Homework 10

CMPSC 360

Kinner Parikh

April 14, 2022

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

Finding c^{-1} :

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

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

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

So a possible value for x is 27.

Question 2: Solve the congruence $55x = 34$ (mod 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}:

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

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

The prime factorization of 455 is 5, 7, 13
Part 1: 3^{2003} mod 5
We know that $3^4 \equiv 1 \text{ mod } 5$
$2003 = 4 \cdot 500 + 3$
$3^{2003} \text{ mod } 5 = 3^{4 \cdot 500} \cdot 3^3 \text{ mod } 5$
$1 \cdot 3^3 \text{ mod } 5 = 27 \text{ mod } 5 = 2 \text{ mod } 5$
Part 2: 3^{2003} mod 7
We know that $3^6 \equiv 1 \text{ mod } 7$
$2003 = 333 \cdot 6 + 5$
$3^{2003} \text{ mod } 7 = 3^{6 \cdot 333} \cdot 3^5 \text{ mod } 7$
$1 \cdot 3^5 \text{ mod } 7 = 243 \text{ mod } 7 = 5 \text{ mod } 7$
Part 3: 3^{2003} mod 13
We know that $3^3 \equiv 1 \text{ mod } 13$
$2003 = 667 \cdot 3 + 2$
$3^{2003} \text{ mod } 7 = 3^{3 \cdot 667} \cdot 3^2 \text{ mod } 13$
$1 \cdot 3^2 \text{ mod } 13 = 9 \text{ mod } 13$

$x = 2 \text{ mod } 5$
$x = 5 \text{ mod } 7$
$x = 9 \text{ mod } 13$
Applying the Chinese Remainder Theorem:
$a_1 = 2, a_2 = 5, a_3 = 9$ and $m_1 = 5, m_2 = 7, m_3 = 13$
So, $M = 5 \cdot 7 \cdot 13 = 455$
Thus, $z_1 = 91, z_2 = 65, z_3 = 35$
$y_1 \cdot 91 = 1 \text{ mod } 5$; so $y_1 = 1$
$y_2 \cdot 65 = 1 \text{ mod } 7$; so $y_2 = 4$
$y_3 \cdot 35 = 1 \text{ mod } 13$; so $y_3 = 3$
We get $x = (2 \cdot 91 \cdot 1) + (5 \cdot 65 \cdot 4) + (9 \cdot 35 \cdot 3) = 2427$
And 2427 mod 455 = 152
Thus, 3^{2003} mod 455 = 152

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:

$2x \equiv 5(\text{mod } 7)$
Applying the backwards pass of Euclid division, we know that 2 inverse of mod 7 is 4.
Multiplying both sides of congruence:
$2(4)x \equiv 5(4)(\text{mod } 7)$
$x \equiv 20(\text{mod } 7)$; Since $2 \cdot 4 \equiv 1(\text{mod } 7)$
So, $x \equiv 6(\text{mod } 7)$

$4x \equiv 2(\text{mod } 6)$
Dividing congruence by 2, we get $2x \equiv 1(\text{mod } 3)$
Applying the backwards pass of Euclid division, we know that 2 inverse of mod 3 is 2.
$2(2)x \equiv 1(2)(\text{mod } 3)$
$x \equiv 2(\text{mod } 3)$; Since $2 \cdot 2 \equiv 1(\text{mod } 3)$
So, $x \equiv 2(\text{mod } 3)$

$x \equiv 2(\text{mod } 3)$
$x \equiv 3(\text{mod } 5)$
$x \equiv 6(\text{mod } 7)$
Applying the Chinese Remainder Theorem:
$a_1 = 2, a_2 = 3, a_3 = 6$ and $m_1 = 3, m_2 = 5, m_3 = 7$
So, $M = 3 \cdot 5 \cdot 7 = 105$
Thus, $z_1 = 35, z_2 = 21, z_3 = 15$
$y_1 \cdot 35 = 1 \text{ mod } 3$; so $y_1 = 2$
$y_2 \cdot 21 = 1 \text{ mod } 5$; so $y_2 = 1$
$y_3 \cdot 15 = 1 \text{ mod } 7$; so $y_3 = 1$
We get $x = (2 \cdot 35 \cdot 2) + (3 \cdot 21 \cdot 1) + (6 \cdot 15 \cdot 1) = 293$
And 293 mod 105 = 83
Thus, the lowest possible simultaneous solution is $x = 83$

Question 9a:

Proof:
We have to find that for every polynomial of degree n with integer coefficients $f(x)$,
we have $f(b_1) \equiv f(b_2) \bmod p$.
We must prove that for every term like $a_k x^k$ in the polynomial $f(x)$ this property holds
Assume $b_1 \equiv b_2 \bmod p$ such that $b_1, b_2, p \in \mathbb{Z}$
This means that, from the definition of congruence modulo, $p \mid (b_1 - b_2)$

Case 1: $b_1 + c \equiv b_2 + c \bmod p$ for arbitrary integer c
From the definition of congruence modulo, $p \mid [b_1 + c - (b_2 + c)] = p \mid (b_1 - b_2)$
So taking the reverse of the definition of congruence modulo, we get $b_1 \equiv b_2 \bmod p$
Thus, $b_1 \equiv b_2 \bmod p \Rightarrow b_1 + c \equiv b_2 + c \bmod p$ for arbitrary integer c

Case 2: $c \cdot b_1 \equiv c \cdot b_2 \bmod p$ for arbitrary integer c
From the definition of congruence modulo, $p \mid (c \cdot b_1 - c \cdot b_2) = p \mid c \cdot (b_1 - b_2)$
We know that as a property of division, if $a \mid b$, then $a \mid bt$. Similarly, we already know that $p \mid (b_1 - b_2)$, so we can say that $p \mid c \cdot (b_1 - b_2)$
Thus, we know that $p \mid c \cdot (b_1 - b_2) = p \mid (b_1 - b_2)$
So taking the reverse of the definition of congruence modulo, we get $b_1 \equiv b_2 \bmod p$
Thus, $b_1 \equiv b_2 \bmod p \Rightarrow c \cdot b_1 \equiv c \cdot b_2 \bmod p$ for arbitrary integer c

Case 3: ${b_1}^k \equiv {b_2}^k \bmod p$ for a positive integer k.
From the definition of congruence modulo, $p \mid ({b_1}^k - {b_2}^k)$
We proceed by induction on k

Base Case: $(k = 1)$
So $p \mid (b_1 - b_2)$, which we already know is true.
The base case is proven

Inductive Hypothesis: $(k = n)$
For an arbitrary positive integer n, assume that $p \mid ({b_1}^n - {b_2}^n)$
From definition of divides, we get ${b_1}^n - {b_2}^n = p \cdot t$ where $t \in \mathbb{Z}$

Inductive Step: $(k = n + 1)$
We have to show that $p \mid ({b_1}^{n+1} - {b_2}^{n+1})$
Expanding the expressions, we get: ${b_1}^{n+1} - {b_2}^{n+1} = b_1 \cdot {b_1}^n - b_2 \cdot {b_2}^n$

Question 9b: