
GO
CLASSES

Modular Arithmetic - 2

GO CLASSES

Which is/are true ?

$12 \equiv 8 \ (mod\ 4)$

$15 \equiv 12 \ (mod\ 3)$

$0 \equiv 12 \ (mod\ 13)$

$-1 \equiv 2 \ (mod\ 3)$

if we have

$$\begin{aligned} a &= c \\ b &= d, \end{aligned}$$

then we can combine them in many different ways, to obtain:

$$\begin{aligned} a+b &= c+d, \\ a-b &= c-d, \\ a\times b &= c\times d. \end{aligned}$$

Suppose we have the following two congruence relations:

$$\begin{aligned} a &\equiv c \pmod{m} \\ b &\equiv d \pmod{m}. \end{aligned}$$

Are we able to combine these to obtain

$$\begin{aligned} a+b &\equiv c+d \pmod{m}, \\ a-b &\equiv c-d \pmod{m}, \\ a\times b &\equiv c\times d \pmod{m}? \end{aligned}$$

Theorem

$$\begin{aligned} &\textit{If} && a \equiv b \pmod{m} && \textit{and} \\ &&& c \equiv d \pmod{m}, && \textit{then} \\ &&& a+c \equiv b+d \pmod{m}. \end{aligned}$$

Theorem

$$\begin{aligned} &\textit{If} && \begin{cases} a \equiv b \pmod{m} && \textit{and} \\ c \equiv d \pmod{m}, && \textit{then} \end{cases} \\ &&& a \times c \equiv b \times d \pmod{m}. \end{aligned}$$

GO CLASSES

given $a \equiv b \pmod{m}$

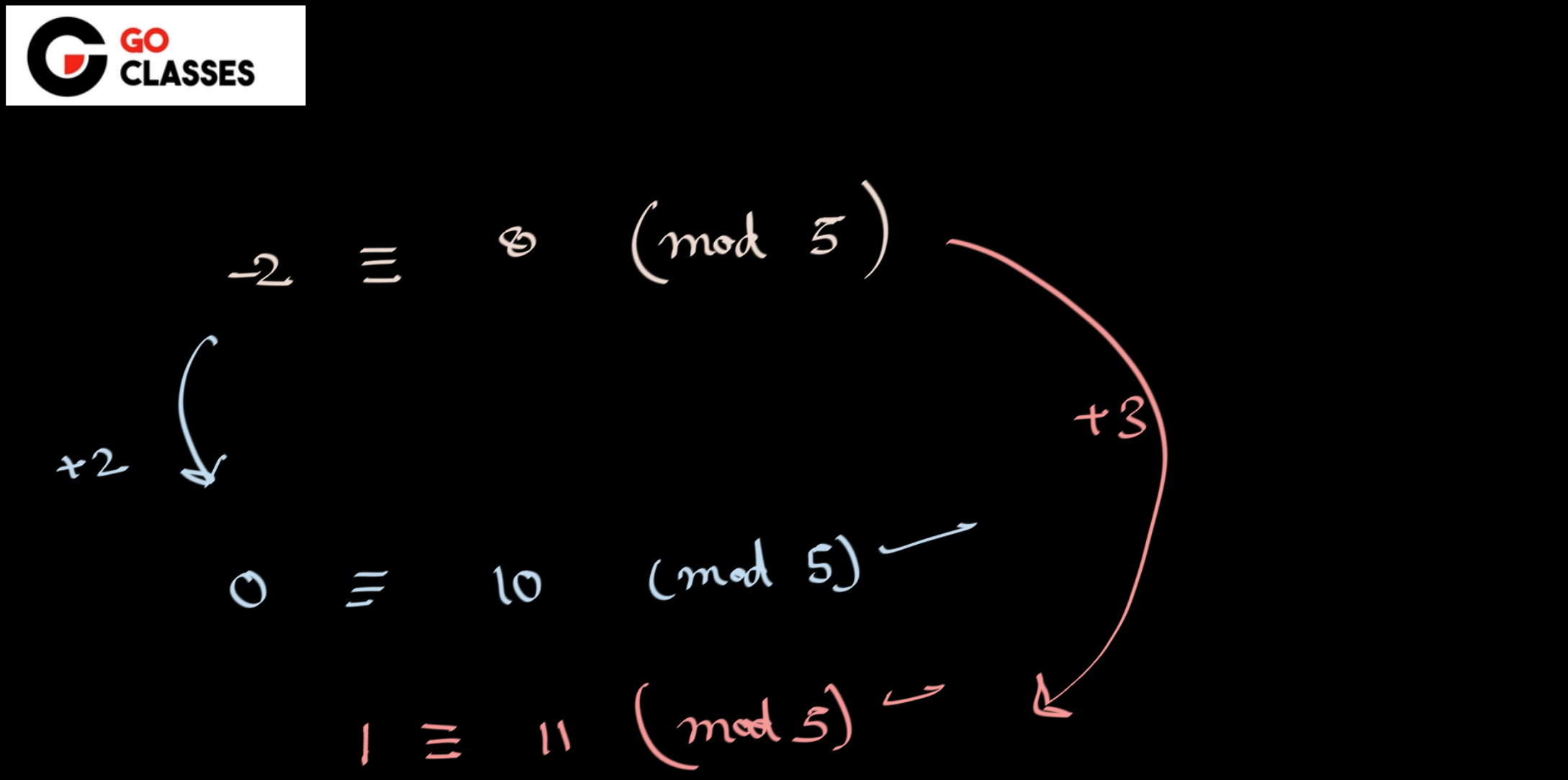
$$a + k \equiv b + k \pmod{m}$$

Proof :

$$a \equiv b \pmod{m} \quad \text{— (1)} \qquad \text{given}$$

$$k \equiv k \pmod{m} \quad \text{— (2)}$$

$$a + k \equiv b + k \pmod{m}$$


GO CLASSES
$-2 \equiv 8 \pmod 5$
+2
+3
$0 \equiv 10 \pmod 5$
$1 \equiv 11 \pmod 5$

