International Journal of Mathematics Trends and Technology
ISSN: 2231-5373/ https://doi.org/10.14445/22315373/IJMTT-V71I5P101
Volume 71 Issue 5, 1-8, May 2025

Original Article

Congruence and Real Life Applications - I

Priti Upreti[1], S. Tiwari[2]

[1,2]*Department of Mathematics, Moti Lal Nehru College (University of Delhi), Delhi, India.*

[1]*Corresponding Author : priti.69upreti@gmail.com*

Received: 18 March 2025 Revised: 23 April 2025 Accepted: 12 May 2025 Published: 26 May 2025

Abstract - *Congruence is a very powerful concept in the study of Number Theory, Cryptography and Modular Arithmetic. For a given positive integer n, any two integers u_1 and u_2 are said to be congruent modulo n if they have the same remainder upon division by n. In this paper we discuss properties of congruence, Fermat's theorem and Wilson's theorem. We also discuss various examples of real life applications of these concepts, especially the various divisibility tests and computations related to calendar.*

Keywords - *Congruence, Fermat's theorem, Wilson's theorem, Primality test, Divisibility test.*

1. Introduction

The theory of congruence was introduced by the great mathematician Carl Friedrich Gauss(1777-1855) in his book "Disquisitiones Arithmeticae". In "Disquisitiones Arithmeticae", he put forth the concept and notation of congruence. The book also highlights the fact that congruence is a powerful technique in mathematics. Gauss was induced to adopt the symbol(≡) because of the close analogy of congruence with the algebraic equality. The development of primality testing and factoring methods have been crucial for advancements in number theory and cryptography, particularly with the advent of algorithms like Miller-Rabin and the AKS primality test as discussed by M. Richard [3] in his work. F. Umar and S. Muhammad [1] utilize mathematical principles to determine Julian dates and calendar-related computations. The paper also focuses on a systematic approach to calculating Julian dates, which is a key element in understanding the Julian calendar and its relationship to the Gregorian calendar. The properties of congruence and their applications to the divisibility theory are investigated in the research work by M. Lemma and D. Allard[2]. Some interesting developments in primality testing that have extensive applications in cryptography have been explored by C. Pomerance[6].

In this article we study the role of Fermat's theorem and the Wilson's theorem in various applications in Number theory.

Definition 1.1.[5] Two integers u_1 and u_2 are said to be congruent modulo n, where n >1 is an integer if n divides the difference u_1 - u_2. This is symbolized by $u_1 \equiv u_2 (mod\ n)$. For example $-37 \equiv 2 (\mathrm{mod}\ 13)$ as $-37 - 2 = -39$ which is divisible by 13. If u_1 - u_2 is not divisible by n, then we say that u_1 is incongruent to u_2 modulo n and in this case we write $u_1 \not\equiv u_2 (mod\ n)$. For example $37 \not\equiv 5 (mod\ 15)$ as $37 - 5$ is not divisible by 15.

1.2. Properties of Congruence.[5]

Let n > 1 be fixed and u_1, u_2, u_3 and u_4 be arbitrary integers, then the following properties hold.

(i) $u_1 \equiv u_1 (mod\ n)$

(ii) If $u_1 \equiv u_2 (mod\ n)$, then $u_2 \equiv u_1 (mod\ n)$

(iii) If $u_1 \equiv u_2 (mod\ n)$ and $u_3 \equiv u_4 (mod\ n)$, then $u_1 \pm u_3 \equiv u_2 \pm u_4 (mod\ n)$ and $u_1 u_3 \equiv u_2 u_4 (mod\ n)$

It is important to note that the cancellation law does not hold in congruence. This means that if $u_1 u_3 \equiv u_2 u_3 (mod\ n)$ where $n > 1$ and u_1, u_2 *and* $u_3 \in \mathbb{Z}$, then $u_1 \equiv u_2 (mod\ n)$ may not hold. For example

$3 \times 4 \equiv 3 \times 6 (\mathrm{mod}\ 6)$. But $4 \not\equiv 6 (\mathrm{mod}\ 6)$

In fact, we have the following theorem.

