Number Theory - Day 4

Overview
- Intro to Modular Arithmetic
- Problems

$\frac{12}{4} = 3$ R 0 → $12 \equiv 0 \pmod 4$

$\frac{a}{b} = q$ R c → $a \equiv c \pmod b$

$a = b \cdot q + c$

$12 + 16 = 28/4$ → R 0

$0 + 0 = 0$

$a \equiv b \pmod c$

$k \equiv z \pmod c$

$\Rightarrow a + k \equiv b + z \pmod c$

$12 \equiv 22 \pmod{10}$

R 2 R 2

$11 \equiv 1 \pmod{10}$

$205 \equiv 5 \pmod{10}$

$11 + 205 \equiv 1 + 5 \pmod{10}$

$\equiv 6 \pmod{10}$

$13 \equiv 3 \pmod{10}$; $19 \equiv 9 \pmod{10}$

$13 + 19 \equiv 3 + 9 \pmod{10}$

$\equiv 12 \pmod{10}$

$\equiv 2 \pmod{10}$

$12 \pmod{10}$ $\frac{12}{10}$ → R 2

3. True or False: 356 ≡ 24 (mod 4).

$356 \equiv 24 \pmod 4$

$356 \pmod 4 = 24 \pmod 4$

a b c ÷ 4 or not

b c ÷ 4

$25 \cdot 4 = 100$

$\frac{356}{4} = q + 0$ → 0

$\frac{24}{4} = 6 + 0$ → 0

$356 \equiv 24 \pmod 4$

→ True

$-15 \pmod 3$

$\frac{-15}{3} = -5$ R 0

$-15 \pmod 3 = 0$

$-16 \pmod 3$

$\frac{-16}{3} = -5 + R(-1)$

$= -6 + R(2)$

$-16 = -5 \cdot 3 + (-1)5$ → $-16 \equiv 2 \pmod 3$

$= -6 \cdot 3 + (2)$ $\equiv -1 \pmod 3$

$5 \equiv -1 \pmod 3$

$\boxed{\begin{aligned} a &\equiv b \pmod c \\ &\equiv c + b \pmod c \end{aligned}}$

$12 \equiv 2 \pmod 5$

$12 \equiv 7 \pmod 5$

$7 \pmod 5$ → 2

Modular Identity

$a \equiv k \pmod b$

$a \equiv mb + k \pmod b$

$13 \equiv 1 \pmod 2$

$13 \equiv 2m + 1 \pmod 2$

$2 \cdot 24 + 1$

$13 \equiv 49 \pmod 2$

residue table for mod 5

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

5 +

6

7 (mod 5)

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$2 \cdot 3 = 6$

$6 \pmod 5$

$\equiv 1$

$4 + 3 \pmod 5 = 7 \pmod 5$

$= 2$

7 inverse of 100

100 is an inverse of 7 (mod 5)

Inverses

given → $a \cdot b \equiv 1 \pmod k$

b is a's inverse modulo k

$20 \equiv 5 \pmod 5$

$\equiv 0 \pmod 5$

$5x \equiv 1 \pmod 6$

x → modular inverse of 5 mod 6

	0	1	2	3	4	5
0						
1						
2						
3						
4						
5	0	5	4	3	2	1

$10 \pmod 6 = 4$

$15 \pmod 6 = 3$

$5x \equiv 1 \pmod 6$

$\cdot 5 \quad \cdot 5$

$5x \cdot 5 \equiv 5 \pmod 6$

$x = 5$ $(5 \cdot 5)x \equiv 5 \pmod 6$

$1 \cdot x \equiv 5 \pmod 6$

$25 \pmod 6 \Rightarrow 1$ $x \equiv 5 \pmod 6$

$6 \cdot 4 = 24$ 25

+1

$\frac{5}{6}$ → R 5

$\frac{11}{6}$ → R 5

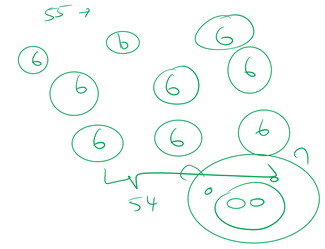
$x \equiv 6m + 5 \pmod 6$

11

17

→ 11 cows · 5 = 55

55 →



54

last digit of 3^{2021}?

$112 \pmod{10} = 2$

$3^{2021} \pmod{10}$

$3^2 = -1 \pmod{10}$

$9 \equiv -1 \pmod{10}$

3^{2021}

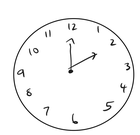
3^2 3^2

...

$(3^2)^{1010} \cdot 3 \pmod{10}$

$(-1)^{1010} \cdot 3 \pmod{10}$

$1 \cdot 3 \pmod{10} = \boxed{3 \pmod{10}}$



17:00 → NPT

05:00 (mod 12)

→ 5:00

0, 1, 2, 3, 4 17:00 (mod 12) = 5

5:00 pm

$103 \equiv 3 \pmod{10}$

remainder

$3\overline{12} \equiv 0 \pmod 4$

$-1 \quad -1$

$311 \equiv -1 \pmod 4$ → residue

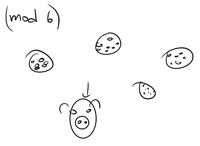
$\equiv 4 + (-1) = 3 \pmod 4$

$311 \pmod 4$

Farmer John has x cows, and he wants find out what x is.

$x \cdot 5 \equiv 1 \pmod 6$

$5x$ →



34. Prove that for any integer n, the number $n^3 + 5n$ is divisible by 6.

$3^3 + 5 \cdot 3$

$27 + 15 = 42$

$n^3 + 5n$

$n(n^2 + 5)$

odd + 5

n = odd

odd (even)

$n^3 + 5n$

$n(n^2 + 5)$

$n(n^2 + 5)$

$n^2 \equiv 1 \pmod 3$

$(1^2 + 5)$

$6 - (\text{mod}(3)) = 0$

6

2 3

$(3^2)^2 = 3^4$

$9^2 = 81$

$n \equiv 0 \bmod 3$

$n \equiv 1 \bmod 3$

$n \equiv 2 \pmod 3$

Prove that the last digit of a fourth power can only be 0, 1, 5, or 6.

$n^4 \pmod{10}$

n	$n^4 \pmod{10}$
0	0
1	1
2	6
3	1
4	6
5	5
6	6
7	1
8	6
9	1

$5 \cdot 5 \ldots$

$n \equiv 2 \pmod 3$

$n \equiv -1 \pmod 3$

$n(1 + 5)$

13

$n \equiv 1 \pmod 3$

$n = 4$

$4(4^2 + 5)$

$4(16 + 5) = 4(21)$ → 13

$n(n^2 + 5)$ → ? | 3 ?

2

$n \equiv 0 \bmod 3$

$n \equiv 1 \pmod 3$

$1(1^2 + 5)$

$1(6) = 6 \pmod 3 = \boxed{0} \pmod 3$

$(-1)^{20}$

2^{20}

$n = 2 \pmod 3$

$2(2^2 + 5)$

$9 \cdot 2 = 18 \pmod 3 = 0 \pmod 3$