$-2 \equiv 8 \pmod 5$

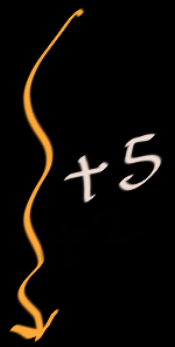
$+2$

$0 \equiv 8 \pmod 5$ ⟶ false

No

GO CLASSES

$-2 \equiv \quad ? \quad (\text{mod } 5)$



$3 \equiv \quad ? \quad (\text{mod } 5)$

GO CLASSES

Which are ALWAYS true?

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

1. $a+n \equiv b \pmod{n}$ ✓
2. $a+3n \equiv b+2n \pmod{n}$
3. $a+k \equiv b+n \pmod{n}$ ✗
4. $a+k+3n \equiv b+k \pmod{n}$ ✓
5. $a+2k \equiv b+k \pmod{n}$ ✗

GO CLASSES

$a \equiv b \pmod{n}$

H.W.

ashesh to Everyone 7:29 PM

a

n|(a-b) is not same as n|(a+2k-b-k)

$a+2k \equiv b+k \pmod{n}$ ← false

$a+k \equiv b \pmod{n}$ ← false

THEOREM 5 Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \qquad \text{and} \qquad ac \equiv bd \pmod{m}.$$

Proof: We use a direct proof. Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, there are integers s and t with $b = a + sm$ and $d = c + tm$. Hence,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

and

$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm).$$

Hence,

$$a + c \equiv b + d \pmod{m} \qquad \text{and} \qquad ac \equiv bd \pmod{m}.$$

GO CLASSES

$c \equiv d \pmod m$

$a \equiv b \pmod m$ $\Rightarrow$ $a + c \equiv b + d \pmod m$

$m \mid b - a \Rightarrow b - a = k_1 m \Rightarrow b = k_1 m + a$

$m \mid d - c \Rightarrow d - c = k_2 m \Rightarrow d = k_2 m + c$

$b + d = a + c + m(k_1 + k_2)$

$b + d \equiv a + c \pmod m$

GO CLASSES

$c \equiv d \pmod m$

$a \equiv b \pmod m$ $\Rightarrow$ $ac \equiv bd \pmod m$

$m \mid b-a \Rightarrow b-a = k_1 m \Rightarrow b = k_1 m + a$

$m \mid d-c \Rightarrow d-c = k_2 m \Rightarrow d = k_2 m + c$

$bd = (k_1 m + a)(k_2 m + c) = ac + m(k)$

$$\begin{cases} a \equiv r \pmod m \\ a + km \equiv r \pmod m \end{cases}$$

$$b + d = a + c + mk$$

Remainder of $b+d$ Same as Remainder of $a+c$

$b+d \bmod m$ $\quad$ $a+c \bmod m$

GO CLASSES

$3 \mid 15 \Rightarrow 15 = 3 \times 5$

$10 \mid 50 \Rightarrow 50 = 10 \times 5$

GO CLASSES

$a \equiv c \pmod m$

If

$a \bmod m \cdot c \bmod m \pmod m$

$m \mid a-b$ or $m \mid b-a$

GO CLASSES

Example

$3 \equiv -2 \mod 5$ — ①

$2 \equiv -3 \mod 5$ — ②

$6 \equiv 6 \mod 5$

GO CLASSES

Example

$-1 \equiv 7 \pmod 8$

$17 \equiv 25 \pmod 8$

$\Rightarrow -17 \equiv 175 \pmod 8$ (+24 = 7)

$\Rightarrow 7 \equiv 175 \pmod 8$ (7 ↓)

Can you cancel arbitrary number ?

$8.2 \equiv 3.2 \pmod{10}$ True

$8.\cancel{2} \equiv 3.\cancel{2} \pmod{10}$

$\Rightarrow 8 \equiv 3 \pmod{10}$

[You can not divide by arbitary number.]

Can you cancel arbitrary number ?

$8.2 \equiv 3.2 \ (mod\ 10)$

$8.2 \equiv 3.2 \ (mod\ 10)$

$8 \equiv 3 \ (mod\ 10)$

Just have to give 1 example

Person1 : in the village it rains everyday

Person2 : in the village it does not rain everyday

GO CLASSES

$8^{8^{\cdot 3}} \equiv$?

$8^{8^{\cdot 3}} \pmod{10}$

$8^{8^{\cdot 3}}$

$8^{\cdot 3}$

4

8^{4}

GO CLASSES

$8 \cdot 3 \equiv 88 \cdot 3 \mod 10$

$8 \cdot 3 \equiv 88 \cdot 3 \mod 10$

$8 \equiv 88 \mod 10$

Yes

Example 1. If we know that $a \equiv 3 \pmod{7}$ and we know that $b \equiv 4 \pmod{7}$, then we can determine that $ab \equiv 12 \equiv 5 \pmod{7}$.

GO CLASSES

$a \equiv b \mod n$

$k \equiv k \mod n$

$\Downarrow$

$ak \equiv bk \mod n$

"inverse modulo"

Optional Question

Example. (**Solving a congruence**) Solve $3x + 4 \equiv 2x + 8 \pmod 9$.

$$3x + 4 \equiv 2x + 8 \pmod 9$$

$$x + 4 \equiv 8 \pmod 9$$

$$x \equiv 4 \pmod 9$$

$x \equiv 4 \mod 9$

$4-9, 4, 4+9, 4+2\cdot 9$

$4+nk$

$9 \mid x-4 \Rightarrow x-4 = 9k$

$x = 4+9k$

$$x \equiv 4 \mod 9$$

$$\downarrow$$

$$9 \mid x-4$$

$$x-4 = 9k \Rightarrow x = 4+9k$$

Example. (**Solving a congruence**) Solve $3x + 4 \equiv 2x + 8 \pmod 9$.

