8: Modular Arithmetic

EN1106 - Introductory Mathematics

Level I - Semester 1

Applications of Congruences

In this section you shall learn how congruences can be used to develop divisibility tests, like the tests that you may have seen for checking whether an integer is divisible by 3 or 9.

After that, we will present a congruence that can be used to determine the day of the week for any date in history.

Divisibility by powers of 2

- Let $n \in \mathbb{N}$ and let $n=(a_k\, a_{(k-1)} \ldots a_1\, a_0\,)_{10}$, where $0 \leq a_j \leq 9$ for $0 \leq j \leq k$.
- Then $n=a_k \cdot 10^k + a_{(k-1)} \cdot 10^{(k-1)} + \cdots a_1 \cdot 10 + a_0$.
- Notice that because $10 \equiv 0 (\mathrm{mod}\ 2)$, $10^j \equiv 0 (\mathrm{mod}\ 2^j)$ for all $j \in N$ (why?).
- Also notice that for each $j \in N$, $(n-(a_{(j-1)}\, a_{(j-2)} \ldots a_1\, a_0\,)_{10}\,) \equiv 0 (\mathrm{mod}\ 10^j)$.
- Hence for each $j \in N$, $(n-(a_{(j-1)}\, a_{(j-2)} \ldots a_1\, a_0\,)_{10}\,) \equiv 0 (\mathrm{mod}\ 2^j)$ or equivalently for each $j \in N$, $n \equiv (a_{(j-1)}\, a_{(j-2)} \ldots a_1\, a_0\,)_{10}\ (\mathrm{mod}\ 2^j)$.
- Therefore for each $j \in N$, $2^j \mid n$ if and only if $2^j \mid (a_{(j-1)}\, a_{(j-2)} \ldots a_1\, a_0\,)_{10}$ (how?).

Example 9:

Let $n = 64{,}388{,}128$.

- because $(a_0)_{10} = 8$ is divisible by 2^1, n is divisible by 2,
- because $(a_1a_0)_{10} = 28$ is divisible by 2^2, n is divisible by 4,
- because $(a_2a_1a_0)_{10} = 128$ is divisible by 2^3, n is divisible by 8,
- because $(a_3a_2a_1a_0)_{10} = 8{,}128$ is divisible by 2^4, n is divisible by 16,
- because $(a_4a_3a_2a_1a_0)_{10} = 88{,}128$ is divisible by 2^5, n is divisible by 32.

- However, because $(a_5a_4a_3a_2a_1a_0)_{10} = 388{,}128$ is not divisible by 2^6, n is not divisible by 64.

Divisibility by 3 and 9

- Let n ∈ N and let $n = (a_k a_{k-1} \dots a_1 a_0)_{10}$, where $0 \leq a_j \leq 9$ for $0 \leq j \leq k$.
- Then $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots a_1 \cdot 10 + a_0$

Notice that for each $j \in \mathbb{N} \cup \{0\}$, $10^j \equiv 1 (\mathrm{mod}\ 3)$.

Hence

$$
\begin{aligned}
a_0 \cdot 10^0 &\equiv a_0 (\mathrm{mod}\ 3) \\
a_1 \cdot 10^1 &\equiv a_1 (\mathrm{mod}\ 3) \\
a_2 \cdot 10^2 &\equiv a_2 (\mathrm{mod}\ 3) \\
&\vdots \\
a_k \cdot 10^k &\equiv a_k (\mathrm{mod}\ 3).
\end{aligned}
$$

- It follows that

$$n = \left(a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots a_1 \cdot 10 + a_0\right) \equiv (a_k + a_{k-1} + \cdots + a_0) (\mathrm{mod}\ 3)$$

- Therefore, n is divisible by 3 if and only if the sum of the digits of n is divisible by 3 (how?).
- By a similar argument it can be shown that, n is divisible by 9 if and only if the sum of the digits of n is divisible by 9.

Example 10:

- Let $n=987654321$.
- Notice that $1+2+\cdots+9=45$.
- Because $3|45$ and $9|45$, n is divisible by both 3 and 9.

Perpetual Calendar

- In this section, we present a formula that gives us the day of the week of any date of any year in the Gregorian calendar.
- This calendar was set up by Pope Gregory in 1582.
- For our purposes, we start from the year 1600
- Because the days of the week form a cycle of length seven, we use a congruence modulo 7.
- We denote each day of the week by a number in the set $\{0,1,2,3,4,5,6\}$.

So, let

Sunday =0,	Monday =1,	Tuesday =2,	Wednesday =3,
Thursday =4,	Friday =5,	Saturday =6.	

Also, we denote each month of the year by a number in the set {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}. So, let

January =11	February =12	March =1	April =2
May =3	June =4	July =5	August =6
September =7	October =8	November =9	December =10

Instead of denoting January by 1, February by 2, March by 3 and so on, we have started numbering from March so that January will be denoted by 11 and February by 12.

- The reason is that the extra day in a leap year comes at the end of February (recall that, leap years would be precisely the years divisible by 4, except that those exactly divisible by 100, would be leap years only if they are divisible by 400. Thus, 2000 is a leap year but 1900 is not a leap year.)

- (for more detail see Rosen, Elementary Number Theory & Its Applications, sixth edition, p 197-200.).

- With this setting, each year is going to start in March and the month of January and February of a particular year would be parts of the preceding year.
- For example, February 1700 is considered the twelfth month of 1699 and September 1700 is considered the seventh month of 1700.

Now, let

$k=$ day of the month,

$m=$ month,

$N=$ year, where N is the current year if the month is not January or February and N is the previous year if the month is January or February. Also, $N=100C+Y$, where

$C=$ century,

$Y=$ particular year of the century.

Example 12:

- For the date August 29, 1967,

  k=29, m=6, N=1967, C=19, Y=67.

- However, for the date February 28, 1967,

  k=28, m=12, N=1966, C=19, Y=66.

Let W denote the day of the week of day k of month m of year N.

Then,

$$W \equiv \left(k + [2.6m - 0.2] - 2C + Y + \left[\frac{Y}{4}\right] + \left[\frac{C}{4}\right]\right) \pmod 7$$

where for each x ∈ R, [x]= the integer part of x.

We can use this congruence to find the day of the week of any date of any year in the Gregorian calendar.

Example 13:

Find the day of the week of January 27, 1700.

Solution:

It is clear that k=27, m=11, N=1699, C=16, and Y=99

(because January is considered as the eleventh month of the preceding year).

Thus, $W \equiv (27 + 28 - 32 + 99 + 24 + 4) = 150 \equiv 3 \pmod 7$.

Therefore, January 27, 1700 was a Wednesday.

Applications of Congruences

- Congruences can be used to develop divisibility tests.
- A congruence has been developed to determine the day of the week for any date in history.