

Homework 10

CMPSC 360

Kinner Parikh

April 10, 2022

Question 1: Solve the congruence $8x \equiv 13 \pmod{29}$

Finding c^{-1} :

$$29 = 8 \cdot 3 + 5$$

$$8 = 5 \cdot 1 + 3$$

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2$$

$$1 = 3 - 2 \cdot 1$$

$$= 3 - (5 - 3)$$

$$= -5 + 3 \cdot 2$$

$$= -5 + (8 - 5) \cdot 2$$

$$= 8 \cdot 2 - 5 \cdot 3$$

$$= 8 \cdot 2 - (29 - 8 \cdot 3) \cdot 3$$

$$= 29 \cdot (-3) + 8 \cdot 11$$

So, $c^{-1} = 11$

Multiplying both sides of congruence by c^{-1} :

$$8 \cdot 11x \equiv 13 \cdot 11 \pmod{29}$$

$$x \equiv 143 \pmod{29} \quad [\text{since } 8 \cdot 11 \pmod{29} = 1]$$

$$x \equiv 143 \equiv 27 \pmod{29} \quad [\text{since } 143 \pmod{29} = 27]$$

So a possible value for x is 27.

Question 2: Solve the congruence $55x = 34 \pmod{89}$ and find all possible values of x

Finding the inverse $55 \pmod{89}$:

$$89 = 55 \cdot 1 + 34$$

$$55 = 34 \cdot 1 + 21$$

$$34 = 21 \cdot 1 + 13$$

$$21 = 13 \cdot 1 + 8$$

$$13 = 8 \cdot 1 + 5$$

$$8 = 5 \cdot 1 + 3$$

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2$$

$$1 = 3 - 2$$

$$= 3 - (5 - 3)$$

$$= -5 + 3 \cdot 2$$

$$= -5 + (8 - 5) \cdot 2$$

$$= 8 \cdot 2 + 5 \cdot (-3)$$

$$= 8 \cdot 2 + (13 - 8) \cdot (-3)$$

$$= 13 \cdot (-3) + 8 \cdot 5$$

$$= 13 \cdot (-3) + (21 - 13) \cdot 5$$

$$= 21 \cdot 5 + 13 \cdot (-8)$$

$$= 21 \cdot 5 + (34 - 21) \cdot (-8)$$

$$= 34 \cdot (-8) + 21 \cdot 13$$

$$= 34 \cdot (-8) + (55 - 34) \cdot 13$$

$$= 55 \cdot 13 + 34 \cdot (-21)$$

$$= 55 \cdot 13 + (89 - 55) \cdot (-21)$$

$$= 89 \cdot (-21) + 55 \cdot 34$$

So $c^{-1} = 34$ Multiplying both sides of congruence by c^{-1} :

$$55 \cdot 34x \equiv 34 \cdot 34 \pmod{89}$$

$$x \equiv 1156 \pmod{89} \quad [\text{since } 55 \cdot 34 \pmod{89} = 1]$$

$$x \equiv 1156 \equiv 88 \pmod{89} \quad [\text{since } 1156 \pmod{89} = 88]$$

So, $x = 88 + 89k$ where $k \in \mathbb{Z}$ satisfies the congruence form: $55x = 34 \pmod{89}$

Question 3:

$$\begin{aligned}z_2 &= 105/7 = 15 \\y_2 \cdot 15 &= 1 \pmod{7} \rightarrow y_2 = 1 \\(7 \cdot 11 \cdot 7) &+ (4 \cdot 10 \cdot 15) + (6 \cdot 9 \cdot 9) = 1625 \\x &= 1625 \pmod{105} = 50\end{aligned}$$

Question 4: Using Fermat's Little Theorem find $3^{2003} \pmod{455}$

Question 5:

TIME FOR FUN

Question 6: We chose two prime numbers $p = 17$, $q = 11$, and $e = 7$. Calculate d and show the public and private keys.