In this case, I'll solve the modular equation by adding or subtracting the same thing from both sides.

$$\begin{array}{rrcrcrcl}
 & 3x & + & 4 & \equiv & 2x & + & 8 \pmod 9 \\
- & & & 4 & \equiv & & & 4 \pmod 9 \\
\hline
 & 3x & & & \equiv & 2x & + & 4 \pmod 9 \\
- & 2x & & & \equiv & 2x & & \pmod 9 \\
\hline
 & x & & & \equiv & & & 4 \pmod 9
\end{array}$$

The solution is $x \equiv 4 \pmod 9$. □

$[\,9 \mid 3x+4-(2x+8)\,]$

$3x+4 \quad -2x-8 \quad = 9k$

$x = 4+9k$

https://sites.millersville.edu/bikenaga/abstract-algebra-1/modular-arithmetic/modular-arithmetic.pdf

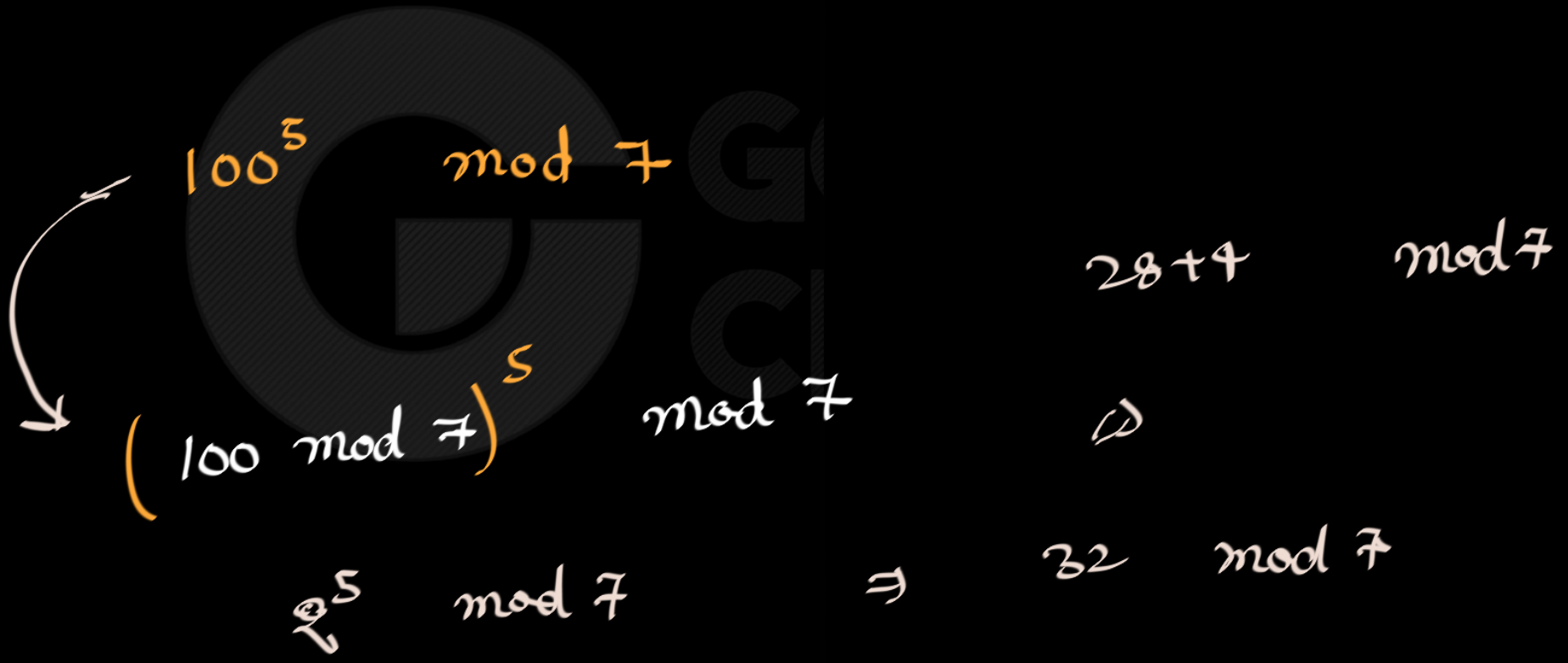
True/False

H.W.