Theorem 1.3. Let $n > 1$ be a fixed integer and u_1, u_2 *and* $u_3 \in \mathbb{Z}$. If $u_1 u_3 \equiv u_2 u_3 (mod\ n)$, then $u_1 \equiv u_2 \left(mod\ \frac{n}{d}\right)$ where d= gcd(u_3, n).

We now state some important theorems related to congruence.

Theorem 1.4. Let u $\in \mathbb{Z}$ and u $\equiv$ r(mod n) where $0 \leq r <$ n, then r is the remainder when u is divided by n.
For example $-11 \equiv 6(\text{mod } 17)$, 6 is the remainder when we divide – 11 by 17.

Theorem 1.5. $u_1 \equiv u_2 (mod\ n)$ if and only if each of u_1 and u_2 leave the same remainder when divided by n.

It may be further noted that upon using division algorithm for n > 1 , for any integer u we have $u = nq + r$ where r and q are integers such that $0 \leq r <$ n.
$\Rightarrow$ u $\equiv$ r(mod n).
This means that any integer u is congruent to r mod n where $0 \leq r <$ n. Hence every integer is congruent mod n to exactly one of the values from $0, 1, 2, \ldots,$ n $- 1$.This leads to the following definitions:

Definition 1.6. Any collection of n integers $u_1, u_2, \ldots, u_n$ is said to form a complete set of residues modulo n if every integer is congruent modulo n to one and only one of the u_K.
Further, the set of integers $0, 1, 2, \ldots, n - 1$ is called the set of least non negative residue $mod\ n$.

2. Fermat's Theorem and its applications

Theorem 2.1.(Fermat's Theorem): Let q be a prime and q does not divide u , then $u^{q-1} \equiv 1(\text{mod q})$.

This directly leads to the important result that for a prime number q, $u^q \equiv$ u(mod q). Fermat's theorem has many applications and is central to most of the work done in number theory. In the least, it can be a labor saving device in certain calculations. We illustrate this using the following example.

Example 2.2. Find the remainder when 5^{38} is divisible by 17.

Solution. Using Fermat's theorem
$\Rightarrow$ $5^{16} \equiv 1(\text{mod } 17)$
$\Rightarrow$ $(5^{16})^2 \equiv 1(\text{mod } 17)$
$\Rightarrow$ $5^{32} \equiv 1(\text{mod } 17)$
Now $5^2 \equiv 8(\text{mod } 17)$
$\Rightarrow$ $(5^2)^2 \equiv (8)^2 \equiv -4(\text{mod } 17)$
$\Rightarrow$ $5^4 \times 5^2 \equiv -4 \times 8 \equiv 2(\text{mod } 17)$
$\Rightarrow$ $5^6 \equiv -4 \times 8 \equiv 2(\text{mod } 17)$
$\Rightarrow$ $5^{32} \times 5^6 \equiv 2 \times 1(\text{mod } 17)$
Hence remainder is 2.

Another use of Fermat's theorem is as a tool in testing the non- primality of a given integer n. If it could be shown that the congruence $u^n \equiv u(\text{mod n})$ fails to hold for some choice of u, then n, is necessarily composite. We illustrate this application using the following example.

Example 2.3. Show that 1763 is composite.

