W202 - Homework 2

Problem 1a: Alice's favorite number is 5. She sends (5, S). What is S?

- $d = 7$ (Alice's private key)
- $e = 3$ (Alice's public key)
- $N = 33$
- $D = 5$ (Alice's favorite number)

} know variables

Solution: Alice uses the RSA signing algorithm to sign her favorite number.

↳ $\underbrace{S}_{\text{signature}} = \underbrace{D}_{\text{favorite \#}}^{\overbrace{d}^{\text{private key}}} \bmod \underbrace{N}_{p \cdot q}$ } RSA signing algorithm

↳ $S = 5^7 \bmod 33$
$S = 78{,}125 \bmod 33$
$\underline{\underline{S = 14}}$

} used SageMath for calculation

Answer: S is 14. Alice signs her favorite number using her private key "d", and sends (5, 14) to Bob.

Problem 1b: Verify (5, S) came from Alice.

- $d = 7$ (Alice's private key)
- $e = 3$ (Alice's public key)
- $N = 33$
- $S = 14$ (Alice's signature - problem 1a)
- $D = 5$ (Alice's favorite # - message)

known variables

Solution: Bob uses RSA verification algorithm to verify Alice's signature (5, 14).

↳ $D = S^e \bmod N$

D → favorite #; S → digital signature; e → public key; N → $p \cdot q$

RSA verification algorithm

↳ $D = 14^3 \bmod 33$

$D = 2733 \bmod 33$

$\underline{\underline{D = 5}}$

Used Sage Math for calculation

Answer: Using the RSA verification algorithm, Bob is able to verify Alice's signature (5, 14) because he is able to recover Alice's favorite number using Alice's public key.

Problem 1c :

Referring to properties of the RSA equation for digital signatures :

$$- \; S = D^{d} \bmod N$$

$$- \; D = S^{e} \bmod N$$

we know that a unique "e" and "d" (public and private key pair) are generated for Alice, and values "e" and "d" are modular inverses of each other. This means a document signed with Alice's private key (producing a digital signature) can be verified by anybody with Alice's public key. As only Alice knows her private key (an nobody else), we are guaranteed that only Alice could have sent message (5,14) because we can use Alice's digital signature and public key to recover her favorite number 5.

Problem 2a : Describe the homomorphic property.

Homomorphism, in plain english, is a preserved mathematical relationship when an original element "M" is transformed to a new element "C". Changes to "C" follow the same mathematical relationship that transformed "M" to "C".

As an example, the retail price of a burger is double the wholesale cost. Given this mathematical relationship, if we change the retail price of the burger, we know the wholesale price has also changed in accordance with the 2x relationship between wholesale and retail pricing.

Problem 2b: Explain how padding helps avoid homomorphism problem.

The traditional RSA algorithm (without padding) carries a homomorphic property that preserves a mathematical relationship between the message and ciphertext. By adding a padding scheme to the message, then encrypting the padded message with the RSA algorithm, the homomorphic property is removed because the ciphertext no longer has a direct mathematical relationship with the original message. The ciphertext must first be decrypted, then the padding scheme must also be applied in order to recover the original message.

As seen from the equations:

↳ $E(m) \cdot E(m') \bmod N \equiv E(mm') \bmod N$

(RSA algorithm without padding is homomorphic)

↳ $E(m+\varepsilon) \cdot E(m'+\varepsilon) \bmod N \not\equiv \left[(m+\varepsilon)(m'+\varepsilon)\right]^{e} \bmod N$

(RSA algorithm with padding removes homomorphic property under multiplication)

Problem 3a : Minimum number of equations to reveal secret?

- Organization : 10
- Quorum : 4
- Mod : 17
- $f(1) = 0$, $f(5) = 5$
  $f(6) = 5$, $f(8) = 10$
  $f(10) = 6$

} known variables

Solution : Refer to properties of Shamir's Secret Sharing to determine minimum number of equations to derive secret.

