ASSIGNMENT #9 SOLUTIONS

1: $4^1 = 4 \equiv 4 \bmod 5$ $\quad 4^2 = 16 \equiv 1 \bmod 5$

SO THE PATTERN IS $4, 1, 4, 1, 4, 1 \ldots$.

=

$4^1 = 4 \equiv 4 \bmod 9$ $\quad 4^2 = 16 \equiv 7 \bmod 9$ $\quad 4^3 \equiv 4 \cdot 7 \bmod 9$

$\equiv 28 \bmod 9$

$\equiv 1 \bmod 9$

SO THE PATTERN IS $4, 7, 1, 4, 7, 1, 4, 7, 1, 4 \ldots$

=

$5^1 \equiv 5 \bmod 8$. NOTE $-3 \equiv 5 \bmod 8$ SO

$5^2 \equiv (-3)^2 \bmod 8$

$\equiv 9 \bmod 8 \equiv 1 \bmod 8$ (OR NOTICE THAT $5^2 = 25 \equiv 1 \bmod 8$)

SO THE PATTERN IS $5, 1, 5, 1, 5, 1, 5, 1 \ldots$.

=

FROM THE SECOND EXAMPLE, WE KNOW $4^2 \equiv 7 \bmod 9$.

SO $7 \bmod 9$, $7^2 \bmod 9$, $7^3 \bmod 9$, $7^4 \bmod 9 \ldots$

IS THE SAME AS $4^2 \bmod 9$, $4^4 \bmod 9$, $4^6 \bmod 9$, $4^8 \bmod 9$

WHICH GIVES $7, 4, 1, 7, 4, 1, 7, 4, 1 \ldots$.

$5^1 \equiv 5 \bmod 9$ $\quad 5^2 = 25 \equiv 7 \bmod 9$

NOTE $-2 \equiv 7 \bmod 9$

SO $5^3 = 5^2 \cdot 5 \equiv -2 \cdot 5 \bmod 9$

$\equiv -10 \bmod 9 \equiv 8 \bmod 9$

NOTE $-1 \equiv 8 \bmod 9$

SO $5^4 = 5^3 \cdot 5 \equiv (-1) \cdot 5 \bmod 9$

$\equiv -5 \bmod 9 \equiv 4 \bmod 9$

$5^5 = 5^4 \cdot 5 \equiv 4 \cdot 5 \bmod 9 \equiv 20 \bmod 9 \equiv 2 \bmod 9$

$5^6 = 5^5 \cdot 5 \equiv 2 \cdot 5 \bmod 9 \equiv 10 \bmod 9 \equiv 1 \bmod 9$

SO THE PATTERN IS $5, 7, 8, 4, 2, 1, 5, 7, 8, 4, 2, 1, 5, 7 \ldots$

=

$5^1 \equiv 5 \bmod 11$ $\quad 5^2 = 25 \equiv 3 \bmod 11$ $\quad 5^3 = 5^2 \cdot 5 \equiv 3 \cdot 5 \bmod 11$

$\equiv 15 \bmod 11$

$\equiv 4 \bmod 11$

$5^4 = 5^2 \cdot 5^2 \equiv 3 \cdot 3 \bmod 11 \equiv 9 \bmod 11.$

$5^5 = 5^2 \cdot 5^3 \equiv 3 \cdot 4 \bmod 11 \equiv 12 \bmod 11 \equiv 1 \bmod 11$

SO THE PATTERN IS $5, 3, 4, 9, 1, 5, 3, 4, 9, 1, 5, 3 \ldots$

$5^1 \equiv 5 \bmod 13$ $\quad 5^2 = 25 = 12 + 13 \equiv 12 \bmod 13$

NOTE $-1 \equiv 12 \bmod 13$.

SO $5^3 = 5^1 \cdot 5^2 \equiv 5 \cdot (-1) \bmod 13$

$\equiv -5 \bmod 13 \equiv 8 \bmod 13$

AND $5^4 = 5^2 \cdot 5^2 \equiv (-1)(-1) \bmod 13$

$\equiv 1 \bmod 13$

SO THE PATTERN IS $5, 12, 8, 1, 5, 12, 8, 1 \ldots$

#2: 17 IS PRIME.

$$\begin{array}{r} 14 \\ 17 \overline{)\,250} \\ \underline{17} \\ 80 \\ \underline{68} \\ 12 \end{array}$$

SO $\not\mid$ 250 IS NOT DIVISIBLE BY 17.