Solution. Fermat's theorem tells us that if q is prime and q does not divide u, then $u^{q-1} \equiv 1(mod\ q)$. Hence for proving that 1763 is composite it is sufficient to show that $2^{1762} \not\equiv 1(\text{mod } 1763)$.
Now
$2^{11} \equiv 285(\text{mod } 1763)$
$\Rightarrow$ $(2^{11})^2 \equiv 285 \times 285 \equiv 127(\text{mod } 1763)$
$\Rightarrow$ $(2^{22})^2 \equiv 127 \times 127 \equiv 262(\text{mod } 1763)$
$\Rightarrow$ $2^{44} \times 2^{44} \equiv 262 \times 262 \equiv 1650(\text{mod } 1763)$
$\Rightarrow$ $2^{88} \times 2^{44} \equiv 1650 \times 262 \equiv 365(\text{mod } 1763)$
$\Rightarrow$ $(2^{132})^2 \equiv 365 \times 365 \equiv 1000(\text{mod } 1763)$
$\Rightarrow$ $(2^{264})^2 \equiv 1000 \times 1000 \equiv 379(\text{mod } 1763)$
$\Rightarrow$ $(2^{528})^3 \equiv 379 \times 379 \times 379 \equiv 262(\text{mod } 1763)$

$\Rightarrow \quad 2^{1584} \times 2^{132} \times 2^{44} \equiv 262 \times 365 \times 262 \equiv 1067(\text{mod } 1763)$
$\Rightarrow \quad 2^{1760} \times 2^{2} \equiv 1067 \times 4 \equiv 792(\text{mod } 1763)$
Hence $2^{1762} \not\equiv 1(\text{mod } 1763)$. This gives that 1763 is a composite number.

3. Wilson's Theorem and its applications

Theorem 3.1.(Wilson's Theorem): If q is a prime number then
$(q-1)! \equiv -1(\text{mod q})$.

The converse of Wilson Theorem is also true i.e.,If $(n-1)! \equiv -1(\text{mod n})$, then n is prime.
Taken together, Wilson's theorem and its converse provide a necessary and sufficient condition for determining primality. Further we also give here an important result which is a consequence of the Wilson's theorem.

Corollary 3. 2. The quadratic congruence $y^2 + 1 \equiv 0(mod\ q)$, where q is an odd prime has a solution iff $q \equiv 1(mod\ 4)$.

Proof. Let k be any solution of $y^2 + 1 \equiv 0(\text{mod q})$,this gives that $k^2 \equiv -1(\text{mod q})$. Also as q does not divide k, from Fermat's theorem, we have

$1 \equiv k^{q-1} \equiv (k^2)^{\frac{q-1}{2}} \equiv (-1)^{\frac{q-1}{2}}(modq)$
$\Rightarrow \quad 1 \equiv (-1)^{\frac{q-1}{2}}(modq)$. This means that $\frac{q-1}{2}$ must be even. Hence $\frac{q-1}{2} = 2m$.
$\Rightarrow \quad q - 1 = 4m$
$\Rightarrow \quad q \equiv 1(\text{mod } 4)$.
Now for the converse part, consider

$$(q-1)! = 1 \times 2 \times 3 \times \ldots \times \tfrac{q-1}{2} \times \tfrac{q+1}{2} \times \ldots \times (q-2)(q-1) \tag{1}$$

We know that
$q - 1 \equiv -1(\text{mod q})$
$q - 2 \equiv -2(\text{mod q})$
.
.
.
$\frac{q+1}{2} \equiv -\left(\frac{q-1}{2}\right)(\text{mod q})$
Using above congruence in (1), we have

$$(q-1)! \equiv 1 \times (-1) \times 2 \times (-2) \times \ldots \times \left(\frac{q-1}{2}\right) \times -\left(\frac{q-1}{2}\right)(\text{mod q})$$
$$\equiv (-1)^{\frac{q-1}{2}}\left[1 \times 2 \times 3 \times \ldots \left(\frac{q-1}{2}\right)\right]^2 (mod\ q)$$
$$\equiv (-1)^{\frac{q-1}{2}}\left[\ \left(\frac{q-1}{2}\right)!\ \right]^2 (mod\ q)$$

Since $q \equiv 1(mod\ 4)$,
$\Rightarrow \quad q - 1 = 4m$for some m
$\Rightarrow \quad \frac{q-1}{2}$ is even

Hence $(q-1)! \equiv \left[\ \left(\frac{q-1}{2}\right)!\ \right]^2 (mod\ q)$ (2)

Using Wilson theorem, we have

$$(q-1)! \equiv -1(mod\ q) \tag{3}$$

Using (2) and (3) we have

$\left[\ \left(\frac{q-1}{2}\right)!\ \right]^2 \equiv -1(mod\ q)$.

