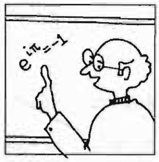
Classroom



In this section of* Resonance, *we invite readers to pose questions likely to be raised in a classroom situation. We may suggest strategies for dealing with them, or invite responses, or both. "Classroom" is equally a forum for raising broader issues and sharing personal experiences and viewpoints on matters related to teaching and learning science.

Modular Arithmetic and the Calendar

Fr. James Philip
Mary Matha College
Podimattam, Parathode,
Kanjirapally, Kerala 686412,
India.

Introduction

The present article introduces a technique to determine the day of the week corresponding to a given date. There are many methods in vogue for the purpose, but the beauty of this method lies in that it has a solid mathematical basis and that it is easy to handle. Even a layman in mathematics can easily understand and use the technique and the calculations can be carried out mentally, with a little practice.

However, to appreciate the full strength and beauty of the technique, it is worthwhile to examine the mathematical basis of it, namely, the modular arithmetic, which was developed by the great mathematician, Carl Friedrich Gauss[1]. It is surprising that such an abstract concept as the residue classes should give rise to a simple, direct and down-to-earth application. But, it is often the case with mathematics, 'the queen of all sciences'.

[1]For a biographical sketch, see *Resonance*, Vol.2, No.6 pp.60-67, 1997.

The Arithmetic Progression

Consider the set **Z** of integers. We can separate the elements of **Z** into 5 subsets as follows:

$A_0 = \{\ldots, -15, -10, -5, 0, 5, 10, \ldots\}$,
$A_1 = \{\ldots, -14, -9, -4, 1, 6, 11, \ldots\}$,
$A_2 = \{\ldots, -13, -8, -3, 2, 7, 12, \ldots\}$,
$A_3 = \{\ldots, -12, -7, -2, 3, 8, 13, \ldots\}$,
$A_4 = \{\ldots, -11, -6, -1, 4, 9, 14, \ldots\}$.

This is called partitioning and it may be noted that any integer belongs to one and only one of these five sets. Further each of these sets forms an arithmetic progression (AP) with common difference 5.

Such a partitioning is not special to the number 5. Rather, for every positive integer m, we can partition **Z** into m distinct subsets, each of which is an AP with common difference m.

Now, choose an element, say –15, from the first class A_0. Any other element in A_0 can be written as the sum of –15 and a multiple of 5. So we may take –15 as a representative of A_0. Similarly, if we choose a number, say 12, from A_2, any element in A_2 can be written as 12 + a multiple of 5. The same is true for any class and it follows that each class is uniquely determined by any of its representatives. So we may also use this element to denote the class. Thus, $A_0 = [-15]$, $A_1 = [6]$, $A_2 = [-13]$, etc., where $[r]$ denotes the class containing the element r.

It is evident that the choice of the representative is arbitrary and we may choose the most convenient one and the obvious choice is 0, 1, 2, ., $m-1$ and we call these the residues. Thus for $m = 5$, we have $A_0 = [0]$, $A_1 = [1]$, $A_2 = [2]$, $A_3 = [3]$, $A_4 = [4]$.

In general, for a given positive integer m, the set **Z** has the partitioning [0], [1], [2], ..., $[m-1]$. These ideas have been formally developed by Gauss in his *Disquisitiones Arithmeticae* and we adopt the gaussian terminology.

The Residue Classes

Definition: Let a and b be two elements in the same arithmetic progression. Then we say that 'a is congruent to b modulo m' where m is the common difference of the progression. This is denoted by $a \equiv b \pmod{m}$.

Thus $a \equiv b \pmod{m}$ means that m divides $(a-b)$, written $m \mid (a-b)$, or that $a-b$ is a multiple of m, or that a and b differ by a multiple of m. For example, for $m=5$, -27 and 13 belong to the same class [3] (or, A_3) and we see that $-27-13 = -40$, a multiple of 5. So we say that $-27 \equiv 13 \pmod{5}$. Also, $10 \equiv 2 \pmod{4}$, since $10-2=8$ is a multiple of 4, etc.

Definition: For a fixed a, the integers x such that $x \equiv a \pmod{m}$ are the elements of the form $x = a + mk$, $k \in \mathbf{Z}$. This arithmetic progression is called a residue class modulo m.