$$\begin{aligned}n &= pq = 17 \cdot 11 = 187 \\k &= (p-1)(q-1) = 16 \cdot 10 = 160 \\de &\equiv 1 \pmod{160}, \text{ so } d \cdot 7 \equiv 1 \pmod{160}\end{aligned}$$

$$160 = 7 \cdot 22 + 6$$

$$7 = 6 \cdot 1 + 1$$

$$6 = 1 \cdot 6$$

$$1 = 7 - 6$$

$$= 7 - (160 - 7 \cdot 22)$$

$$= -160 + 7 \cdot 23$$

So, we know that $d = 23$

The public key is: $(187, 7)$

The private key is: $(187, 23)$

Question 7: Given $p = 37$ and $q = 43$, can we choose $d = 71$? If yes, justify your answer, otherwise suggest one value for d . Then compute the public and the private keys.

$$n = pq = 37 \cdot 43 = 1591$$

$$k = (p - 1)(q - 1) = 36 \cdot 42 = 1512$$

Finding the inverse of 71 mod 1512:

$$1512 = 71 \cdot 21 + 21$$

$$71 = 21 \cdot 3 + 8$$

$$21 = 8 \cdot 2 + 5$$

$$8 = 5 \cdot 1 + 3$$

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2$$

$$1 = 3 - 2$$

$$= 3 - (5 - 3)$$

$$= -5 + 3 \cdot 2$$

$$= -5 + (8 - 5) \cdot 2$$

$$= 8 \cdot 2 + 5 \cdot (-3)$$

$$= 8 \cdot 2 + (21 - 8 \cdot 2) \cdot (-3)$$

$$= 21 \cdot (-3) + 8 \cdot 8$$

$$= 21 \cdot (-3) + (71 - 21 \cdot 3) \cdot 8$$

$$= 71 \cdot 8 + 21 \cdot (-27)$$

$$= 71 \cdot 8 + (1512 - 71 \cdot 21) \cdot (-27)$$

$$= 1512 \cdot (-27) + 71 \cdot 575$$

The inverse of 71 mod 1512 is 575. So $e = 575$

We must calculate $\gcd(575, 1512)$

$$1512 = 575 \cdot 2 + 362$$

$$575 = 362 \cdot 1 + 213$$

$$362 = 213 \cdot 1 + 149$$

$$213 = 149 \cdot 1 + 64$$

$$149 = 64 \cdot 2 + 21$$

$$64 = 21 \cdot 3 + 1$$

$$21 = 1 \cdot 21$$

So $\gcd(575, 1512) = 1$, which means we can choose $d = 71$

Public key: (1591, 575)

Private key: (1591, 71)

Question 8:

$$2x \equiv 5 \pmod{7}$$

Applying the backwards pass of Euclid division, we know that 2 inverse of mod 7 is 4.

Multiplying both sides of congruence:

$$2(4)x \equiv 5(4) \pmod{7}$$

$$x \equiv 20 \pmod{7}; \text{ Since } 2 \cdot 4 \equiv 1 \pmod{7}$$

$$\text{So, } x \equiv 6 \pmod{7}$$

$$4x \equiv 2 \pmod{6}$$

Dividing congruence by 2, we get $2x \equiv 1 \pmod{3}$

Applying the backwards pass of Euclid division, we know that 2 inverse of mod 3 is 2.

$$2(2)x \equiv 1(2) \pmod{3}$$

$$x \equiv 2 \pmod{3}; \text{ Since } 2 \cdot 2 \equiv 1 \pmod{3}$$

$$\text{So, } x \equiv 2 \pmod{3}$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 6 \pmod{7}$$

Applying the Chinese Remainder Theorem:

$$a_1 = 2, a_2 = 3, a_3 = 6 \text{ and } m_1 = 3, m_2 = 5, m_3 = 7$$

$$\text{So, } M = 3 \cdot 5 \cdot 7 = 105$$

$$\text{Thus, } z_1 = 35, z_2 = 21, z_3 = 15$$

$$y_1 \cdot 35 \equiv 1 \pmod{3}; \text{ so } y_1 = 2$$

$$y_2 \cdot 21 \equiv 1 \pmod{5}; \text{ so } y_2 = 1$$

$$y_3 \cdot 15 \equiv 1 \pmod{7}; \text{ so } y_3 = 1$$

$$\text{We get } x = (2 \cdot 35 \cdot 2) + (3 \cdot 21 \cdot 1) + (6 \cdot 15 \cdot 1) = 293$$

$$\text{And } 293 \pmod{105} = 83$$

Thus, the lowest possible simultaneous solution is $x = 83$