3.4. Congruence.

Karl Friedrich Gauss (1777-1855), a celebrated German mathematician, introduced the concept of congruence which laid the foundation of modern theory of numbers.

Definition. Let m be a fixed positive integer. Two integers a and b are said to be *congruent modulo* m, if $a - b$ is divisible by m. symbolically this is expressed as $a \equiv b \pmod{m}$.

To illustrate, let $m = 3$. It is easy to verify that

$1 \equiv 4 \pmod 3$, $-2 \equiv 1 \pmod 3$, $6 \equiv 0 \pmod 3$, $35 \equiv 2 \pmod 3$.

When $a - b$ is not divisible by m, a is said to be *incongruent* to b modulo m. It is expressed as $a \not\equiv b \pmod{m}$.

For example, $1 \not\equiv 5 \pmod 3$, $-2 \not\equiv 2 \pmod 3$.

Note. When $m = 1$, every two integers are congruent modulo m and this case is not so useful and interesting. Therefore m is usually taken to be a positive integer greater than 1.

Theorem 3.4.1. For any two integers a and b, $a \equiv b \pmod{m}$ if and only if a and b leave the same remainder when divided by m.

Proof. Let r be the remainder when a is divided by m. Then there exists some integer q such that $a = qm + r, 0 \le r < m$.

Since $a \equiv b \pmod{m}$, $a - b = km$ where k is an integer.

$$\text{Therefore } b = a - km = (qm + r) - km = (q - k)m + r$$

and this shows that b leaves the same remainder r.

Conversely, let r be the same remainder when a and b are divided by m. Then $a = q_1 m + r, b = q_2 m + r$, where q_1, q_2 are integers and $0 \le r < m$.

Therefore $(a - b) = (q_1 - q_2)m$, i.e., $m|(a - b)$ and this proves that $a \equiv b \pmod{m}$.

To illustrate, let $m = 5$. Since $21 \equiv 4.5 + 1$ and $-14 = -3.5 + 1$, 21 and -14 leave the same remainder upon division by 5. Therefore $21 \equiv -14 \pmod 5$.

Properties.

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 $a \equiv b \pmod{m}$, then for any integer c

$$\begin{aligned} a+c &\equiv b+c \pmod{m} \\ ac &\equiv bc \pmod{m}. \end{aligned}$$

5. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$\begin{aligned} a+c &\equiv b+d \pmod{m} \\ ac &\equiv bd \pmod{m}. \end{aligned}$$

6. If $a \equiv b \pmod{m}$ and $d|m$ where $d > 0$, then $a \equiv b \pmod{d}$.

Proofs of properties $1-4$ and 6 are immediate.

Proof. **5.** $a \equiv b \pmod{m} \Rightarrow a - b = km$ and
$c \equiv d \pmod{m} \Rightarrow c - d = lm$, where k, l are integers.
$(a + c) - (b + d) = (k + l)m$.

Therefore $a + c \equiv b + d \pmod{m}$ since $k + l$ is an integer.

By property 4,
$a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$ and
$c \equiv d \pmod{m} \Rightarrow bc \equiv bd \pmod{m}$.

Therefore $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.

Definition. If $a \equiv b \pmod{m}$, then b is said to be a *residue* of a modulo m.

By division algorithm there exist integers q and r satisfying $a = qm+r$ with $0 \leq r \leq m - 1$.

Since $a - r = qm$, $a \equiv r \pmod{m}$ and this shows that r is a residue of a modulo m. r is said to be the *least non-negative residue* of a modulo m.

Let a be an arbitrary integer. Upon division by m, a leaves one and only one of the integers $0, 1, 2, \ldots, m - 1$ as the remainder.

Therefore whatever the integer a may be, the least non-negative residue of a is one and only one of $0, 1, 2, \ldots, m - 1$.

The whole set of integers is divided into m distinct and disjoint subsets, called the *residue classes modulo* m, denoted by $\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{m-1}$ and defined by

$$\begin{aligned}
\bar{0} &= \{0, \pm m, \pm 2m, \ldots\} \\
\bar{1} &= \{1, 1 \pm m, 1 \pm 2m, \ldots\} \\
\bar{2} &= \{2, 2 \pm m, 2 \pm 2m, \ldots\} \\
&\cdots \quad \cdots \quad \cdots \\
\overline{m-1} &= \{m - 1, (m - 1) \pm m, (m - 1) \pm 2m, \ldots\}.
\end{aligned}$$

Any two integers in a residue class are congruent modulo m and any two integers belonging to two different residue classes are incongruent modulo m.

Theorem 3.4.2. If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for all positive integers n.

Proof. We use the principle of induction to prove the theorem.

The theorem is true for $n = 1$.

Let us assume that the theorem is true for some positive integer k. Then $a^k \equiv b^k \pmod{m}$.

$a^k \equiv b^k \pmod{m}$ and $a \equiv b \pmod{m}$ together imply that

$a^k.a \equiv b^k.b \pmod{m}$, i.e., $a^{k+1} \equiv b^{k+1} \pmod{m}$.

This shows that the thoerem is true for the positive integer $k + 1$ if we assume it to be true for k.

By the principle of induction, the theorem is true for all positive integers n.

Note. The converse of the theorem fails to hold.

$a^k \equiv b^k \pmod{m}$ does not necessarily imply $a \equiv b \pmod{m}$.

For example, $9^2 \equiv 7^2 \pmod{8}$ but $9 \not\equiv 7 \pmod{8}$

$4^3 \equiv 7^3 \pmod{9}$ but $4 \not\equiv 7 \pmod{9}$.

Theorem 3.4.3. If $ax \equiv ay \pmod{m}$ and a is prime to m, then $x \equiv y \pmod{m}$.

Proof. $ax - ay = km$, where k is an integer

or, $x - y = \frac{km}{a}$.

Since $x - y$ is an integer, $a|km$. Since a is prime to m and $a|km$, it follows that $a|k$. Therefore $k = aq$, where q is an integer.

Hence $x - y = qm$ and this proves the theorem.

Note. $ax \equiv ay \pmod{m}$ does not necessarily imply $x \equiv y \pmod{m}$.

For example, $3.2 \equiv 3.4 \pmod{6}$ does not imply $2 \equiv 4 \pmod{6}$.

We can cancel the common factor a freely from both sides of the congruence (mod m) provided a is prime to m.

$3.-2 \equiv 2 \pmod{8}$, $\quad 3.14 \equiv 2 \pmod{8}$.

Cancelling the factor 3 which is prime to 8 we get the correct congruence $-2 \equiv 14 \pmod{8}$.

Cancellation is allowed however, in some restricted sense which is provided in the following theorem.

Theorem 3.4.4. If $d = gcd(a, m)$, then $ax \equiv ay \pmod{m} \Leftrightarrow x \equiv y \pmod{\frac{m}{d}}$.

Proof. We have $ax - ay = qm$ where q is an integer.

Since $gcd(a, m) = d$, $a = dr$ and $m = ds$ where r and s are integers prime to each other.

Therefore $drx - dry = qds$ or, $x - y = \frac{qs}{r}$.

Since $x - y$ is an integer, $r|qs$.

r is prime to s and $r|qs$ implies $r|q$, i.e., $\frac{q}{r}$ is an integer k.

Therefore $x - y = ks$ and this says $x \equiv y \pmod{\frac{m}{d}}$.

Conversely, $x \equiv y \pmod{\frac{m}{d}} \Rightarrow \frac{m}{d}|(x - y) \Rightarrow m|d(x - y) \Rightarrow m|a(x - y) \Rightarrow ax \equiv ay \pmod{m}$.

Corollary. If $ax \equiv ay \pmod{m}$ and $a|m$, then $x \equiv y \pmod{\frac{m}{a}}$.

For example, $4.7 \equiv 4.10 \pmod{6}$. Cancellation of 4 from both sides does not give a correct congruence because 4 is not prime to 6. Since $gcd(4, 6) = 2$, we get the correct congruence $7 \equiv 10 \pmod{\frac{6}{2}}$.

Again, $4.7 \equiv 4.10 \pmod{12}$. Since $4|12$, we get the correct congruence $7 \equiv 10 \pmod{3}$ from the corollary.

Theorem 3.4.5. $x \equiv y \pmod{m_i}$, for $i = 1, 2, \ldots, r \Leftrightarrow x \equiv y \pmod{m}$, where $m = [m_1, m_2, \ldots, m_r]$, the *lcm* of $m_1, m_2, \ldots, m_r$.

Proof. $x \equiv y \pmod{m_i} \Rightarrow m_i|(x - y)$ for $i = 1, 2, \ldots, r$

$\Rightarrow x - y$ is a common multiple of $m_1, m_2, \ldots, m_r$

$\Rightarrow [m_1, m_2, \ldots, m_r]|(x - y)$, i.e., $m|(x - y)$

$\Rightarrow x \equiv y \pmod{m}$.

Conversely, $x \equiv y \pmod{m} \Rightarrow m|(x - y)$

$\Rightarrow m_1 m_2 \ldots m_r|(x - y)$

$\Rightarrow m_i|(x - y)$ for $i = 1, 2, \ldots, r$

$\Rightarrow x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$.

Corollary. If $x \equiv y \pmod{m_1}$, $x \equiv y \pmod{m_2}$ and m_1, m_2 are relatively prime, then $x \equiv y \pmod{m_1 m_2}$.

Theorem 3.4.6. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integral coefficients a_i.

If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

Proof. Since $a \equiv b \pmod{m}$, $a^k \equiv b^k \pmod{m}$ where k is a positive integer. Therefore $a_i a^k \equiv a_i b^k \pmod{m}$ where a_i is an integer.

Adding these congruences for $i = 0, 1, 2, \ldots, n$, we have

$$a_0 + a_1 a + a_2 a^2 + \cdots + a_n a^n \equiv a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n \pmod{m}$$

or, $f(a) \equiv f(b) \pmod{m}$.

3.4.7. Divisibility tests.

1. Let $n = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_2 10^2 + a_1 10 + a_0$ where a_k are integers and $0 \le a_k \le 9$, $k = 0, 1, \ldots, m$ be the decimal representation of a positive integer n.

Let $S = a_0 + a_1 + \cdots + a_m$, $T = a_0 - a_1 + \cdots + (-1)^m a_m$. Then

(i) n is divisible by 2 if and only if a_0 is divisible by 2;

(ii) n is divisible by 9 if and only if S is divisible by 9;

(iii) n is divisible by 11 if and only if T is divisible by 11.

Proof. Let us consider the polynomial

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0.$$

(i) We have $10 \equiv 0 \pmod 2$.

Therefore $f(10) \equiv f(0) \pmod 2$.

But $f(10) = n$ and $f(0) = a_0$.

Therefore $n - a_0$ is divisible by 2.

Hence n is divisible by 2 if and only if a_0 is divisible by 2.

(ii) We have $10 \equiv 1 \pmod 9$.

Therefore $f(10) \equiv f(1) \pmod 9$.

But $f(10) = n$ and $f(1) = S$.

Therefore $n \equiv S \pmod 9$.

This proves that $N - S$ is divisible by 9.

Hence n is divisible by 9 if and only if S is divisible by 9.

(iii) We have $10 \equiv -1 \pmod{11}$.

Therefore $f(10) \equiv f(-1) \pmod{11}$.

But $f(10) = n$ and $f(-1) = T$.

Therefore $n \equiv T \pmod{11}$.

This proves that $n - T$ is divisible by 11.

Hence n is divisible by 11 if and only if T is divisible by 11.

For example, 35078571 is divisible by 9 since the sum of the digits $3+5+0+7+8+5+7+1 (= 36)$ is divisible by 9.

It is also divisible by 11 because the sum $1-7+5-8+7-0+5-3 (= 0)$ is divisible by 11.

The number 23572 is divisible by 2, since the integer a_0 in the units place is 2 which is divisible by 2. It is not divisible by 9, since the sum $2+3+5+7+2 (= 19)$ is not divisible by 9. It is not divisible by 11, since the sum $2-7+5-3+2 (= -1)$ is not divisible by 11.