Hence the given quadratic congruence has a solution $y = \left(\frac{q-1}{2}\right)!$.
We illustrate the applications of the above theorems using the following example.

Example 3.3. Find the solution of $y^2 + 1 \equiv 0(mod\ 29)$.

Solution . Since $29 \equiv 1(mod 4)$, therefore the given quadratic congruence has a solution say

$$\left(\frac{29\ -1}{2}\right)! = 14!$$

Now

$$\begin{aligned} 14! &= 14 \times 13 \times 12 \times 11 \times 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 \\ &\equiv (14 \times 2) \times (13 \times 3) \times (12 \times 4) \times (11 \times 5) \times (10 \times 6) \times (9 \times 8) \times 7(mod\ 29) \\ &\equiv -1\ \times 10 \times (-10) \times (-3) \times (2) \times (-15) \times 7(mod\ 29) \\ &\equiv -1 \times 20 \times 18(mod\ 29) \\ &\equiv 12(mod\ 29) \end{aligned}$$

and

$$12^2 + 1 \equiv 0(mod\ 29)$$

Hence $y = 12$ is a solution of the given quadratic congruence.

The following theorem is the another consequence of Wilson's theorem.

Theorem 3.4.[4] Every prime number q such that $q \equiv 1(mod\ 4)$, can be written as the sum of the square of two integers. That is we can write $q = u^2 + v^2$ where *u* and *v* are positive integers.

Proof. Let q be a prime number such that $q \equiv 1(mod\ 4)$. Then from Corollary (3.2) there exists integer k such that

$$k^2 + 1 \equiv 0(mod\ q) \tag{4}$$

Let us define $f(x, y) = x + ky$ where $0 \leq x, y \leq L$ and $L = \left[\sqrt{q}\right]$ ([ ] stands for the greatest integer function.)

Since $\sqrt{q}$ is not an integer it gives $L < \sqrt{q} < L + 1$.

Now x and y each take any of the $L + 1$ values (0,1,2,…L), the pair(x, y) has $(L + 1)^2$ possible values . Further as $(L + 1)^2 > q$ we get thats $f(x, y)$ has more than p possible values.

Using the definition of complete residue modulo p, there are two different pairs (x_1, y_1) and (x_2, y_2) such that

$$f(x_1, y_1) \equiv f(x_2, y_2)(mod\ p)$$

$$\begin{aligned} &\Rightarrow \quad x_1 + ky_1 \equiv x_2 + ky_2(mod\ q) \\ &\Rightarrow \quad (x_1 - x_2) \equiv k(y_2 - y_1)(mod\ q) \\ &\Rightarrow \quad (x_1 - x_2)^2 \equiv k^2(y_2 - y_1)^2(mod\ q) \\ &\Rightarrow \quad (x_1 - x_2)^2 \equiv -1(y_2 - y_1)^2(mod\ q) \qquad \text{(Using(4))} \\ &\Rightarrow \quad q|(x_1 - x_2)^2 + (y_1 - y_2)^2| \end{aligned} \tag{5}$$

Since the pair(x_1, y_1) and $(x_2, y_2)$are distinct this gives

$$(x_1 - x_2)^2 + (y_1 - y_2)^2 > 0$$

and $0 \leq x_1, x_2 < L$ which gives

$$-L < x_1 - x_2 < L$$

$$\Rightarrow \quad 0 \leq (x_1 - x_2)^2 < L^2 < q$$

Similarly,

$$0 \leq (y_1 - y_2)^2 < q$$

Using the above discussion we have

$$0 < (x_1 - x_2)^2 + (y_1 - y_2)^2 < 2q \tag{6}$$

Using (5) and (6) we have

$$(x_1 - x_2)^2 + (y_1 - y_2)^2 = q$$

Remark 3.5 . As an illustration of the above result we may note that as 13, 17,29,37,41 are prime integers which are congruent to 1 mod 4 we can express them as

$$13 = 2^2 + 3^2 \qquad 37 = 1^2 + 6^2$$
$$17 = 1^2 + 4^2 \qquad 41 = 5^2 + 4^2$$
$$29 = 2^2 + 5^2$$

On the other hand the numbers 3, 31, 43 are congruent to 3 modulo 4. We can easily check there do not exist any integers a and b such $q = a^2 + b^2$.