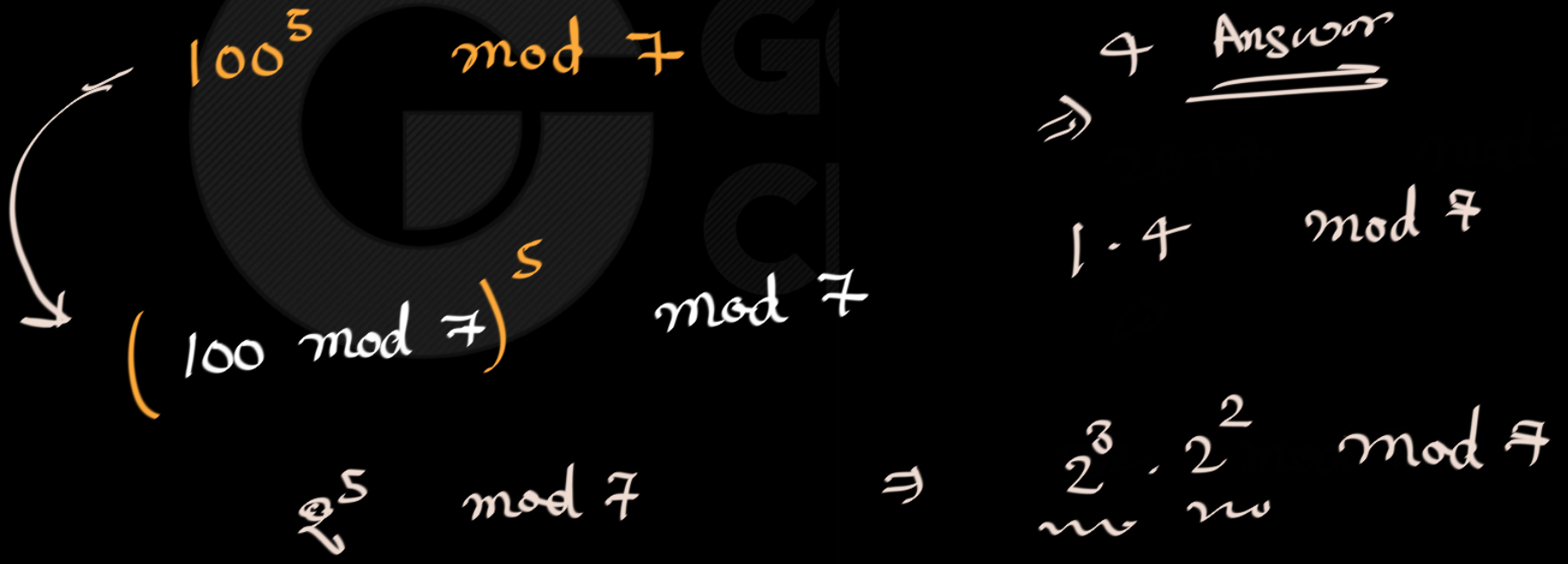
(a) $101 \equiv 2 \pmod 3$

(b) $-101 \equiv 1 \pmod 3$

Example. (**Reducing an expression mod n**) Reduce $100^5 \pmod 7$ to an element in the standard residue system $\{0, 1, \ldots, 6\}$.



Example. (**Reducing an expression mod n**) Reduce $100^5 \pmod 7$ to an element in the standard residue system $\{0, 1, \ldots, 6\}$.



GO CLASSES

$a \equiv b \mod n$

$a \equiv b \mod n$

$\forall \exists \; a^k \equiv b^k \mod n$

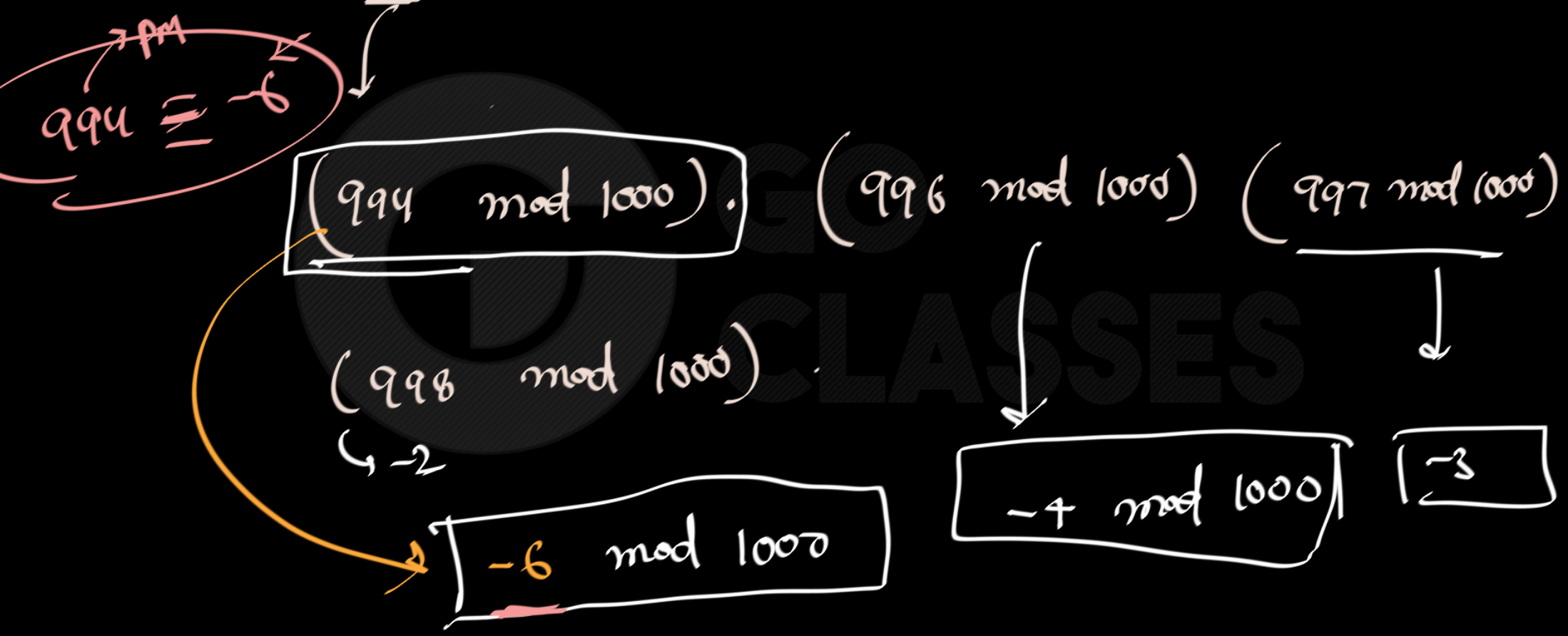
$100^5 \mod 7$

Example. (**Reducing an expression mod n**) Reduce $100^5 \pmod 7$ to an element in the standard residue system $\{0, 1, \ldots, 6\}$.

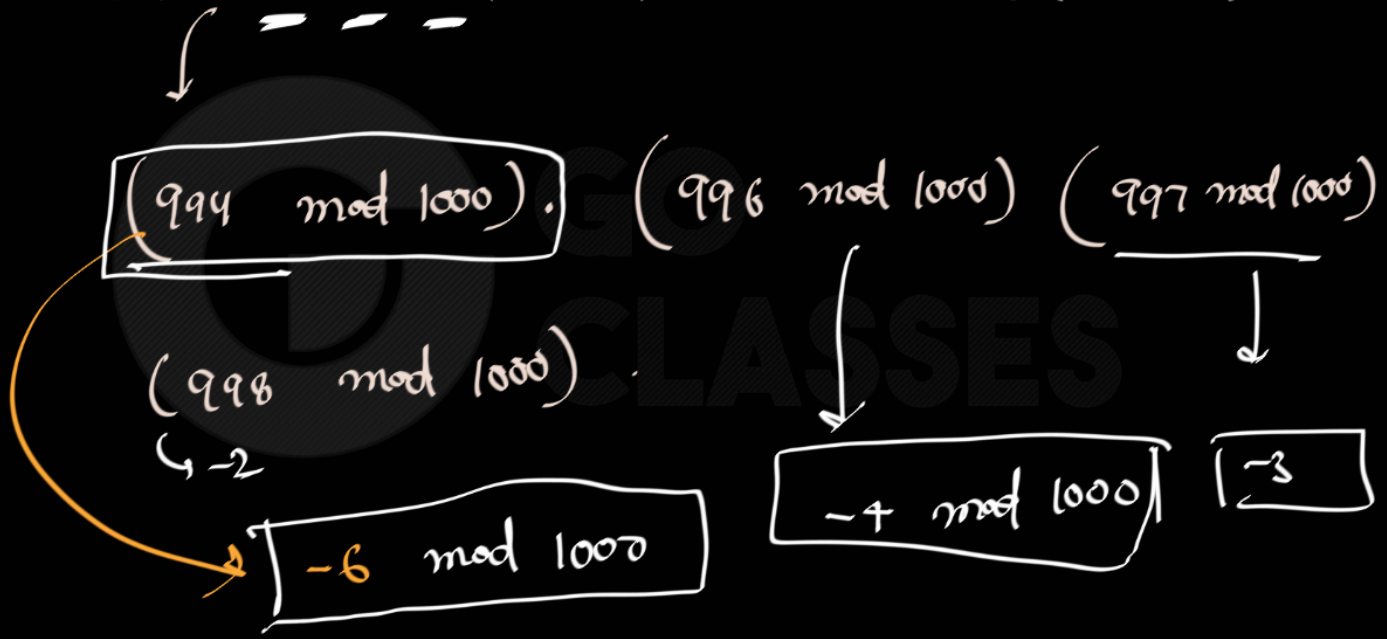
$100 \equiv 2 \pmod 7$, so

$$100^5 \equiv 2^5 \equiv 32 = 4 \pmod 7 . \quad \square$$

Example. Simplify $994 \cdot 996 \cdot 997 \cdot 998 \pmod{1000}$ to a number in the range $\{0, 1, \ldots 999\}$.



Example. Simplify $994 \cdot 996 \cdot 997 \cdot 998 \pmod{1000}$ to a number in the range $\{0, 1, \ldots 999\}$.



$(-6) \times (-4) \times (-3) \times (-2) \pmod{1000}$

$24 \times 6 = 144$

GO CLASSES

$$994 \equiv -6 \pmod{1000}$$

$$\downarrow +1000$$

$$994 \equiv 994 \pmod{1000}$$

Example. Simplify $994 \cdot 996 \cdot 997 \cdot 998 \pmod{1000}$ to a number in the range $\{0, 1, \ldots 999\}$.

Rather than deal with large "positive" numbers, I'll convert them to small "negative" numbers:

$$994 \equiv -6 \pmod{1000}, \quad 996 \equiv -4 \pmod{1000}, \quad 997 \equiv -3 \pmod{1000}, \quad 998 \equiv -2 \pmod{1000}.$$

So

$$994 \cdot 996 \cdot 997 \cdot 998 \equiv (-6)(-4)(-3)(-2) \equiv 144 \pmod{1000}. \quad \square$$

Example . Can we simplify 17^{753} in arithmetic modulo 9?

$17^{753} \mod 9$

$(17 \mod 9)^{753} \mod 9$

$17 \equiv -1 \mod 9$

17

-1

8

GO CLASSES

Option 1

$17^{753} \mod 9$

① $(-1)^{753} \mod 9$

② $= -1 \mod 9$

③ $= 8$

Option 2

$17^{753} \mod 9$

$8^{753} \mod 9$

$17 \equiv -1 \mod 9$

$8 \cdot 8^{752} \mod 9$

$8 \cdot (8^2)^{376} \mod 9$

$8 \cdot 64^{376} \mod 9$

$8 \cdot 1^{376} \mod 9 \Rightarrow 8$

GO CLASSES

$17^{753} \mod 9$

$(-1)^{753} \mod 9$

$16^{523} \mod 9$

$(-2)^{523} \mod 9$

tharun kumar to Everyone 8:34 PM

tk

instead of 17 there if we have
16 as -2
15 as -3
14 as -4
can we write like this?