Answer : A minimum (or threshold) of 4 equations are required to reveal secret. Shamir's Secret Sharing leverages a set of linear equations, where a minimum number of solutions to the equations are required to derive a secret. As the question states a quorum of 4 people are required, we know the minimum number of shares required is 4 people / equations.

Problem 3b: Write system of linear equations, when solved, will recover secret.

- Organization : 10
- Quorum : 4
- Mod : 17
- $f(1) = 0$, $f(5) = 5$
  $f(6) = 5$, $f(8) = 10$
  $f(10) = 6$

} known variables

Solution: Construct 4 polynomial equations of structure $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_{q-1} x^{q-1}$ where q = quorom and $x = f(x)$.

$\hookrightarrow f(1) = 0 = a_0 + a_1(1) + a_2(1)^2 + a_3(1)^3$
$0 = a_0 + a_1 + a_2 + a_3 \pmod{17}$

$\hookrightarrow f(5) = 5 = a_0 + a_1(5) + a_2(5)^2 + a_3(5)^3$
$5 = a_0 + 5a_1 + 25a_2 + 125a_3 \pmod{17}$

$\hookrightarrow f(6) = 5 = a_0 + a_1(6) + a_2(6)^2 + a_3(6)^3$
$5 = a_0 + 6a_1 + 36a_2 + 216a_3 \pmod{17}$

$\hookrightarrow f(8) = 10 = a_0 + a_1(8) + a_2(8)^2 + a_3(8)^3$
$10 = a_0 + 8a_1 + 64a_2 + 512a_3 \pmod{17}$

(see next page)

Answer: The following 4 polynomial equations, when solved simultaneously, will reveal secret a_0:

$$0 = a_0 + a_1 + a_2 + a_3 \pmod{17}$$
$$5 = a_0 + 5a_1 + 25a_2 + 125a_3 \pmod{17}$$
$$5 = a_0 + 6a_1 + 36a_2 + 216a_3 \pmod{17}$$
$$10 = a_0 + 8a_1 + 64a_2 + 512a_3 \pmod{17}$$

Problem 4a: Write all integers (mod 15) in CRT notation.

Solution:

- $\hookrightarrow$ Prime factors of 15 $\rightarrow$ 3 and 5
- $\hookrightarrow$ Integers of mod 15 $\rightarrow$ 0, 1, 2 .. $\rightarrow$ .. 13, 14

Answer:

$$
\begin{aligned}
0 \bmod 15 &= \langle 0 \bmod 3,\ 0 \bmod 5 \rangle = \langle 0, 0 \rangle \\
1 \bmod 15 &= \langle 1 \bmod 3,\ 1 \bmod 5 \rangle = \langle 1, 1 \rangle \\
2 \bmod 15 &= \langle 2 \bmod 3,\ 2 \bmod 5 \rangle = \langle 2, 2 \rangle \\
3 \bmod 15 &= \langle 0 \bmod 3,\ 3 \bmod 5 \rangle = \langle 0, 3 \rangle \\
4 \bmod 15 &= \langle 1 \bmod 3,\ 4 \bmod 5 \rangle = \langle 1, 4 \rangle \\
5 \bmod 15 &= \langle 2 \bmod 3,\ 0 \bmod 5 \rangle = \langle 2, 0 \rangle \\
6 \bmod 15 &= \langle 0 \bmod 3,\ 1 \bmod 5 \rangle = \langle 0, 1 \rangle \\
7 \bmod 15 &= \langle 1 \bmod 3,\ 2 \bmod 5 \rangle = \langle 1, 2 \rangle \\
8 \bmod 15 &= \langle 2 \bmod 3,\ 3 \bmod 5 \rangle = \langle 2, 3 \rangle \\
9 \bmod 15 &= \langle 0 \bmod 3,\ 4 \bmod 5 \rangle = \langle 0, 4 \rangle \\
10 \bmod 15 &= \langle 1 \bmod 3,\ 0 \bmod 5 \rangle = \langle 1, 0 \rangle \\
11 \bmod 15 &= \langle 2 \bmod 3,\ 1 \bmod 5 \rangle = \langle 2, 1 \rangle \\
12 \bmod 15 &= \langle 0 \bmod 3,\ 2 \bmod 5 \rangle = \langle 0, 2 \rangle \\
13 \bmod 15 &= \langle 1 \bmod 3,\ 3 \bmod 5 \rangle = \langle 1, 3 \rangle \\
14 \bmod 15 &= \langle 2 \bmod 3,\ 4 \bmod 5 \rangle = \langle 2, 4 \rangle
\end{aligned}
$$

