by any one of the primes $2, 3, 5, 7, \cdots, p$. Hence the number is either a prime itself or being a composite number, divisible by a prime greater than p. In both cases p fails to be the greatest prime and therefore the number of prime is infinite.

2.5 Congruence relation between integers

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 $m = 3$, then $1 \equiv 4 \pmod 3$ as $1-4$ is divisible by 3. $-2 \equiv 1 \pmod 3$, $6 \equiv 0 \pmod 3$ and $35 \equiv 2 \pmod 3$ as $-2-1 = -3$, $6-0 = 6$ and $35-2 = 33$ are divisible by 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 useful and interesting. So, m is usually taken to be a positive integer greater than 1.

Theorem 2.5.1 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 remainder when a is divided by m. Then there exists 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

So, $b = a - km = qm + r - km$

$= (q-k)m + r$

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 $a = q_1 m + r$ and

$b = q_2 m + r$ where q_1, q_2 are integers and $0 \le r < m$

So, $a - b = (q_1 - q_2)m$. So, $m \mid (a-b)$ and this proves that $a \equiv b \pmod m$.

To illustrate, let $m = 5$. Since $21 = 4.5 + 1$ and $-14 = (-3).5 + 1$

21 and -14 leave the same remainder 1 upon division by 5 So, $21 \equiv -14 \pmod 5$.

Properties

1. $a \equiv a \pmod m$

2. If $a \equiv b \pmod m$ then $b \equiv a \pmod m$

3. If $a \equiv b \pmod m$, $b \equiv c \pmod m$ then $a \equiv c \pmod m$

4. If $a \equiv b \pmod m$ then for any integer c,

$$a+c \equiv (b+c) \pmod m$$
$$ac \equiv bc \pmod m$$

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

$$a+c \equiv (b+d) \pmod m$$
$$ac \equiv bd \pmod m$$

6. If $a \equiv b \pmod m$ and $d \mid m$, $d > 0$ then $a \equiv b \pmod d$.

Proof: 1. $a - a = 0$; so, it is divisible by m.

So, $a \equiv a \pmod m$

2. Given $a \equiv b \pmod m$, so, let $a - b = km$, k is an integer. Then $b - a = (-k)m = k'm$ where $k' = -k$ is an integer So, $b - a$ is divisible by m. So, $b \equiv a \pmod m$

3. Given $a \equiv b \pmod m$ and $b \equiv c \pmod m$

So, let $a - b = k_1 m$ and $b - c = k_2 m$ where k_1, k_2 are two integers. So, $a - c = (a-b) + (b-c) = k_1 m + k_2 m = (k_1 + k_2)m = k'm$ where $k' = k_1 + k_2$ is an integer. So, $a - c$ is divisible by m.

So, $a \equiv c \pmod m$

4. Given $a \equiv b \pmod m$. So $a - b = km$ where k is an integer. Now $(a+c) - (b+c) = a - b = km$ and $ac - bc = c(a-b) = (kc)m$. So $a+c \equiv (b+c) \pmod m$ and $ac \equiv bc \pmod m$

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.

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

So, $a+c \equiv (b+d) \pmod m$ as $k+l$ is an integer.

By property 4,

$a \equiv b \pmod m \Rightarrow ac \equiv bc \pmod m$

$c \equiv d \pmod m \Rightarrow bc \equiv bd \pmod m$

So, $ac \equiv bc \pmod m$ and $bc \equiv bd \pmod m$

$\Rightarrow ac \equiv bd \pmod m$ by property 3.

6. As $d \mid m$, so $m = kd$, where k is an integer

As $a \equiv b \pmod m$, $a - b = k_1 m$ where k_1 is an integer

So, $a - b = (k_1 k)d$ where kk_1 is an integer and also $d > 0$.

So, $a \equiv b \pmod d$

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 $a = qm + r$, $0 \le r \le m-1$

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.