The Wilson's theorem is very helpful in checking the primality of a number. This application is called the Primality Test.

Example 3.6. (Primality Test). With the help of Wilson theorem show that 19 is a prime number.

Solution. Consider $(19-1)! = 18!\,(mod\ 19)$

$$\begin{aligned} 18! &= 18\times 17\times 16\times 15\times 14\times 13\times 12\times 11\times 10\times 9\times 8\times 7\times 6\times 5\times 4\times 3\times 2\times 1 \\ &= (18\times 1)\times(17\times 2)\times(16\times 3)\times(15\times 4)\times(14\times 5)\times(13\times 6) \\ &\quad \times(12\times 7)\times(11\times 8)\times(10\times 9) \\ &\equiv (-1)(-4)(10)(3)(-6)(2)(8)(-7)(-5)(mod 19) \\ &\equiv (-1)(120)(96)(35)(mod 19) \\ &\equiv (-1)(6)(1)(-3) \\ &\equiv 18 \equiv -1(mod 19) \end{aligned}$$

Hence using Wilson's theorem 19 is a prime number.

Now below is another use of congruence. Here with the help of congruence we can check if a number is not a perfect square.
Theorem 3.7. [4]Show that $u^2 \equiv 1$ or $0(mod\ 4)$ where $u \in Z$.

Proof. Since $\{-1,0,1,2\}$ is a complete residue system of $mod\ 4$, for any integer *a* exactly one of the following is true.

$u \equiv -1\ (mod\ 4)$, $u \equiv 0\ (mod\ 4)$, $u \equiv 1(mod\ 4)$, $u \equiv 2\ (mod\ 4)$

$\Rightarrow$ $u^2 \equiv 1\ (mod\ 4)$, $u^2 \equiv 0\ (mod\ 4)$, $u^2 \equiv 1(mod\ 4)$, $u^2 \equiv 4 \equiv 0\ (mod\ 4)$

Hence any perfect square gives the remainder 0 and 1 when divided by 4. But the converse is not true as we can see that $13 \equiv 1(mod 4)$, but 13 is not a perfect square.

Example 3.8. Is 22051946 a perfect square?
Solution. $22051946 = 220519\times 100 + 46 \equiv 46(mod 4) \quad \equiv 2(mod 4)$
Hence 22051946 is not a perfect square.

Example 3.9 . Is 3190491 a perfect square?

Solution. $3190491 = 31904\times 100 + 91 \equiv 91(mod 4) \equiv 13\times 7(mod 4)$

$$\equiv 1\times 3(mod 4)$$
$$\equiv 3(mod 4)$$

Hence 3190491 is not a perfect square.

One of the another application of congruence, is the non existence of Integral roots of a polynomial $f(x)$. This can be seen in the following result.
Remark 3.10[4]: Non Existence of Integral Roots of a polynomial with integral coefficients.
Let a polynomial $f(x)$ with integral coefficients has an integer root say α. It follows that $f(\alpha) = 0$ which gives $f(\alpha) \equiv 0$ (modn) for all integer $(n > 1)$. If it could be shown that for all integer $\alpha \in Z$, $f(\alpha) \not\equiv 0(mod\ n)$ for some n. It gives $f(x)$ has no integral root.

Example 3.11. Prove that the polynomial $f(x) = x^5 - x^2 + x - 3$ has not integer roots.