Problem 46 - 1 :

Equation : $4 + 7 \mod 15$

① Apply addition property :

↳ $4 \mod 15 + 7 \mod 15$

② Solve each term :

↳ $4 + 7 = 11$

$\boxed{\text{Answer : } 11 \pmod{15}}$

Problem 46 - 2 :

Equation : $8 - (3 \times 4) \mod 15$

① Apply subtraction and multiplication property :

↳ $8 \mod 15 - (3 \mod 15)(4 \mod 15)$

② Solve each term :

↳ $8 - (12 \mod 15)$

↳ $8 - 12 = -4$

③ Add answer by modulo (15) to get congruent value in range [0, 14] :

↳ $-4 + 15 = 11$

$\boxed{\text{Answer : } 11 \pmod{15}}$

Problem 4b-3:

Equation: $7^{-1} \bmod 15$

① Rewrite to solve via Extended Euclidean Algo:

↳ $7^{-1} \bmod 15$

↳ $7x \equiv 1 \bmod 15$

② Solve equation using Extended Euclidean Alg:

↳ $GCD(7, 15)$

↳ $7x + 15y = 1$

↳ $15 = 7(2) + \underline{(1)}$ → (confirming GCD = 1)

$7 = 1(7) + (0)$

↳ $1 = 15(1) + 7\underline{\underline{(-2)}}$ → $x = -2$

③ Add answer by modulo (15) to get congruent value in range [0, 14]:

↳ $-2 + 15 = \underline{\underline{13}}$

$$\boxed{\text{Answer: } 13 \pmod{15}}$$

Problem 4b - 4 :

Equation : $\dfrac{3^2+6}{7} \mod 15$

① Apply associative & multiplication property:

↳ $(3^2 \bmod 15) + (6 \bmod 15) \cdot 7^{-1} \bmod 15$

② Apply exponentiation property:

↳ $((3 \bmod 15)^2 \bmod 15 + (6 \bmod 15)) \cdot 7^{-1} \bmod 15$

③ Solve terms :

↳ $((9 \bmod 15) + (6 \bmod 15)) \cdot 7^{-1} \bmod 15$

↳ $(9 + 6) \cdot 7^{-1} \bmod 15$

↳ $(15) \cdot 7^{-1} \bmod 15$

④ Apply multiplication property:

↳ $(15) \cdot 7^{-1} \bmod 15$

↳ $(15 \bmod 15) \cdot (7^{-1} \bmod 15)$

⑤ Solve terms :

↳ $(15 \bmod 15) \cdot (7^{-1} \bmod 15)$

↳ $(0) \cdot (13)$ → (Answer $7^{-1} \bmod 15$ from problem 4b-3)

$\boxed{\text{Answer : } 0 \pmod{15}}$

Problem 4b-5:

Equation: $3^2 - 4 \bmod 15$

① Apply subtraction property:

↳ $(3^2 \bmod 15) - (4 \bmod 15)$

② Apply exponentiation property:

↳ $((3 \bmod 15)^2 \bmod 15) - (4 \bmod 15)$

③ Solve terms:

↳ $((3)^2 \bmod 15) - (4 \bmod 15)$

↳ $(9 \bmod 15) - (4 \bmod 15)$

↳ $(9) - (4) = \underline{\underline{5}}$

$\boxed{\text{Answer: } 5 \pmod{15}}$

Problem 4c - 1 :