Example. Can we simplify 17^{753} in arithmetic modulo 9? We first note that $17 \equiv -1 \pmod 9$, because 17 and -1 differ by a multiple of 9. Theorem 16 allows us to then combine this congruence relation as many times as we would like. In particular, by combining 753 copies, we obtain $17^{753} \equiv (-1)^{753} \pmod 9$. Since $(-1)^n = -1$ for any odd integer n, we have $17^{753} \equiv -1 \pmod 9$. Finally, if we would like to have a simple, positive answer, then we can add 9 to obtain a final answer of 8.

GATE CSE 2016

The value of the expression $13^{99} \pmod{17}$ in the range 0 to 16, is _____.

gate2016-cse-set2 | modular-arithmetic | normal | numerical-answers

$(-4)^{99} \mod 17 \Rightarrow -4 \cdot (-4)^{98} \mod 17$

$-4 \cdot ((-4)^2)^{49} \mod 17$

$\Rightarrow -4 \cdot -1 \mod 17$

$-4 \cdot 16^{49} \mod 17$

$= -4 \cdot (-1)^{49} \mod 17$

$= 4 \mod 17$

$= 4$

https://gateoverflow.in/39588/gate-cse-2016-set-2-question-29

GATE CSE 2019

The value of $3^{51} \bmod 5$ is _____

https://gateoverflow.in/302827/gate-cse-2019-question-21

GO CLASSES

The value of $3^{51} \bmod 5$ is _____

Option 1

$(-2)^{51} \bmod 5$

$-2 \cdot (-2)^{50} \bmod 5$

$-2 \cdot (4)^{25} \bmod 5$

$-2 \cdot (-1)^{25} \bmod 5 = -2 \cdot -1 \bmod 5 = 2$

Option 2

$3^{51} \bmod 5$

$3 \cdot 3^{50} \bmod 5$

$3 \cdot 9^{25} \bmod 5$

$3 \cdot 4^{25} \bmod 5$

$3 \cdot 4 \cdot 4^{24} \bmod 5$

$12 \cdot 16^{12} \bmod 5$

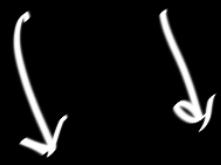
2 Answer

2 mod 5

P

12 mod 5

17 x 18 mod 19



$-2 \times -1 \mod 19$

$= 2$

Answer

$18^{489391312} \ mod \ 19$

$(-1)^{even} \ mod \ 19$

$= 1$

Find the last digit of 7^{100}

$7^{100} \mod 10$

$(-3)^{100} \mod 10$

$9^{50} \mod 10 \Rightarrow$ 1 Answer

Find the last digit of 7^{100}

[Solution: 1]

$7^{100} \equiv (7^2)^{50} \equiv 49^{50} \equiv (-1)^{50} \equiv 1 \bmod 10.$

https://www.math.cmu.edu/~cargue/arml/archive/15-16/number-theory-09-13-15-solutions.pdf

Compute the last digit of 2017^{2017}. mod 10

$7^{2017} \mod 10$

2017^{2017} $\quad 2017$

$(-3)^{2017} \mod 10$

$-3 \cdot (-3)^{2016} \mod 10$

$-3 \quad 9^{1008}$

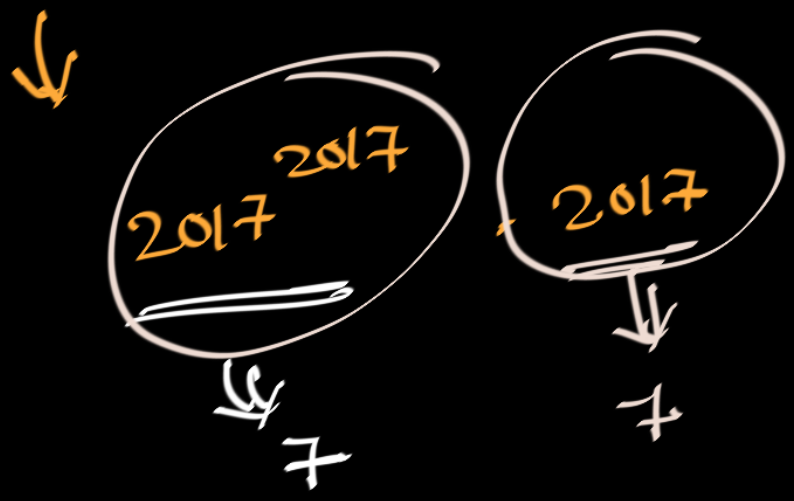
$-3 \cdot (-1)^{\text{even}} = -3 \mod 10$

7 Answer

https://people.math.wisc.edu/~erman/567/Exam_1a_SOLUTIONS.pdf

GO CLASSES

$2017^{2018} \mod 10$



$\mod 10$

$\Rightarrow$ 9 Answer.

2. On this page **only the answer will be graded**. Circle your answer.

(a) Compute the last digit of 2017^{2017}.

Solution: $2017 \equiv 7(\mod 10)$. And $7^4 \equiv (7^2)^2 \equiv 9^2 \equiv 1(\mod 10)$. So we write $2017 = 4 \cdot 504 + 1$ and we get

$$7^{2017} \equiv (7^4)^{504} \cdot 7^1 \equiv 1^{504} \cdot 7^1 \equiv 7(\mod 10).$$

https://people.math.wisc.edu/~erman/567/Exam_1a_SOLUTIONS.pdf

(a) $7 \cdot 9 \pmod{36}$.

(b) $8 - 21 \pmod{31}$.

(c) $68 \cdot 69 \cdot 71 \pmod{72}$.

H.W

(d) $108! \pmod{83}$.

Soln on the next page.

