We also have $a \equiv b \pmod{m}$. Thus, $aa^k \equiv bb^k \pmod{m}$ or equivalently, $a^{k+1} \equiv b^{k+1} \pmod{m}$. Hence, by the Principle of Mathematical Induction (PMI), the result holds for all $n \in \mathbb{N}$.

Proof of Part 7: As $ac \equiv bc \pmod{m}$, we get $m \mid ac - bd = c(a-b)$. Thus, $c(a-b) = mk$, for some $k \in \mathbb{Z}$. Since, $(c,m) = d$, $c = dk_1$ and $m = dk_2$, for some $k_1, k_2 \in \mathbb{Z}$. Thus, $dk_1(a-b) = dk_2$ or $k_2 | a-b$ as $\gcd(k_1, k_2) = 1$.

Thus, $a \equiv b \pmod{k_2 = \frac{m}{d}}$.

Proof of Part 8, 9 and 10 are left for the readers. $\square$

**Definition 3.** *Let $m \in \mathbb{N}$ be a given. For each $a \in \mathbb{Z}$, the* ***residue class*** *(or the* congruence class *or* equivalence class*) of a* ***modulo*** *m, denoted $[a]$ or $[a]_m$, is defined as*

$$[a] = \{x \in \mathbb{Z} | x \equiv a \pmod{m}\}.$$

Thus, the set $\{[0], [1], [2], \ldots, [m-1]\}$, denoted $\mathbb{Z}_m$, has some nice properties.

**Theorem 4.** *Let $p(x) = \sum\limits_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficients $c_k$. If $a \equiv b \pmod{n}$, then $p(a) \equiv p(b) \pmod{n}$.*

*Proof.* Since, $a \equiv b \pmod{n}$, we have seen that $a^k \equiv b^k \pmod{n}$ and hence, $c_k a^k \equiv c_k b^k \pmod{n}$, for $k = 0, 1, 2, \ldots, m$. Adding these $m+1$ congruences, we get

$$p(a) = \sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k = p(b) \pmod{n}.$$

$\square$

If $p(x)$ is a polynomial with integral coefficients, we say that $a$ is a solution of the congruence $p(x) \equiv 0 \pmod{n}$ if $p(a) \equiv 0 \pmod{n}$.

**Corollary 5.** *If a is a solution of $p(x) \equiv 0 \pmod{n}$ and $a \equiv b \pmod{n}$, then b is also a solution of $p(x) \equiv 0 \pmod{n}$.*

**Theorem 6.** *Let $M = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + 10a_1 + a_0$ be the decimal expansion of the positive integer $M$, $0 \le a_k < 10$, and let $S = a_0 + a_1 + \cdots + a_m$. Then, $9|M$ if and only if $9|S$.*

*Proof.* Let $p(x) = \sum\limits_{k=0}^{m} a_k x^k$. Then $p(10) = M$ and $p(1) = S$. But, $10 \equiv 1 \pmod 9$ and hence $p(10) \equiv p(1) \pmod 9$. Thus, we have $M \equiv S \pmod 9$. □

**Theorem 7.** *Let $M = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + 10a_1 + a_0$ be the decimal expansion of the positive integer $M$, $0 \le a_k < 10$, and let $T = a_0 - a_1 + \cdots + (-1)^m a_m$. Then, $11|M$ if and only if $11|T$.*

*Proof.* Let $p(x) = \sum\limits_{k=0}^{m} a_k x^k$. Then $p(10) = M$ and $p(-1) = T$. As $10 \equiv -1 \pmod{11}$, we get $p(10) \equiv p(-1) \pmod{11}$ and hence, $M \equiv T \pmod{11}$. □

### Fermat's Little Theorem

It is easy to see that

$$\begin{aligned}
1^4 &\equiv 1 \pmod 5;\ 2^4 \equiv 1 \pmod 5;\ 3^4 \equiv 1 \pmod 5;\ 4^4 \equiv 1 \pmod 5 \\
5^4 &\equiv 0 \pmod 5 \\
6^4 &\equiv 1 \pmod 5;\ 7^4 \equiv 1 \pmod 5;\ 8^4 \equiv 1 \pmod 5;\ 9^4 \equiv 1 \pmod 5 \\
10^4 &\equiv 0 \pmod 5
\end{aligned}$$

**Theorem 8.** *[Fermat's Little Theorem] Let $p$ be a prime and suppose that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod p$.*

*Proof.* We begin by considering the first $p-1$ positive multiples of $a$. That is, consider the integers

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

- None of these numbers is congruent to another modulo $p$.

  Let $ra \equiv sa \pmod p$ for $1 \le r < s \le p-1$. As $p \nmid a$, $a$ can be canceled to give $r \equiv s \pmod p$, which is impossible as $0 < s - r < p$.

- Similarly, it is easy to check that none of these numbers is congruent to zero modulo $p$.

Hence, $\{a \pmod p, 2a \pmod p, \ldots, (p-1)a \pmod p\} = \{1, 2, \ldots, p-1\}$. Therefore,

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod p.$$

Or equivalently,

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod p.$$

Since, $\gcd(p, (p-1)!) = 1$, using Theorem 2.thm:procon:7, we have $a^{p-1} \equiv 1 \pmod p$. □

**Corollary 9.** *If $p$ is prime, then $a^p \equiv a \pmod p$ for any integer $a$.*

*Proof.* If $p|a$, then $p|a^p - a$ and hence the result is true.
If $p \nmid a$, then using theorem 8, $a^{p-1} \equiv 1 \pmod p$. Now, multiplying both sides by $a$, we get $a^p \equiv a \pmod p$. □

**Alternate proof:** The result is clearly true for $p = 2$ as both $a$ and $a^2$ have the same parity. Let $p$ be an odd prime, then $a^p$ and $a$ have same sign. Thus, it is sufficient to prove the result for positive integers. So, let us fix a prime $p$ and prove the result using induction on $a$. If $a = 1$, then clearly $a^p \equiv a \pmod p$ holds.

Assume the result holds for $a$, *i.e.*, $a^p \equiv a \pmod p$. We need to prove that $(a+1)^p \equiv (a+1) \pmod p$.

We first observe that since $p$ is a prime $p \mid \binom{p}{k} = \dfrac{p!}{k!(p-k)!}$ for $k = 1, 2, \ldots, p-1$. Hence, $(a+1)^p \equiv a^p + 1 \pmod p$. But, by induction hypothesis, $a^p \equiv a \pmod p$. Hence, we get $(a+1)^p \equiv a^p + 1 \equiv (a+1) \pmod p$.