Equation : $4 + 7 \pmod{15}$

① Apply associative property :

↳ $(4 \bmod 15) + (7 \bmod 15)$

② Separate by factors of 15 (3, 5) :

↳ $(4 \bmod 3, 4 \bmod 5) + (7 \bmod 3, 7 \bmod 5)$

③ Simplify terms :

↳ $(11 \bmod 3, 11 \bmod 5)$

④ Reduce to values in range of modulus :

↳ $(2 \bmod 3, 1 \bmod 5)$

$$\boxed{\text{Answer : } (2 \bmod 3, 1 \bmod 5)}$$

Problem 4c-2 :

Equation : $8 - (3 \cdot 4) \pmod{15}$

① Apply subtraction and multiplication property:

↳ $(8 \bmod 15) - (3 \bmod 15)(4 \bmod 15)$

② Separate terms by factors of 15 (3,5) :

↳ $(8 \bmod 3, 8 \bmod 5) - (3 \bmod 3, 3 \bmod 5)$
$\cdot (4 \bmod 3, 4 \bmod 5)$

③ Simplify terms :

↳ $(8 \bmod 3, 8 \bmod 5) - (12 \bmod 3, 12 \bmod 5)$

↳ $(-4 \bmod 3, -4 \bmod 5)$

④ Reduce to values in range of modulus :

↳ $(2 \bmod 3, 1 \bmod 5)$

$\boxed{\text{Answer : } (2 \bmod 3, 1 \bmod 5)}$

Problem 4C - 3:

Equation: $3^2 + 6 \pmod{15}$

① Apply addition property:

↳ $(3^2 \bmod 15) + (6 \bmod 15)$

② Apply exponentiation property:

↳ $((3 \bmod 15)^2 \bmod 15) + (6 \bmod 15)$

③ Simplify terms:

↳ $((3)^2 \bmod 15) + (6 \bmod 15)$

↳ $(9 \bmod 15) + (6 \bmod 15)$

④ Separate terms by factors of 15 (3,5):

↳ $(9 \bmod 3, 9 \bmod 5) + (6 \bmod 3, 6 \bmod 5)$

⑤ Simplify terms:

↳ $(15 \bmod 3, 15 \bmod 5)$

⑥ Reduce to values in range of modulus:

↳ $(0 \bmod 3, 0 \bmod 5)$

$\boxed{\text{Answer: } (0 \bmod 3, 0 \bmod 5)}$

Problem 4c-4 :

Equation : $3^2 - 4 \pmod{15}$

① Apply subtraction property :

↳ $(3^2 \bmod 15) - (4 \bmod 15)$

② Apply exponentiation property :

↳ $((3 \bmod 15)^2 \bmod 15) - (4 \bmod 15)$

③ Simplify terms :

↳ $((3)^2 \bmod 15) - (4 \bmod 15)$

↳ $(9 \bmod 15) - (4 \bmod 15)$

④ Separate terms by factors of 15 (3, 5) :

↳ $(9 \bmod 3, 9 \bmod 5) - (4 \bmod 3, 4 \bmod 5)$

⑤ Simplify terms :

↳ $(5 \bmod 3, 5 \bmod 5)$

⑥ Reduce to values in range of modulus :

↳ $(2 \bmod 3, 0 \bmod 5)$

$\boxed{\text{Answer : } (2 \bmod 3,\ 0 \bmod 5)}$

Problem 5a :

Equations : $x \equiv 3 \mod 7$

$x \equiv 4 \mod 9$

① Check modulos are relatively prime :

↳ $GCD(7,9)$

↳ $9 = 7(1) + (2)$

$7 = 2(3) + (\underline{1}) \rightarrow GCD(7,9) = 1$ } Euclidean Algorithm

$2 = 1(2) + (0)$

② Solve for x using CRT equation :

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \mod M$$

where $\underset{a_1}{x \equiv 3} \mod \underset{m_1}{7}$; $\underset{a_2}{x \equiv 4} \mod \underset{m_2}{9}$ } For two congruent equations

