W9 Pre-Lecture

Modular Arithmetic is a system of arithmetic for integers, which contains the remainder

A number x mod N is the equivalent of asking for the remainder of x when divided by N. Two integers a and b are said to be congruent (or in the same equivalence class) modulo N if they have the same remainder upon division by N. In such a case, we say that $a \equiv b \pmod N$

Modular Arithmetic as Remainders

To find $123 + 321 \pmod{11}$ we can take

$$123 + 321 = 444$$

and divide it by 11, which gives us

$$123 + 321 \equiv 4 \pmod{11}$$

We can also do

$$\begin{aligned} 123 + 321 &\equiv 2 + 2 \pmod{11} \\ &\equiv 4 \end{aligned}$$

Congruence

For a positive integer n, the integers a and b are congruent mod n if their remainders when divided by n are the same.

$$52 \equiv 24 \pmod 7$$

Another way of defining this is that integers a and b are congruent mod n if their difference $(a-b)$ is an integer multiple of n, that is, if $\frac{a-b}{n}$ has a remainder of 0.

$$36 \equiv 10 \pmod{13}$$

$36 - 10 = 26$ is an integer multiple of $n = 13$

Addition

Properties of Addition in Modular Arithmetic

1) If $a+b=c$, then $a \ (\mathrm{mod}\ N) + b \ (\mathrm{mod}\ N) \equiv c \ (\mathrm{mod}\ N)$
2) If $a \equiv b \ (\mathrm{mod}\ N)$, then $a+K \equiv b+K \ (\mathrm{mod}\ N)$ for any integer K
3) If $a \equiv b \ (\mathrm{mod}\ N)$ and $c \equiv d \ (\mathrm{mod}\ N)$, then $a+c \equiv b+d \ (\mathrm{mod}\ N)$
4) If $a \equiv b \ (\mathrm{mod}\ N)$, then $-a \equiv -b \ (\mathrm{mod}\ N)$

Example:

1. It is currently 7:00 pm. What time (in AM or PM) will it be in 1000 hours?

$$1000 \equiv 16 + (24 \times 41) \equiv 16$$

The time in 1000 hrs is equivalent to the time in 16 hrs. Therefore it will be 11.00 am in 1000 hrs.

2. Find the sum of 31 and 148 in modulo 24.

Solution 1

$31 \equiv 7$

31 in modulo 24 is 7. With property 2 and 1,

$$31 + 148 \equiv 7 + 148 \equiv 155 \ (\mathrm{mod}\ 24)$$
$$\equiv 11$$

Solution 2

148 in modulo 24 is 4. $7+4=11$.

Multiplication

Properties of Multiplication in Modular Arithmetic

1. If $a \cdot b = c$, then $a \ (\mathrm{mod}\ N) \cdot b \ (\mathrm{mod}\ N) \equiv c \ (\mathrm{mod}\ N)$
2. If $a \equiv b \ (\mathrm{mod}\ N)$, then $Ka \equiv Kb \ (\mathrm{mod}\ N)$ for any integer K.
3. If $a \equiv b \ (\mathrm{mod}\ N)$ and $c \equiv d \ (\mathrm{mod}\ N)$, then $ac \equiv bd \ (\mathrm{mod}\ N)$

Examples:

3. What is $(8 \times 16) \pmod 7$?

Since $8 \equiv 1 \pmod 7$ and $16 \equiv 2 \pmod 7$, we have

$$(8 \times 16) \equiv (1 \times 2) \equiv 2 \pmod 7$$

4. Prove property 3 of multiplication in modular arithmetic.

By the definition of equivalence, $a-b$ is a multiple of N and $c-d$ is a multiple of N. That is,

$$a-b = k_1 N, \quad c-d = k_2 N$$

for constants k_1 and k_2. Then

$ac \equiv bd$

$$\begin{aligned} ac - bd &= ac - bd + bc - bc \\ &= c(a-b) + b(c-d) \\ &= c(k_1 N) + b(k_2 N) \\ &= (ck_1 + ck_2)N \end{aligned}$$

This implies $ac-bd$ is a multiple of N and therefore $ac-bd \equiv 0 \pmod N$, or $ac \equiv bd \pmod N$.

QED

Gradescope

1. Select all values congruent to 11 mod 7

4, -10, 53, -3

2. What is the remainder of the following sum when divided by 13?

$28 + 54 + 143 + 98 + 118$

$28 \equiv 2$, $54 \equiv 2$, $143 \equiv 0$, $98 \equiv 7$, $118 \equiv 1$

Remainder $= 2 + 2 + 0 + 7 + 1$
$= 12$

3. At a sporting event half time show 7 contestants are lined up numbered 1 to 7.

If the host points at the contestants in the order 1, 2, 3, 4, 5, 6, 7, 6, 5, 4, 3, 2, 1, 2, ... and says the 1000th person pointed to will win a prize, which position is the winner?

mod = 12

$1000 \equiv 4 + (83 \cdot 12) \equiv 4 \pmod{12}$

The 1000th person is on the 4th position