Solution. Consider$f(x)(mod 4)$. Now $\{-1,0,1,2\}$ is complete set of residue modulo 4 and

$f(0) = -3 \not\equiv 0(mod 4)$, $f(1) = -2 \not\equiv 0(mod 4)$

$f(-1) = -4 \not\equiv 0(mod 4)$, $f(2) = 27 \not\equiv 0(mod 4)$

Hence there does not exist any integer α such that

$f(\alpha) \equiv 0(mod 4)$

This gives that the polynomial $f(x)$ has no integral root.

Example.3.12 Prove that the polynomial $f(x) = x^3 + x^2 - x + 3$ has no integral root.

Solution. $f(x) = x^3 + x^2 - x + 3$. We can easily check that

$f(1) \equiv 0(mod 2)$, $f(0) \equiv 0(mod 3)$, $f(1) \equiv 0(mod 4)$,

therefore, we take $n = 5$ and $\{-2, -1,0,1,2\}$ is a complete set of residue modulo 5 and

$f(0) = 3 \not\equiv 0(mod5)$, $f(1) = 4 \not\equiv 0(mod5)$, $f(-1) = 4 \not\equiv 0(mod5)$,

$f(2) = 13 \not\equiv 0(mod5)$ $f(-2) = 1 \not\equiv 0(mod\ 5)$

Hence $f(\alpha) \not\equiv 0(mod\ 5)$ for all $\alpha \in Z$

$\Rightarrow$ $f(x)$ has no integral root.

4. Divisibility Test

One of the most interesting applications of congruence theory involves finding special criterion under which a given integer is divisible by another integer. Let us observe this in the following theorem.

Theorem 4.1. Let $Q(x) = \sum C_k\, x^k$ be a polynomial function of x with integral coefficients C_k. If $u \equiv v(modn)$, then $Q(u) \equiv Q(v)(modn)$.

Solution. Since $u \equiv v(mod\ n)$

$\Rightarrow$ $u^k \equiv v^k(mod\ n)$

$\Rightarrow$ $C_k u^k \equiv C_k v^k(mod\ n)$

$\Rightarrow$ $\sum C_k\, u^k \equiv \sum C_k\, v^k(modn)$

$\Rightarrow$ $Q(u) \equiv Q(v)(modn)$

Theorem 4.2. (Divisibility by 2^k). Let $I = \alpha_k 10^k + \alpha_{k-1}10^{k-1} + \cdots + \alpha_1 10 + \alpha_0$. Then 2^k divides *I* iff the number represented by the last k digits is divisible by 2^k.

Solution. Let$f(x) = \alpha_k x^k + \alpha_{k-1}10^{k-1} + \cdots + \alpha_1 10 + \alpha_0$, then

$f(10) = I$ and $f(0) = \alpha_0$.

Since $10 \equiv 0(mod\ 2)$.Hence by Theorem 4.1,$f(10) \equiv f(0)(mod\ 2)$ which gives

$I \equiv \alpha_0(mod\ 2)$.

$I \equiv 0(mod\ 2)$ if and only if $\alpha_0 \equiv 0(mod\ 2)$

Now we observe that

$10^i \equiv 0(mod4)$ for all $i \geq 2$

$\Rightarrow$ $10^i \alpha_i \equiv 0(mod4)$ for all $i \geq 2$

this gives that $I = \sum_{i=2}^{k} 10^i \alpha_i + 10\alpha_1 + \alpha_0 \equiv 0 + 10\alpha_1 + \alpha_0(mod4)$

$\Rightarrow$ $I \equiv 0(mod2^2)$ if and only if $10\alpha_1 + \alpha_0 \equiv 0(mod2^2)$.

Likewise we can prove that I is divisible by 2^3, iff the number $\alpha_2 10^2 + \alpha_1 10 + \alpha_0$ is divisible by 2^3 or the number formed by the last three digits is divisible by 2^3. In general, we can prove that the integer I is divisible by 2^k iff the number formed by the last k digits is divisible by 2^k.