$M = m_1 \cdot m_2$; $M_1 = \frac{M}{m_1}$; $M_2 = \frac{M}{m_2}$

③ Calculate value for M :

↳ $M = m_1 \cdot m_2$

$M = 7 \cdot 9$

$\underline{\underline{M = 63}}$

④ Calculate values for M_1 and M_2 :

↳ $M_1 = \frac{M}{m_1} = \frac{63}{7} = \underline{\underline{9}}$

↳ $M_2 = \frac{M}{m_2} = \frac{63}{9} = \underline{\underline{7}}$

⑤ Calculate values for M_1^{-1} and M_2^{-1} :

↳ $M_1^{-1} = M_1 \cdot M_1^{-1} \equiv 1 \bmod m_1$

$= 9 \cdot M_1^{-1} \equiv 1 \bmod 7$

$= 9x \equiv 1 \bmod 7$ (let $M_1^{-1} = x$)

$= 9x + 7y = 1$

$= 9 = 7(1) + (2)$

$= 7 = 2(3) + (\underline{\underline{1}})$

$= 2 = 1(2) + (0)$

$= 1 = 7 + 2(-3)$

$= 1 = 7 + (9 + 7(-1))(-3)$

$= 1 = 7 + 9(-3) + 7(3)$

$= 1 = 7(4) + \underline{\underline{9(-3)}}$

Extended Euclidean Algorithm

$\underline{\underline{M_1^{-1} = -3}}$

$\hookrightarrow M_2^{-1} = M_2 \cdot M_2^{-1} \equiv 1 \bmod m_2$

$= 7 \cdot M_2^{-1} \equiv 1 \bmod 9$

$= 7x \equiv 1 \bmod 9$ (let $M_2^{-1} = x$)

$= 7x + 9y = 1$

$= 9 = 7(1) + (2)$

$= 7 = 2(3) + \underline{(1)}$

$= 2 = 1(2) + (0)$

$= 1 = 7 + 2(-3)$

$= 1 = 7 + (9 + 7(-1))(-3)$

$= 1 = 7 + 9(-3) + 7(3)$

$= 1 = 7\underline{\underline{(4)}} + 9(-3)$

$\underline{\underline{M_2^{-1} = 4}}$

Extended Euclidean Algorithm

⑥ Substitute values in equation to solve x:

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M$

$x = (3 \cdot 9 \cdot -3 + 4 \cdot 7 \cdot 4) \bmod 63$

$x = (-81 + 112) \bmod 63$

$x = (31) \bmod 63$

Used SageMath

$x = 31$

$\boxed{\text{Answer: } 31 \pmod{63}}$

check answer:

$31 \equiv 3 \bmod 7$ ✓

$31 \equiv 4 \bmod 9$ ✓

Problem 5b :

Equations : $X \equiv 137 \bmod 423$
$X \equiv 87 \bmod 191$

① Check modulus are relatively prime :

↳ GCD(423, 191)

↳
$$\left.\begin{aligned}
423 &= 191(2) + (41) \\
191 &= 41(4) + (27) \\
41 &= 27(1) + (14) \\
27 &= 14(1) + (13) \\
14 &= 13(1) + (12) \\
13 &= 12(1) + (\underline{1}) \rightarrow \text{GCD} = 1 \\
12 &= 1(12) + (0)
\end{aligned}\right\} \text{Euclidean Algorithm}$$

② Solve for x using CRT equation :

$$\left.\begin{aligned}
&X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M \\
&\text{where } X \equiv \underset{a_1}{137} \bmod \underset{m_1}{423} \; ; \; X \equiv \underset{a_2}{87} \bmod \underset{m_2}{191} \\
&M = m_1 \cdot m_2 \; ; \; M_1 = \frac{M}{m_1} \; ; \; M_2 = \frac{M}{m_2}
\end{aligned}\right\} \text{For two Congruent equations}$$

③ Calculate value for M :