For a given positive integer m, the set $\mathbf{Z}$ is thus partitioned into m residue classes [0], [1], [2], ... $[m-1]$ and each integer belongs to exactly one of these classes. (The case for $m = 5$ has been discussed above.)

We have assumed this separation to be a partitioning; this is because 'belonging to the same residue class' is an equivalence relation.

Operations on the Modulo Classes

We can define the following operations on the residue classes:

1. **Addition modulo m:** Let a and b be integers. We define an operation called addition modulo m denoted by $a +_m b$ such that $a +_m b = r$ where r is the least nonnegative remainder when the ordinary sum $a+b$ of a and b is divided by m. Clearly $0 \le r < m$. Eg: $10 +_4 6 = 0$ [since, $10 + 6 = 16 \equiv 0 \pmod{4}$], $7 +_6 8 = 3$ [since, $7+8 = 15 \equiv 3 \pmod{6}$], $-18 +_7 8 = 4$ [since, $-18 + 8 = -10 \equiv 4 \pmod{7}$].

It is easy to show that the set $(0,1,2,\dots,m-1)$ forms a commutative group under addition modulo m. We give *Table* 1 of addition modulo 4 as an example for verification:

Table 1.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

2. **Multiplication modulo m:** Let a and b be integers. We define the operation called 'multiplication modulo m' denoted by

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Table 2.

$\times_4$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Table 3.

$a \times_m b$ such that $a \times_m b = r$ where r is the least nonnegative remainder obtained when the ordinary product ab of a and b is divided by m. Again, $0 < r < m$.

Eg: $10 \times_4 6 = 0$ [since, $10 \times 6 = 60 \equiv 0 (\text{mod } 4)$], $7 \times_6 8 = 2$ [since, $7 \times 8 = 56 \equiv 2 (\text{mod } 6)$], $-18 \times_7 8 = 3$ [since, $-18 \times 8 = -144 \equiv 3 (\text{mod } 7)$].

In this case, if p is a prime number, the nonzero residue classes modulo p form a commutative group under multiplication modulo p. However, if p is composite, this fails to be a group. These can be easily proved, but we content ourselves with tables 2 and 3 of multiplication reduced to modulo 5 and 4 for verification.

The Field of Residue Classes

Congruence may be regarded as a generalized form of equality. Some of the elementary properties of equality which carry over to congruences are listed below:

(i) If $a \equiv x (\text{mod m})$ and $b \equiv y (\text{mod m})$, then $a + b \equiv x + y \ (\text{mod } m)$, and $ab \equiv xy \ (\text{mod } m)$.
(ii) If $a \equiv b (\text{mod } m)$, then $a + c \equiv b + c \ (m \text{ mod } m)$ and $ac \equiv bc \ (\text{mod } m)$

The residue classes together with the above operations give the following results:

Theorem: For a positive integer m, the set of residue classes modulo m is a commutative ring with respect to addition modulo m and multiplication modulo m.
Theorem: The set of residue classes modulo m is a field with respect to the above operations, if and only if m is prime.

The proof is routine work and we do not attempt it here. Now we proceed to the determination of the day.

The Calendar

The idea of the residue classes can conveniently be used to determine the day of the week for any given date – past, present or future. The method makes use of the fact that there are 7 days in a week and a day repeats itself exactly after 7 days. Each day of the week can be considered a residue class and there are 7 such classes. Before we go into the actual determination, let us examine how the days in a calendar occur.

Basic Information

The time that the Earth takes to revolve around the Sun once is approximately 365 days, 5 hours, 48 minutes and 46 seconds. But an ordinary year is taken as 365 days which is short by about 1/4th of a day. This shortage is made up by adding an extra day to every 4th year and such a year is called a leap year. The extra day is added to the shortest month, February. But this is found to be an overcorrection and to rectify the defect every centennial year (years like 100, 1300, 2500, etc.) is considered an ordinary year and not a leap year. However, if the centennial year is divisible by 400 it is still a leap year. Thus 400, 1200, 2800, etc. are leap years.

These facts together with the concept of residue classes pave our way towards our aim.

