Tutorial 2: Divisibility and Congruence

MATH 1200A02: Problems, Conjectures, and Proofs

Joe Tran (jtran0@yorku.ca)

York University

September 19, 2023

Divisibility

Definition (Divisibility)

Let $a, b \in \mathbb{Z}$ be integers. We say that a divides b if there exists some integer $k \in \mathbb{Z}$ such that $b = ka$, i.e. b is an integer multiple of a. We denote a divides by by $a \mid b$.

Example

Determine whether the following divides each of the following numbers:

$$3 \mid 27 \quad 4 \mid 16 \quad 5 \mid 13 \quad 2 \mid 6 \quad 3 \mid 111$$

Now suppose we have $n \in \mathbb{N}$ (positive integer, or natural number), and a and b are integers. What does it mean for n to divide $a - b$?

Congruence Modulo n

The statement n divides $a - b$ means that there exists some integer $k \in \mathbb{Z}$ such that

$$a - b = kn$$

From this statement here, is the same as saying a is congruent to b, modulo n, and we write

$$a \equiv b \pmod{n}$$

So we have three equivalent ways of stating congruence modulo n.

- $a \equiv b \pmod{n}$
- $n \mid a - b$
- There exists an integer $k \in \mathbb{Z}$ such that $a - b = kn$.

Example

Let $a = 10$, $b = 3$ and $n = 7$. Then is $10 \equiv 3 \pmod{7}$ true? What about if $b = 10$? $b = 17$? $b = 24$? What is the general case for the value of b that makes $10 \equiv b \pmod{7}$ true?

Properties of Congruence Modulo n

Theorem (Theorem 3.28, page 147)

Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$ be integers such that

$$a \equiv b \pmod{n} \quad c \equiv d \pmod{n}$$

Then

1. $a + c \equiv b + d \pmod{n}$
2. $ac \equiv bd \pmod{n}$
3. *For* $m \in \mathbb{N}$, $a^m \equiv b^m \pmod{n}$

Properties of Congruence Modulo n

Example

Let $a = 10$, $b = 3$, $c = 6$, $d = -1$, $n = 7$, and $m = 2$. Then we have

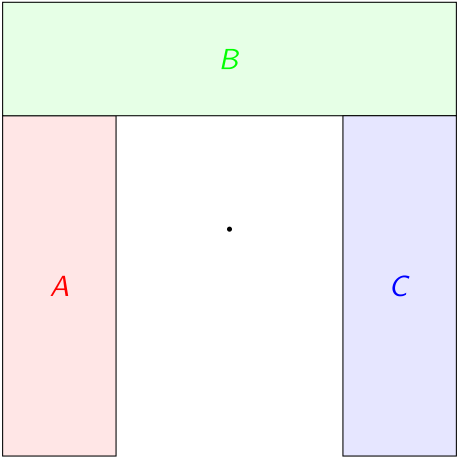
$$10 \equiv 3 \pmod 7 \quad 6 \equiv -1 \pmod 7$$

Both of which are true since $10 - 3 = 7k_1$ and $6 - (-1) = 7k_2$ for some integers $k_1, k_2 \in \mathbb{Z}$ (in particular, $k_1 = k_2 = 1$). Using Theorem 3.28, observe we have (1) $a + c = 16$ and $b + d = 2$, (2) $ac = 60$ and $bd = -3$, and (3) $a^2 = 100$ and $b^2 = 9$. And so now,

1. $(a + b) - (b + d) = 16 - 2 = 14 = 7k_3 \Rightarrow 16 \equiv 2 \pmod 7$
2. $ac - bd = 60 - (-3) = 63 = 7k_4 \Rightarrow 60 \equiv -3 \pmod 7$
3. $a^2 - b^2 = 100 - 9 = 91 = 7k_5 \Rightarrow 100 \equiv 9 \pmod 7$

Participation Activity

Please be seated with your groups according to the map of the room below:



Participation Activity

Activity 1 (10 minutes)

1. Let $m = 3$ for Group A, $m = 5$ for Group B, $m = 7$ for Group C
   1. List all elements in $S = \{a \in \mathbb{Z} : -20 \leq a \leq 20 \text{ and } a \equiv 1 \pmod{m}\}$
   2. Let $S_1 = \{a \in \mathbb{Z} : a \equiv 1 \pmod{m}\}$
      1. Determine whether S_1 is closed under subtraction. Justify your answer.
      2. Determine whether S_1 is closed under multiplication. Justify your answer.

Participation Activity

Activity 2 (10 minutes)

Let $n = 4$ for Group A, $n = 6$ for Group B, $n = 7$ for Group C.

1. Use Theorem 3.28 (3) to compute n^2, n^4, $(= n^{2^2})$, $n^8(= n^{2^3})$, and $n^{16}(= n^{2^4})$ modulo 100
2. Write 22 as a sum of powers of 2 and use part (a) to find the last two digits of n^{22}.
3. Write 99 as a sum of powers of 2, and compute the last two digits of n^{99}

Hint

Say if we want to compute n^4 mod 100, first observe that $n^4 = n^{2^2}$, but also $n^2 = (n)^2$ so by Theorem 3.28, $n^4 \equiv n^2 \pmod{100}$ is the same as $(n^2)^2 \equiv (n)^2 \pmod{100}$, which is also the same as $n^($