Divisibility Tests for 3, 9 and 11

Theorem 4.3. Divisibility Tests for 3, 9 and 11

Let $I = \alpha_k 10^k + \alpha_{k-1}10^{k-1} + \cdots . + \alpha_2 10^2 + \alpha_1 10 + \alpha_0$where $\alpha_k \neq 0$ and $0 \leq \alpha_i < 10$ for $i = 0,1,2, \ldots, k$.

Let $S = \alpha_0 + \alpha_1 + \cdots + \alpha_k$ and $T = \alpha_0 - \alpha_1 + \alpha_2 + \cdots + (-1)^k \alpha_k$, then

(i) *I* is divisible by 3 and 9 iff *S* is divisible by 3 and 9, respectively.

(ii) *I* is divisible by 11 iff *T* is divisible by 11.

Proof . (i) Define $f(x) = \alpha_k x^k + \alpha_{k-1}10^{k-1} + \cdots + \alpha_1 10 + \alpha_0$, then $f(10) = I$ and $f(1) = S$.

Since

$10 \equiv 1(mod\ 3)$

$\Rightarrow$ $f(10) \equiv f(1)(mod\ 3)$

$\Rightarrow$ $I \equiv S(mod\ 3)$

$\Rightarrow$ $I \equiv 0(mod\ 3)$ iff $S \equiv 0(mod\ 3)$.

Hence *I* is divisible by 3 iff S is divisible by 3

In the same manner we can prove that *I* is divisible by 9 iff *S* is divisible by 9.

(ii) Since $10 \equiv -1(mod11)$

$\Rightarrow \quad f(10) \equiv f(-1)(mod11)$and $f(-1) = T$
$\Rightarrow \quad I \equiv T(mod11)$
which gives I is divisible by 11 iff T is divisible by 11.

5. Application to the Calendar

In this section, our goal is to determine the day of the week for a given date after the year 1582, following the adaption of the Gregorian calendar at that time. Define four integers N, M, C and Y as follows:
N be the number of the day in the month, M be the number of month, C denotes the number of the centuries and Y the year within the century.

Let d denotes the day of the week, then

$$d \equiv N + [2.6M - 0.2] + Y + \left[\frac{Y}{4}\right] + \left[\frac{C}{4}\right] - 2C - (1 + L)\left[\frac{M}{11}\right](mod7)$$

where [ ] is greatest integer function

day	Sun	Mon	Tue	Wed	Thur	Fri	Sat
d	0	1	2	3	4	5	6

$L = 1$ for the leap year and $L = 0$ for a non leap year.

The leap year are those divisible by 4, except the year divisible by 100, which are leap years only if divisible by 400. For example, 1984, 2000, 2004 and 2400 each are leap years, but 1900, 2100, 1995 and 2401 are not. In Gregorian calendar the leap year day is added at the end of February,therefore we start counting of months from March.

Month	March	April	May	June	July	Aug.	Sep.	Oct.	Nov.	Dec.	Jan.	Feb.
M	1	2	3	4	5	6	7	8	9	10	11	12

Example.5.1. Determine the day of the week for Jan 1, 2011.

Solution. Here $M = 11, C = 20, Y = 11, N = 1, L = 0$, then

$$d \equiv 1 + [2.6 \times 11 - 0.2] + 11 + \left[\frac{11}{4}\right] + \left[\frac{20}{4}\right] - 2 \times 20 - (1 + 0)\left[\frac{11}{11}\right](mod7)$$
$$\equiv 1 + [28.4] + 11 + 2 + 5 - 40 - 1(mod7)$$
$$\equiv 1 + 28 + 11 + 2 + 5 - 40 - 1(mod7)$$
$$\equiv 6(mod7)$$

Hence the first day of 2011 falls on Saturday.

Example.5.2. For the year 2010, determine the
(i) Calendar dates on which Mondays will occur in march
(ii) The month in which the thirteen will fall on a friday.