The Working Rule

An ordinary year has 365 days. But $365 \equiv (1 \bmod 7)$. That is, there are 52 full weeks and an extra day in a year. Let us call this extra day the residue. Thus an ordinary year has a residue 1. Similarly, a leap year has a residue 2.

In 100 years, there are 76 ordinary years and 24 leap years (why?), giving a total residue of $76 + 48 = 124$. This reduced to modulo 7 gives 5 as the residue (for $124 = 17 \times 7 + 5$). So 100 years is equivalent to a residue of 5. We may write this as:

100 years $\equiv 5 (\bmod 7)$.
Now, 200 years $\equiv 2 \times 5 \equiv 3 \pmod 7$
And 300 years $\equiv 3 \times 5 \equiv 1 \pmod 7$
But, 400 is a leap year and has an additional residue.

i.e., $400 \equiv 4 \times 5 \pmod 7 + 1 \equiv 0 \pmod 7$

Now we consider the residues of the months:

January has 31 days and $31 \equiv 3 \pmod 7$ and the residue is 3. February has no residue in the ordinary year and has a residue 1 in a leap year. The residues of the other months are: March – 3, April – 2, May – 3, June – 2, July – 3, Aug – 3, September – 2, October – 3, November – 2. (We will not need December!)

Now the day is determined according to the residue of the given date and the day is fixed as follows: Sunday if residue is 0, Monday for residue 1, Tuesday for 2, Wednesday for 3, Thursday for 4, Friday for 5 and Saturday for 6.

We emphasize that these calculations are simple and can be done mentally. Let us see how this works with examples:

Example 1: Let us find the day corresponding to 1–1–2000.

On January 1, 2000 we will have completed 1999 years. Of these we may leave out 1600, being a multiple of 400 (since 400 years give zero residue). The residue for 300 years is 1 (see above). So with a carry of 1, we may leave out 1600 + 300 = 1900. In the remaining 99 years there are 24 leap years and 75 ordinary years, contributing to a residue of $24 \times 2 + 75 = 123$. Together with the carry, the residue becomes 124. Reduced to modulo 7 this gives the residue at the end of 1999 as 5. Since we are considering January, we do not need to consider the residues of the months. The residue for the date is 1. So the final residue is 6 and the day corresponding to 6 is Saturday. So 1–1–2000 is a Saturday!

Thus, we enter into the new millennium (so to speak) on a Saturday and this may be verified from the calendar for the current year. May it be a peaceful and happy one!

Example 2: As a second example let us find the day on which India became independent.

For 15 August 1947, the completed year is 1946. 1900 has

Box 1. Residues.

The following are the residues required for calculations:

Residue for years: 100 years – 5, 200 years – 3, 300 years – 1, 400 years – 0. An ordinary year – 1, a leap year –2 .

For Months: Jan. – 3, Feb. – 0 in ordinary years, 1 in leap years, Mar. – 3, Apr. – 2. May – 3, Jun. – 2, Jul. – 3, Aug. – 3, Sep. – 2, Oct. – 3, Nov. – 2, (Dec. – 3).

The following are the days corresponding to each residue: 0 – Sun., 1 – Mon., 2 – Tue., 3 – Wed., 4 – Thu., 5 – Fri., 6 – Sat.

residue 1 (example 1). In the 46 years, there are 11 leap years and 35 ordinary years, giving a residue of 22 + 35 = 57. Together with the carry the residue is 58. Reduced to modulo 7 we get 2. So, at the end of 1946 the residue = 2.

In 1947, residue of Jan. = 3
Feb. = 0 (ord. year)
Mar.= 3
Apr.= 2
May = 3
Jun. = 2
Jul. = 3
Aug. =15 (note!)

Total = 33

This reduced to modulo 7 gives the final residue as 5 and the day for 5 is Friday.

Therefore, August 15, 1947 was a Friday.

You may work with your birthday and other important days![1]

In going back into the past, one should bear in mind that in September 1752, 11 days (3rd to 13th) were removed so that 2nd September was followed by 14th September. Also, prior to that, all centuries were observed as leap years, not just when the number of centuries is divisible by 4.

Suggested Reading

[1] Michael Artin, *Algebra*, Prentice Hall of India Ltd., New Delhi, 1994.

[2] David M Burton, *Elementary Number Theory*, Universal Book Stall, New Delhi, 1995.