(e) $60^{59} \pmod{61}$.

https://math.mit.edu/~roed/courses/magic/exams/08mid2PS.pdf

5. **Do the following calculations. As always, when working mod n, leave your answer in the range 0, 1, ..., $n-1$.**

(a) $7 \cdot 9 \pmod{36}$.

This is straight-forward: $7 \cdot 9 \equiv 63 \equiv \boxed{27} \pmod{36}$.

(b) $8 - 21 \pmod{31}$.

Again, this is an easy computation: $8 - 21 \equiv -13 \equiv \boxed{18} \pmod{31}$.

(c) $68 \cdot 69 \cdot 71 \pmod{72}$.

If we note that $68 \equiv -4$, $69 \equiv -3$, and $71 \equiv -1$ (all of these are taken $\pmod{72}$), then we get

$$68 \cdot 69 \cdot 71 \equiv -4 \cdot -3 \cdot -1 \equiv -12 \equiv \boxed{60} \pmod{72}.$$

(d) $108! \pmod{83}$.

Note that 83 divides 108!. Therefore, $108! \equiv \boxed{0} \pmod{83}$.

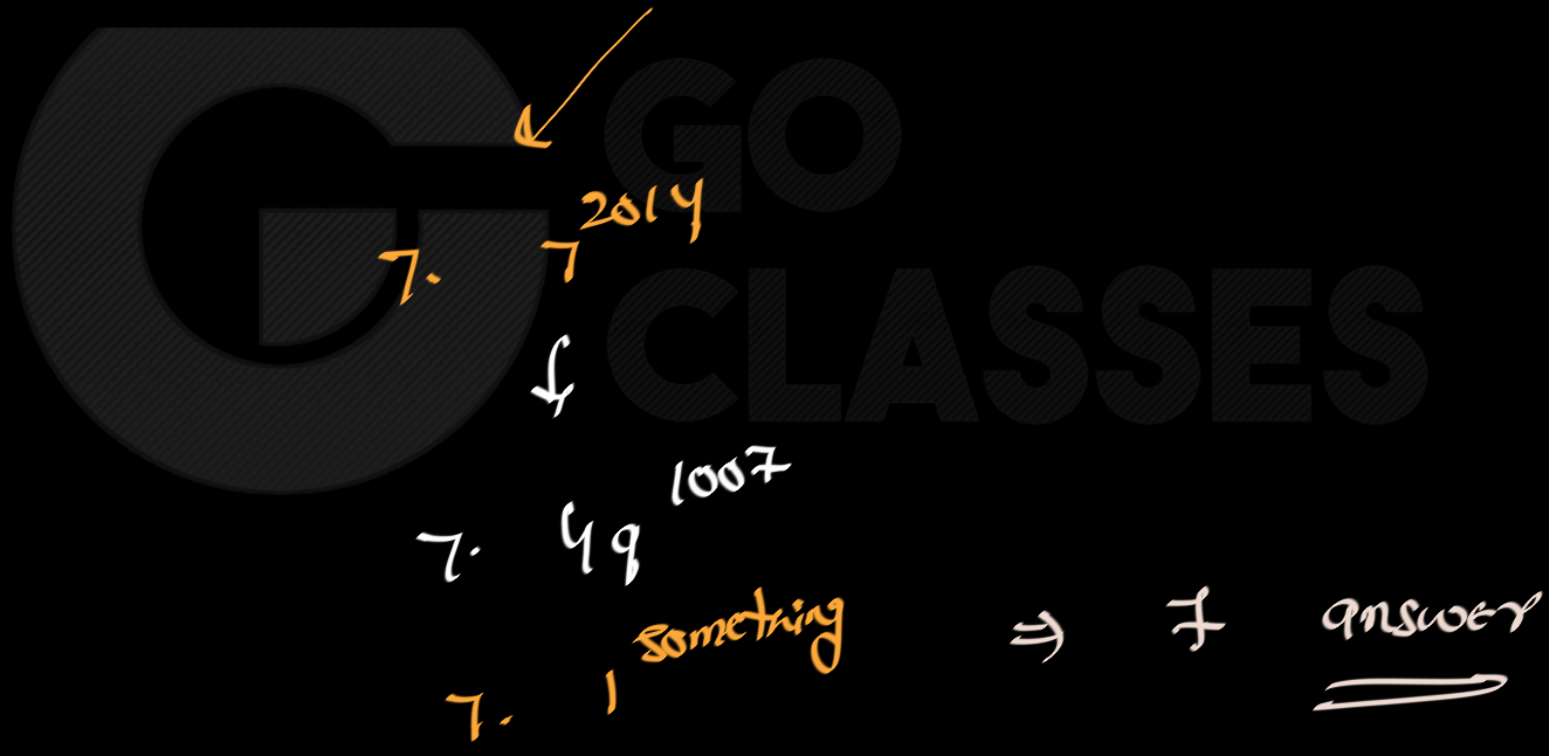
(e) $60^{59} \pmod{61}$.

Observe that $60 \equiv -1 \pmod{61}$. Thus

$$60^{59} \equiv (-1)^{59} \equiv -1 \equiv \boxed{60} \pmod{61}$$

https://math.mit.edu/~roed/courses/magic/exams/08mid2PS.pdf

What is the remainder when 7^{2015} *is divided by* 48*?*



Example 4. *What is the remainder when 7^{2015} is divided by 48?*

Solution. At first, it seems that even modular arithmetic can't prevent this problem from becoming messy. However, upon further inspection, we can see that $7^2 = 49$, which leaves a remainder of 1 when divided by 48! Hence, we can write

$$7^{2015} \equiv 7 \cdot (7^2)^{1007} \equiv 7 \cdot 1^{1007} \equiv \boxed{7} \pmod{48}.$$

Example 2. How can we simplify 20×21 in arithmetic modulo 19?