BY LITTLE FERMAT $\boxed{250^{16} \equiv 1 \bmod 17.}$

11 IS PRIME $591 = 550 + 41$. SINCE 550 IS AN INTEGER MULTIPLE OF 11, AND 41 IS NOT, 591 IS NOT DIVISIBLE BY 11.

BY LITTLE FERMAT: $(591)^{10} \equiv 1 \bmod 11$

$$(591)^{100} = ((591)^{10})^{10} \equiv 1^{10} \bmod 11 \equiv 1 \bmod 11$$

=

7 IS PRIME $194 = 140 + 54$. SINCE 140 IS AN INTEGER MULTIPLE OF 7 AND 54 IS NOT 194 IS NOT DIVISIBLE BY 7.

BY LITTLE FERMAT: $194^6 \equiv 1 \bmod 7$

SO $$194^{60} = (194^6)^{10} \equiv 1^{10} \bmod 7 \equiv 1 \bmod 7$$

=

127 IS PRIME AND 2 IS NOT DIVISIBLE BY 127. BY LITTLE FERMAT $2^{126} \equiv 1 \bmod 127$.

$$2^{12603} = 2^{12600} \cdot 2^3 = (2^{126})^{100} \cdot 2^3 \equiv 1 \cdot 2^3 \bmod 127$$
$$\equiv 8 \bmod 127$$

137 IS PRIME AND 3 IS NOT A MULTIPLE OF 137. BY LITTLE FERMAT $3^{136} \equiv 1 \bmod 137$

$3^{1360} = (3^{136})^{10} \equiv 1^{10} \bmod 137 \equiv \boxed{1 \bmod 137}$

=

13 IS PRIME AND 19 IS NOT A MULTIPLE OF 13. NOTE $19 \equiv 6 \bmod 13$. BY LITTLE FERMAT

$19^{12} \equiv 6^{12} \bmod 13 \equiv 1 \bmod 13$. NOTE $6^2 = 36 \equiv 10 \bmod 13$

$\equiv -3 \bmod 13$

SO $19^{12006} = (19^{12})^{1000} \cdot 19^6 \equiv 1^{1000} \cdot 6^6 \bmod 13$

$\equiv 6^2 \cdot 6^2 \cdot 6^2 \bmod 13$

$\equiv (-3)(-3)(-3) \bmod 13$

$\equiv -27 \bmod 13$

$\equiv \boxed{12 \bmod 13}$

=

NOTE $14 \equiv 1 \bmod 13$ SO $(14)^{1201} \equiv 1^{1201} \bmod 13$

$\equiv \boxed{1 \bmod 13}$

#3: $3^1 \equiv 3 \bmod 5$ $\quad 3^2 \equiv 4 \bmod 5$ $\quad 3^3 = 3^2 \cdot 3 \equiv 4 \cdot 3 \bmod 5$
$\equiv 2 \bmod 5$

~~$3^4 = 3^3 \cdot 3$~~ $3^4 = 3^3 \cdot 3 \equiv 2 \cdot 3 \bmod 5 \equiv 1 \bmod 5$, $\boxed{n = 3}$

=

$5^1 \equiv 5 \bmod 7$, $5^2 = 25 \equiv 4 \bmod 7$, $5^3 = 5^2 \cdot 5 \equiv 4 \cdot 5 \bmod 7$
$\equiv 20 \bmod 7$
$\equiv 6 \bmod 7$

$5^4 = 5^2 \cdot 5^2 \equiv 4 \cdot 4 \bmod 7 \equiv 16 \bmod 7 \equiv 2 \bmod 7 \implies \boxed{n = 4}$

=

NOTE $13 \equiv 3 \bmod 10$

SO $13^1 \equiv 3 \bmod 10$ $\quad 13^2 \equiv 3^2 \bmod 10 \equiv 9 \bmod 10$

$13^3 \equiv 3^2 \cdot 3 \bmod 10 = 9 \cdot 3 \bmod 10 \equiv 27 \bmod 10 \equiv 7 \bmod 10$

$\implies \boxed{n = 3}$

=

NOTE THAT REDUCING MOD 101 ISN'T SO BAD IF YOU BREAK YOUR NUMBERS UP INTO THE 10's PLACE AND THE 1's PLACE.