Solution. (i) Here$M = 1, C = 20, d = 1, L = 0, Y = 10$, then using the formula

$$1 \equiv N + [2.6 \times 1 - 0.2] + 10 + \left[\frac{10}{4}\right] + \left[\frac{20}{4}\right] - 2 \times 20 - (1 + 0)\left[\frac{1}{11}\right](mod7)$$
$$1 \equiv N + 2 + 10 + 2 + 5 - 40(mod7)$$
$$1 \equiv N - 21(mod7)$$
$$N \equiv 22 \equiv 1(mod7)$$
$$N = 1, 8, 15, 22, 29$$

Hence on 1, 8, 15, 22, 29 march Monday occurred.

(ii) Here $M =?, C = 20, d = 6, L = 0, Y = 10, N = 13$. Using the formula

$\Rightarrow \quad 5 \equiv 13 + [2.6 \times M - 0.2] + 10 + \left[\frac{10}{4}\right] + \left[\frac{20}{4}\right] - 40 - (1 + 0)\left[\frac{M}{11}\right](mod7)$

$\Rightarrow \quad 5 \equiv 23 + [2.6 \times M - 0.2] + 10 + 2 + 5 - 40 - \left[\frac{M}{11}\right](mod7)$

$\Rightarrow \quad 5 \equiv -10 + [2.6M - 0.2] - \left[\frac{M}{11}\right](mod7)$

$\Rightarrow \quad 15 \equiv 1 \equiv [2.6M - 0.2] - \left[\frac{M}{11}\right](mod7)$

$\Rightarrow \quad \left[\frac{M}{11}\right] \equiv [2.6M - 0.2] - 1(mod7)$

$\equiv [2.6M - 1.2](mod7)$ (7)

$\Rightarrow \quad \left[\frac{M}{11}\right] = 1$ if $M = 11$ and 12, $\left[\frac{M}{11}\right] = 0$ when $1 \leq M \leq 10$

But $M = 11, 12$gives

$$[2.6 \times 11 - 1.2] = [28.6 - 1.2] = [27.4] = 27 \equiv 6(mod7) \not\equiv 1(mod7)$$

$$[2.6 \times 12 - 1.2] = 30 \equiv 2 \not\equiv 1 = \left[\frac{M}{11}\right](mod7)$$

Hence equation (7) is not satisfied

$\Rightarrow \quad \left[\frac{M}{11}\right] = 0$

Now

$[2.6M - 1.2] \equiv 0(mod7)$ (8)

$\Rightarrow \quad [2.6M - 1.2] = 0 \ or \ 7$

For $M = 6$, equation (8) is satisfied.

Hence Friday falls on 13th August.

6. Conclusion

With the help of various examples, we have seen that the simple concepts of congruence have many applications in the field of arithmetic and day to day life. These concepts have extensive proofs at their back. However, several new applications have been emerging involving congruence modulo and modular arithmetic.

References

[1] Umar Farooq, Muhammad Sarwar, and Muhammad Waqar, "Computing of Julian Calendar By Congruence Relation," *Life Science Journal*, vol. 10, no. 105, 265-269, 2013. [CrossRef] [Publisher Link]

[2] Mulatu Lemma, and Dustin Allard, "Applications of Congruence to Divisibility Theory," *IJRDO-Journal of Mathematics*, vol. 3, no. 11, pp. 32-42, 2017. [CrossRef] [Publisher Link]

[3] Richard A. Mollin, "A Brief History of Factoring and Primality Testing B.C (Before Computers)," *Mathematics Magazine*, vol. 75, no. 1, pp. 18-29, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[4] Gareth A. Jones, and Josephine M. Jones, *Elementary Number Theory*, Springer Verlag, London Limited, 1998. [Google Scholar] [Publisher Link]

[5] D.M. Burton, *Elementary Number Theory*, Seventh Edition, McGraw Hill Education India. Edition, 2012. [Publisher Link]

[6] Carl Pomerance, "Recent Developments in Primality Testing," *The Mathematical Intelligence*, vol. 3, pp. 97-105, 1981. [CrossRef] [Google Scholar] [Publisher Link]