Example 3. Can we simplify 17^{753} in arithmetic modulo 9?

Example 2. How can we simplify 20×21 in arithmetic modulo 19? We first note that $20 \equiv 1 \pmod{19}$ and also that $21 \equiv 2 \pmod{19}$. Theorem 16 tells us that we can combine these equations to obtain $20 \times 21 \equiv 1 \times 2 \equiv 2 \pmod{19}$.

Example 3. Can we simplify 17^{753} in arithmetic modulo 9? We first note that $17 \equiv -1 \pmod{9}$, because 17 and -1 differ by a multiple of 9. Theorem 16 allows us to then combine this congruence relation as many times as we would like. In particular, by combining 753 copies, we obtain $17^{753} \equiv (-1)^{753} \pmod{9}$. Since $(-1)^n = -1$ for any odd integer n, we have $17^{753} \equiv -1 \pmod{9}$. Finally, if we would like to have a simple, positive answer, then we can add 9 to obtain a final answer of 8.

Theorems 15 and 16 show us that we can treat all numbers that are congruent modulo m as the same, in addition and in multiplication operations. Division is much more complicated, and will not be discussed.

https://www2.math.upenn.edu/~mlazar/math170/notes06-2.pdf

GO CLASSES

T/F

$5776 \mod 9 \Rightarrow 0$

A number is divisible by 9 if and only if the sum of its digits (written in base 10) is divisible by 9.

$5776 = 5000 + 700 + 70 + 6$

$= (5 \times 10^3 + 7 \times 10^2 + 7 \times 10^1 + 6) \mod 9$

$(5 + 7 + 7 + 6) \mod 9$

GO CLASSES

$5776 \mod 9$ ← remainder of 5776 divided by 9

=

$5+7+7+6 \mod 9$

GO CLASSES

(5776 mod 11)

Does it also hold for 11?

$5776 = 5\times10^3 + 7\times10^2 + 7\times10^1 + 6$

(Rightmost)

$5\times(-1)^3 + 7\times(-1)^2 + 7\times(-1)^1 + 6$

$= 5(-1) + 7 + 7(-1) + 6$

$-5 + 7 - 7 + 6 = 1$

GO CLASSES

11) 5776 (525
55

27
22

56
55

1

$-5 + \sqrt{7} - \sqrt{7} + 6$

$= 1$

GO CLASSES

$5776 = 5 \times 10^3 + 7 \times 10^2 + 7 \times 10^1 + 6$

$5 \times 1^3 + 7 \times 1^2 + 7 \times 1 + 6$

$= \underline{5 + 7 + 7 + 6} \mod 3$

GO CLASSES

$a = 15$

$b = 10$

$150 \equiv 12 \pmod 6$

$(15 \times 10) \bmod 6$

$(15 \bmod 6 \times 10 \bmod 6) \bmod 6$

$3 \quad 4 \quad 4$

$= 12$

Theorem 19. *A number is divisible by 9 if and only if the sum of its digits (written in base 10) is divisible by 9.*

Proof. In base 10, every number can be written as a sum of ones, tens, hundreds, thousands, and so forth. For example, $5776 = 5000+700+70+6$. More generally, we can write this as $n = c_0 + c_1 10^1 + c_2 10^2 + c_3 10^3 + \ldots$, where the c_i variables

https://www2.math.upenn.edu/~mlazar/math170/notes06-2.pdf

Example. Reduce $497 \cdot 498 \cdot 499 \pmod{500}$ to a number in the range $\{0, 1, \ldots 499\}$, *doing the computation by hand.*

Example. Reduce $497 \cdot 498 \cdot 499 \pmod{500}$ to a number in the range $\{0, 1, \ldots 499\}$, *doing the computation by hand.*

Note that

$$497 = -3 \pmod{500}, \quad 498 = -2 \pmod{500}, \quad 499 = -1 \pmod{500}.$$

So

$$497 \cdot 498 \cdot 499 = (-3)(-2)(-1) = -6 = 494 \pmod{500}. \quad \square$$

https://sites.millersville.edu/bikenaga/abstract-algebra-1/modular-arithmetic/modular-arithmetic.pdf

Class homework

Example 1: Find the remainder when $25^{100} + 11^{500}$ is divided by 3.

We observe that $25 \equiv 1 \pmod 3$ and $11 \equiv -1 \pmod 3$. Raising these to the approopriate powers, $25^{100} \equiv 1^{100} \pmod 3$ and $11^{500} \equiv (-1)^{500} \pmod 3$. That is,

$25^{100} \equiv 1 \pmod 3$ and $11^{500} \equiv 1 \pmod 3$. Adding these congruecies, we get $25^{100} + 11^{500} \equiv 2 \pmod 3$.

Thus the remainder is 2.

https://www.math.toronto.edu/rosent/Mat246Y/PDF/cong.pdf

Class homework

Example 2: What is the remainder when 3^{5555} is divided by 80?

We notice that $3^4 = 81 \equiv 1 \pmod{80}$. That is, we have $3^4 \equiv 1 \pmod{80}$ ---------- (1)

We also know that 5555 when divided by 4, gives a quotient of 1388 and the remainder 3.

Hence, $3^{5555} = (3^4)^{1388} . 3^3$. Now raising congruence (1) to the power of 1388, we have

$(3^4)^{1388} \equiv 1 \pmod{80}$.

Multiplying this by 3^3 we get $(3^4)^{1388} . 3^3 \equiv 3^3 \pmod{80}$.

Which means, $3^{5555} \equiv 27 \pmod{80}$.

Thus the required remainder is 27. Unfortunately you cannot verify this by using your pocket calculator!

https://www.math.toronto.edu/rosent/Mat246Y/PDF/cong.pdf