FOR EXAMPLE: $17^2 = (10+7)(10+7) = 100 + 70 + 70 + 49$
$\equiv -1 + 140 + 49 \bmod 101$
$\equiv -1 + 39 + 49 \bmod 101 \equiv 87 \bmod 101$

$17^3 = 17^2 \cdot 17 \equiv 87 \cdot 17 \bmod 101$

$\equiv (80+7)(10+7) \bmod 101$

$\equiv 800 + 560 + 70 + 49 \bmod 101$

$\equiv -8 + 55 + 70 + 49 \bmod 101$

$\equiv -8 + 125 + 49 \bmod 101$

$\equiv -8 + 24 + 49 \bmod 101$

$\equiv 24 + 41 \bmod 101$

$\equiv 65 \bmod 101$

$17^4 = 17^3 \cdot 17 \equiv 65 \cdot 17 \bmod 101$

$\equiv (60+5)(10+7) \bmod 101$

$\equiv 600 + 50 + 420 + 35 \bmod 101$

$\equiv -6 + 50 + 16 + 35 \bmod 101$

$\equiv 50 + 10 + 35 \bmod 101$

$\equiv 95 \bmod 101 \Longrightarrow \boxed{n=4}$

NOTE $-2 \equiv 9 \bmod 11$

$9^1 = 9 \equiv 9 \bmod 11$ $\quad 9^2 \equiv (-2)(-2) \bmod 11 \equiv 4 \bmod 11$

$9^3 = 9^2 \cdot 9 \equiv 4 \cdot (-2) \bmod 11$

$\equiv -8 \bmod 11 \equiv 3 \bmod 11$

$9^4 = 9^2 \cdot 9^2 \equiv 4 \cdot 4 \bmod 11 \equiv 16 \bmod 11 \equiv 5 \bmod 11 \Longrightarrow \boxed{n = 4}$

=

NOTE $-2 \equiv 13 \bmod 15$

$13^1 \equiv 13 \bmod 15$ $\quad 13^2 \equiv (-2)(-2) \bmod 15 \equiv 4 \bmod 15$

$13^3 \equiv (-2)(4) \bmod 15$

$\equiv -8 \bmod 5 \equiv 7 \bmod 15$

$13^4 \equiv (4)(4) \bmod 15 \equiv 16 \bmod 15 \equiv 1 \bmod 15 \Longrightarrow \boxed{n = 4}$

=

$5^1 \equiv 5 \bmod 23$ $\quad 5^2 = 25 \equiv 2 \bmod 23$ $\quad 5^3 = 5^2 \cdot 5 \equiv 10 \cdot 2 \bmod 23$

$\equiv 20 \bmod 23$

$5^4 = 5^2 \cdot 5^2 \equiv 2 \cdot 2 \bmod 23 \equiv 4 \bmod 23$

$5^5 = 5^4 \cdot 5 \equiv 4 \cdot 5 \bmod 23 \equiv 20 \bmod 23$, NOTE $-3 \equiv 20 \bmod 23$

NEXT PAGE

$5^{10} = 5^5 \cdot 5^5 \equiv (-3)(-3) \bmod 23 \equiv 9 \bmod 23$

$5^{11} = 5^{10} \cdot 5^1 \equiv 9 \cdot 5 \bmod 23 = 45 \bmod 23 = 22 \bmod 23.$

NOTE $-1 \equiv 22 \bmod 23.$

BY LITTLE FERMAT, $5^{22} \equiv 1 \bmod 23$

SO $5^1, 5^2, 5^3, 5^4 \ldots \pmod{23}$ HAS PATTER LENGTH 1, 2, 11, OR 22 (DIVISORS OF 22).

SINCE $5^1 \not\equiv 1 \bmod 23$, $5^2 \not\equiv 1 \bmod 23$, $5^{11} \not\equiv 1 \bmod 23$,

$5^1, 5^2, 5^3, 5^4 \ldots \pmod{23}$ HAS PATTERN LENGTH 22,

WHICH MEANS THAT EVERY NUMBER BETWEEN 1 AND 22 WILL SHOW UP EXACTLY ONCE IN THE FIRST 22 ENTRIES OF ~~[illegible]~~

$5^1 \bmod 23, \; 5^2 \bmod 23, \; 5^3 \bmod 23, \ldots\ldots$

NOTE $-20 \equiv 3 \bmod 23$

AND THAT $5^{16} = 5^5 \cdot 5^{11} \equiv 20(-1) \bmod 23$

$\equiv -20 \bmod 23$

$\equiv 3 \bmod 23.$

SO $\boxed{n = 16}$ WORKS. NO n LESS THAN 16 WORKS BY THE OBSERVATION ABOUT THE PATTERN.

4: NEED TO COMPUTE $3^{11} \bmod 127$ AND $3^{14} \bmod 127$.