2. Let $n = a_m(1000)^m + a_{m-1}(1000)^{m-1} + \cdots + a_1(1000) + a_0$ where a_k are integers and $0 \le a_k \le 999$, $k = 0, 1, \ldots, m$ be the representation of a

positive integer n.

Let $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$. Then

(i) n is divisible by 7 if and only if T is divisible by 7,

(ii) n is divisible by 13 if and only if T is divisible by 13,

(iii) n is divisible by 11 if and only if T is divisible by 11.

Proof. Let us consider the polynomial

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0.$$

(i) We have $1000 \equiv -1 \pmod 7$, since $1001 = 7.11.13$.

$$\text{Therefore } f(1000) \equiv f(-1) \pmod 7.$$

But $f(1000) = n$ and $f(-1) = T$.

$$\text{Therefore } n \equiv T \pmod 7.$$

This implies $n - T$ is divisible by 7.

Hence n is divisible by 7 if and only if T is divisible by 7.

(ii) and (iii) Similar proofs.

To illustrate, let us consider the number $n = 23146123$. n can be expressed as $23(1000)^2 + 146(1000) + 123$.

n is divisible by 7 because the sum $123 - 146 + 23 = 0$ is divisible by 7.

The same argument proves that n is also divisible by 13 and 11.

Worked Examples.

1. Find the least positive residues in $3^{36} \pmod{77}$.

$3^4 \equiv 4 \pmod{77} \Rightarrow 3^{12} \equiv 4^3 \pmod{77} \equiv -13 \pmod{77}$.

This gives $3^{24} \equiv 169 \pmod{77} \equiv 15 \pmod{77}$.

Therefore $3^{36} \equiv 15. - 13 \pmod{77} \equiv 36 \pmod{77}$.

Hence the least positive residue is 36.

2. Use the theory of congruences to prove that $7 | [2^{5n+3} + 5^{2n+3}]$ for all $n \geq 1$.

$2^{5n+3} + 5^{2n+3} = 8.32^n + 125.25^n$.

$32^n - 25^n \equiv 0 \pmod 7$ for all $n \geq 1$.

Therefore $8.32^n - 8.25^n \equiv 0 \pmod 7$ for all $n \geq 1$.

Also we have $133(25)^n \equiv 0 \pmod 7$ for all $n \geq 1$.

Therefore $8.32^n + 125.25^n \equiv 0 \pmod 7$ for all $n \geq 1$.

This implies $7 | [2^{5n+3} + 5^{2n+3}]$ for all $n \geq 1$.

3. Prove that $19^{20} \equiv 1 \pmod{181}$.

$$\begin{aligned} \text{We have } 19^2 &\equiv -1 \pmod{181}, \text{ whence} \\ 19^{20} &\equiv (-1)^{10} \pmod{181}, \text{ by theorem 3.4.2} \\ \text{or, } 19^{20} &\equiv 1 \pmod{181}. \end{aligned}$$

4. Prove that $3.4^{n+1} \equiv 3 \pmod 9$ for all positive integers n.

$$\begin{aligned} 3.4^{n+1} &= 12.4^n = 9.4^n + 3.4^n \\ 3.4^n &= 12.4^{n-1} = 9.4^{n-1} + 3.4^{n-1} \\ \dots & \dots \quad \dots \\ 3.4^2 &= 12.4 = 9.4 + 3.4 \\ 3.4 &= 12 = 9 + 3. \end{aligned}$$

Therefore $3.4^{n+1} = 9(1 + 4 + 4^2 + \cdots + 4^n) + 3$.

Hence $3.4^{n+1} \equiv 3 \pmod 9$.

5. Find the remainder when $1! + 2! + 3! + \cdots + 50!$ is divided by 15.

$5! \equiv 0 \pmod{15}$ and $(5+n)! \equiv 0 \pmod{15}$ for any positive integer n.

Therefore
$$\begin{aligned} 1! + 2! + 3! + \cdots + 50! &\equiv (1! + 2! + 3! + 4!) \pmod{15}. \\ &\equiv 33 \pmod{15} \\ &\equiv 3 \pmod{15}. \end{aligned}$$