# Homework 10

## CMPSC 360

Kinner Parikh

April 10, 2022

**Question 1**: Solve the congruence $8x \equiv 13 \bmod 29$

Finding $c^{-1}$ :

$$\begin{aligned}
29 &= 8 \cdot 3 + 5 \\
8 &= 5 \cdot 1 + 3 \\
5 &= 3 \cdot 1 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 1 \cdot 2
\end{aligned}$$

$$\begin{aligned}
1 &= 3 - 2 \cdot 1 \\
&= 3 - (5 - 3) \\
&= -5 + 3 \cdot 2 \\
&= -5 + (8 - 5) \cdot 2 \\
&= 8 \cdot 2 - 5 \cdot 3 \\
&= 8 \cdot 2 - (29 - 8 \cdot 3) \cdot 3 \\
&= 29 \cdot (-3) + 8 \cdot 11
\end{aligned}$$

So, $c^{-1} = 11$
Multiplying both sides of congruence by $c^{-1}$:

$$\begin{aligned}
8 \cdot 11x &\equiv 13 \cdot 11 \bmod 29 \\
x &\equiv 143 \bmod 29 && [\text{since } 8 \cdot 11 \bmod 29 = 1] \\
x &\equiv 143 \equiv 27 \bmod 29 && [\text{since } 143 \bmod 29 = 27]
\end{aligned}$$

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 mod 89:

$$
\begin{aligned}
89 &= 55 \cdot 1 + 34 \\
55 &= 34 \cdot 1 + 21 \\
34 &= 21 \cdot 1 + 13 \\
21 &= 13 \cdot 1 + 8 \\
13 &= 8 \cdot 1 + 5 \\
8 &= 5 \cdot 1 + 3 \\
5 &= 3 \cdot 1 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 1 \cdot 2
\end{aligned}
$$

$$
\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) \\
&= -5 + 3 \cdot 2 \\
&= -5 + (8 - 5) \cdot 2 \\
&= 8 \cdot 2 + 5 \cdot (-3) \\
&= 8 \cdot 2 + (13 - 8) \cdot (-3) \\
&= 13 \cdot (-3) + 8 \cdot 5 \\
&= 13 \cdot (-3) + (21 - 13) \cdot 5 \\
&= 21 \cdot 5 + 13 \cdot (-8) \\
&= 21 \cdot 5 + (34 - 21) \cdot (-8) \\
&= 34 \cdot (-8) + 21 \cdot 13 \\
&= 34 \cdot (-8) + (55 - 34) \cdot 13 \\
&= 55 \cdot 13 + 34 \cdot (-21) \\
&= 55 \cdot 13 + (89 - 55) \cdot (-21) \\
&= 89 \cdot (-21) + 55 \cdot 34
\end{aligned}
$$

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

$$
\begin{aligned}
55 \cdot 34x &\equiv 34 \cdot 34 \bmod 89 \\
x &\equiv 1156 \bmod 89 & [\text{since } 55 \cdot 34 \bmod 29 = 1] \\
x &\equiv 1156 \equiv 88 \bmod 89 & [\text{since } 143 \bmod 29 = 27]
\end{aligned}
$$

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

**Question 3**:

$z_2 = 105/7 = 15$
$y_2 \cdot 15 = 1 \text{ mod } 7 \rightarrow y_2 = 1$
$(7 \cdot 11 \cdot 7) + (4 \cdot 10 \cdot 15) + (6 \cdot 9 \cdot 9) = 1625$
$x = 1625 \text{ mod } 105 = 50$

**Question 4**: Using Fermat's Little Theorem find $3^{2003}$ mod 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.

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

$$\begin{aligned} 160 &= 7 \cdot 22 + 6 \\ 7 &= 6 \cdot 1 + 1 \\ 6 &= 1 \cdot 6 \end{aligned}$$

$$\begin{aligned} 1 &= 7 - 6 \\ &= 7 - (160 - 7 \cdot 22) \\ &= -160 + 7 \cdot 23 \end{aligned}$$

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:

$$\begin{aligned}
1512 &= 71 \cdot 21 + 21 \\
71 &= 21 \cdot 3 + 8 \\
21 &= 8 \cdot 2 + 5 \\
8 &= 5 \cdot 1 + 3 \\
5 &= 3 \cdot 1 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 1 \cdot 2
\end{aligned}$$

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) \\
&= -5 + 3 \cdot 2 \\
&= -5 + (8 - 5) \cdot 2 \\
&= 8 \cdot 2 + 5 \cdot (-3) \\
&= 8 \cdot 2 + (21 - 8 \cdot 2) \cdot (-3) \\
&= 21 \cdot (-3) + 8 \cdot 8 \\
&= 21 \cdot (-3) + (71 - 21 \cdot 3) \cdot 8 \\
&= 71 \cdot 8 + 21 \cdot (-27) \\
&= 71 \cdot 8 + (1512 - 71 \cdot 21) \cdot (-27) \\
&= 1512 \cdot (-27) + 71 \cdot 575
\end{aligned}$$

The inverse of 71 mod 1512 is 575. So $e = 575$
We must calculate gcd(575, 1512)

$$\begin{aligned}
1512 &= 575 \cdot 2 + 362 \\
575 &= 362 \cdot 1 + 213 \\
362 &= 213 \cdot 1 + 149 \\
213 &= 149 \cdot 1 + 64 \\
149 &= 64 \cdot 2 + 21 \\
64 &= 21 \cdot 3 + 1 \\
21 &= 1 \cdot 21
\end{aligned}$$

So gcd(575, 1512) $= 1$, which means we can choose $d = 71$
Public key: (1591, 575)
Private key: (1591, 71)

**Question 8**:

$2x \equiv 5 (\text{mod } 7)$
$4x \equiv 2 (\text{mod } 6)$
$x \equiv 3 (\text{mod } 5)$