

Project 1 - part 2

$$\begin{aligned} 1a) \quad 15 \cdot 29 \bmod 13 &= (15 \bmod 13) (29 \bmod 13) \bmod 13 \\ &= (2) (3) \bmod 13 \\ &= 6. \end{aligned}$$

$$\begin{aligned} 1b) \quad 2 \cdot 29 \bmod 13 &= (2) (3) \bmod 13 \\ &= 6. \end{aligned}$$

$$\begin{aligned} 1c) \quad 2 \cdot (-3) \bmod 13 &= -6 \bmod 13 \\ &\equiv 7, \text{ move within the same equivalence} \\ &\text{class by adding 13 to } (-6). \end{aligned}$$

$$\begin{aligned} 1d) \quad (-11) \cdot 3 \bmod 13 &= (-11 \bmod 13) (3 \bmod 13) \bmod 13 \\ &= (2) (3) \bmod 13 \\ &= 6. \end{aligned}$$

We computed with the same technique from 1c)

$$-11 \bmod 13 \equiv 2, \text{ by adding 13}$$

$$2a) \quad \frac{1}{5} \bmod 13 = x$$

$$= 5x$$

Can we find an  $x$  such that  $1 \bmod 13 \equiv 5x$ ?

From just thinking about the multiples of 5, we

realize that 40 would do the trick. So we

let  $x = 8$

$$\text{So, } \frac{1}{5} \bmod 13 = 8.$$

$$2b) \quad \frac{1}{5} \bmod 7 = x$$

$$= 5x$$

Using the same thinking as above, we

find that 15 would fit the bill, so we

let  $x = 3$

$$\text{So, } \frac{1}{5} \bmod 7 = 3.$$

$$2c) \quad 3 \cdot \frac{2}{5} \bmod 7 = \overset{(3)}{\cancel{(3 \bmod 7)}} \overset{(2)}{\cancel{(\frac{1}{5} \bmod 7)}} (\frac{1}{5} \bmod 7) \bmod 7$$

$$= \overset{2}{(3)} \overset{2}{\cancel{(3)}} \overset{(3)}{(3)} \bmod 7$$

$$= 18 \bmod 7$$

$$= 4.$$

$$3a) \quad 5x = 4 \pmod{3}$$

We can shift into

$$5x = 1 \pmod{3}$$

and here, we can see that 10 is a multiple of 5 which would give a remainder of 1 when divided by 3. So we solve with  $\boxed{x = 2}$

$$3b) \quad 7x = 6 \pmod{5}$$

again, moving within the equivalence class:

$$7x = 1 \pmod{5}$$

We note that 21 is a multiple of 7 that gives a remainder of 1 when divided by 5, so  $\boxed{x = 3}$

$$3c) \quad 9x = 8 \pmod{7}$$

using the same approach:

$$9x = 1 \pmod{7}$$

36 is a multiple of 9 that gives a remainder of 1 when divided by 7, so  $\boxed{x = 4}$

$$\begin{aligned}
 4a) \quad 3^2 \bmod 13 &= (3 \bmod 13)(3 \bmod 13) \bmod 13 \\
 &= (3)(3) \bmod 13 \\
 &= 9 \bmod 13 \\
 &= 9
 \end{aligned}$$

$$\begin{aligned}
 4b) \quad 7^2 \bmod 13 &= (7 \bmod 13)(7 \bmod 13) \bmod 13 \\
 &= 49 \bmod 13 \\
 &= 10
 \end{aligned}$$

4c) Let's compute a few exponents first:

$$3^2 \bmod 13 = 9 \quad (\text{from 4a})$$

$$\begin{aligned}
 3^4 \bmod 13 &= (3^2 \bmod 13)(3^2 \bmod 13) \bmod 13 \\
 &= (9)(9) \bmod 13 \\
 &= 81 \bmod 13 \\
 &= 3
 \end{aligned}$$

$$\begin{aligned}
 3^8 \bmod 13 &= (3^4 \bmod 13)(3^4 \bmod 13) \bmod 13 \\
 &= (3)(3) \bmod 13 \\
 &= 9
 \end{aligned}$$

$$\begin{aligned}
 \text{So, } 3^{10} \bmod 13 &= (3^2 \bmod 13)(3^8 \bmod 13) \bmod 13 \\
 &= (9)(9) \bmod 13 \\
 &= 3
 \end{aligned}$$

4d) We compute some exponents, like before:

pg. 5

$$\begin{aligned} 7^2 \bmod 13 &= (7 \bmod 13)(7 \bmod 13) \bmod 13 \\ &= 49 \bmod 13 \\ &= 10 \end{aligned}$$

$$\begin{aligned} 7^4 \bmod 13 &= (7^2 \bmod 13)(7^2 \bmod 13) \bmod 13 \\ &= (10)(10) \bmod 13 \\ &= 9 \end{aligned}$$

$$\begin{aligned} 7^8 \bmod 13 &= (7^4 \bmod 13)(7^4 \bmod 13) \bmod 13 \\ &= (9)(9) \bmod 13 \\ &= 3 \end{aligned}$$

$$\begin{aligned} 7^{16} \bmod 13 &= (7^8 \bmod 13)(7^8 \bmod 13) \bmod 13 \\ &= (3)(3) \bmod 13 \\ &= 9 \end{aligned}$$

$$\begin{aligned} 7^{32} \bmod 13 &= (7^{16} \bmod 13)(7^{16} \bmod 13) \bmod 13 \\ &= (9)(9) \bmod 13 \\ &= 3 \end{aligned}$$

$$\begin{aligned} 7^{64} \bmod 13 &= (7^{32} \bmod 13)(7^{32} \bmod 13) \bmod 13 \\ &= (3)(3) \bmod 13 \\ &= 9 \end{aligned}$$

$$\begin{aligned} 7^{100} \bmod 13 &= (7^4 \bmod 13)(7^{32} \bmod 13)(7^{64} \bmod 13) \bmod 13 \\ &= (9)(3)(9) \bmod 13 \\ &= \boxed{9} \end{aligned}$$

4e1 In the prior problem, I noticed even exponents of  $7 \pmod{13}$  were alternating between 3 and 9, so I figured an odd exponent would be the key to finding  $x$ .

pg. 6

$x = 1$  and  $x = 3$  were not it:

$$7^1 \pmod{13} = 7$$

$$7^3 \pmod{13} = 5$$

$$\begin{aligned} 7^5 \pmod{13} &= (7^4 \pmod{13}) (7 \pmod{13}) \pmod{13} \\ &= (9) (7) \pmod{13} \\ &= 63 \pmod{13} \\ &= 11 \end{aligned}$$

So,  $\boxed{x = 5}$  works out.