$3^1 \equiv 3 \bmod 127$ $3^2 \equiv 9 \bmod 127$ $3^3 \equiv 27 \bmod 127$ $3^4 \equiv 81 \bmod 127$

$3^5 = 243 = 254 - 11 = 127 \cdot 2 - 11 \equiv -11 \bmod 127$

SO $3^{10} = (3^5)^2 \equiv (-11)^2 \bmod 127 \equiv 121 \bmod 127$

$\equiv -6 \bmod 127$

$\boxed{3^{11} = 3^{10} \cdot 3 \equiv -6 \cdot 3 \bmod 127 \equiv -18 \bmod 127 \equiv 109 \bmod 127}$

$3^{15} = 3^5 \cdot 3^{10} \equiv (-11)(-6) \bmod 127 \equiv 66 \bmod 127.$

WERE LUCKY THAT 66 IS DIVISIBLE BY 3. (THIS TECHNIQUE DOES NOT ALWAYS WORK) (OR TO BE MORE PRECISE, THIS TECHNIQUE IS NOT ALWAYS SO SIMPLE)

SO $\boxed{3^{14} \equiv 22 \bmod 127}$

SINCE $(g^a)^b = g^{a \cdot b} = g^{b \cdot a} = (g^b)^a$ $(g^a)^b \bmod m = (g^b)^a \bmod m$

IN THIS SPECIFIC CASE, WE NEED TO COMPUTE $(3^{11})^{14} \bmod 127$. NOTE $14(11) = 14(10+1)$

$= 140 + 14 = 154$

SO $(3^{11})^{14} = 3^{154}$.

$154 = 126 + 28$. BY LITTLE FERMAT $3^{126} \equiv 1 \bmod 127$.

SO $(3^{11})^{14} = 3^{154} = 3^{126} 3^{28} \equiv 1 \cdot 3^{28} \bmod 127$

THE FIRST FOUR MULTIPLES OF 127 ARE 127, 254, 381 AND 508

$3^{28} = (3^{14})^2 \equiv 22^2 \bmod 127$.

$$\begin{array}{r} 22 \\ \times\ 22 \\ \hline 44 \\ 440 \\ \hline 484 \end{array}$$

$484 = 508 - 24$

SO $(3^{11})^{14} = (3^{14})^4 = 3^{154} = 3^{126} 3^{28} \equiv 3^{28} \bmod 127$

$\equiv (3^{14})^2 \bmod 127$

$\equiv 22^2 \bmod 127 \equiv -24 \bmod 127 \equiv \boxed{103 \bmod 127}$

5: IF THE PATTERN IS NOT VERY LONG, THE CODE IS EASY TO CRACK BY SIMPLY COMPUTING THE FIRST FEW ENTRIES OF THE SEQUENCE BY HAND.

6: ASKING FOR THE LAST TWO DIGITS IS THE SAME AS ASKING FOR THE REDUCTION mod 100.

REDUCING ~~MOD~~ mod 100 IS NOT SO TERRIBLE:

$31^1 \equiv 31 \bmod 100$

$31^2 = (30+1)(30+1) = 900+30+30+1 \equiv 0+30+30+1 \bmod 100$

$\equiv 61 \bmod 100$

$31^3 = 31^2 \cdot 31 \equiv 61 \cdot 31 \bmod 100$

$\equiv (60+1)(30+1) \bmod 100 \equiv 180+60+30+1 \bmod 100$

$\equiv 0+60+30+1 \bmod 100$

$\equiv 91 \bmod 100$

$31^4 = 31^3 \cdot 31 \equiv 91 \cdot 31 \bmod 100$

$\equiv (90+1)(30+1) \bmod 100$

$\equiv 2700 + 90 + 30 + 1 \bmod 100$

$\equiv 121 \bmod 100$

$\equiv 21 \bmod 100$

$31^5 \equiv 31^4 \cdot 31 \equiv (21)(31) \bmod 100$

$\equiv (20+1)(30+1) \bmod 100$

$\equiv 600 + 20 + 30 + 1 \bmod 100$

$\equiv 51 \bmod 100$

So $31^{10} \bmod 100 \equiv (31^5)^2 \bmod 100$

$\equiv (51)(51) \bmod 100$

$\equiv (50+1)(50+1) \bmod 100$

$\equiv 2500 + 50 + 50 + 1 \bmod 100$

$\equiv 1 \bmod 100$

So $31^{1000} = (31^{10})^{100} \equiv 1^{100} \bmod 100 \equiv 1 \bmod 100$

SO THE LAST TWO DIGITS ARE 01.