↳ $M = m_1 \cdot m_2$

$$\left.\begin{aligned}
M &= 423 \cdot 191 \\
\underline{\underline{M}} &\underline{\underline{= 80{,}793}}
\end{aligned}\right\} \text{used Sage Math for calculation}$$

④ Calculate values for M_1 and M_2 :

$\hookrightarrow M_1 = \frac{M}{m_1} = \frac{80{,}793}{423} = \underline{\underline{191}}$

$\hookrightarrow M_2 = \frac{M}{m_2} = \frac{80{,}793}{191} = \underline{\underline{423}}$

used SageMath for calculation

⑤ Calculate values for M_1^{-1} and M_2^{-1} :

$\hookrightarrow M_1^{-1} = M_1 \cdot M_1^{-1} \equiv 1 \bmod m_1$

$= 191 \cdot M_1^{-1} \equiv 1 \bmod 423$

$= 191x \equiv 1 \bmod 423$ (let $M_1^{-1} = x$)

$= 191x + 423y = 1$

$= 423 = 191(2) + (41)$

$= 191 = 41(4) + (27)$

$= 41 = 27(1) + (14)$

$= 27 = 14(1) + (13)$

$= 14 = 13(1) + \underline{(1)}$

$= 13 = 1(13) + (0)$

$= 1 = 14 + 13(-1)$

$= 1 = (41 + 27(-1)) + (27 + 14(-1))(-1)$

$= 1 = 41 + 27(-1) + 27(-1) + 14(1)$

$= 1 = (423 + 191(-2)) + 27(-2) + 14(1)$

Extended Euclidean Algorithm

(see next page)

$$= \quad 1 = 423 + 191(-2) + (191 + 41(-4))(-2)$$
$$+ (41 + 27(-1))(1)$$
$$= \quad 1 = 423 + 191(-2) + 191(-2) + 41(8)$$
$$+ 41(1) + 27(-1)$$
$$= \quad 1 = 423 + 191(-4) + 41(9) + 27(-1)$$
$$= \quad 1 = 423 + 191(-4) + (423 + 191(-2))(9)$$
$$+ ((191 + 41(-4))(-1)$$
$$= \quad 1 = 423 + 191(-4) + 423(9) + 191(-18)$$
$$+ 191(-1) + 41(4)$$
$$= \quad 1 = 423(10) + 191(-23) + 41(4)$$
$$= \quad 1 = 423(10) + 191(-23) + ((423 + 191)(-2))(4)$$
$$= \quad 1 = 423(10) + 191(-23) + 423(4) + 191(-8)$$
$$= \quad 1 = 423(14) + 191\underline{\underline{(-31)}}$$

$$\underline{\underline{M_1^{-1} = -31}}$$

$\hookrightarrow M_2^{-1} = M_2 \cdot M_2^{-1} \equiv 1 \bmod m_2$

$= 423 \cdot M_2^{-1} \equiv 1 \bmod 191$

$= 423x \equiv 1 \bmod 191$ (let $x = M_2^{-1}$)

$= 423x + 191y = 1$

$= 423 = 191(2) + (41)$

$= 191 = 41(4) + (27)$

$= 41 = 27(1) + (14)$

$= 27 = 14(1) + (13)$

$= 14 = 13(1) + \underline{(1)}$

$= 13 = 1(13) + (0)$

$= 1 = 14 + 13(-1)$

$= 1 = (41 + 27(-1)) + (27 + 14(-1))(-1)$

$= 1 = 41 + 27(-1) + 27(-1) + 14(1)$

$= 1 = 423 + 191(-2) + 27(-2) + 14(1)$

$= 1 = 423 + 191(-2) + (191 + 41(-4))(-2) + (41 + 27(-1))(1)$

$= 1 = 423 + 191(-2) + 191(-2) + 41(8) + 41(1) + 27(-1)$

$= 1 = 423 + 191(-4) + 41(9) + 27(-1)$

Extended Euclidean Algorithm

(see next page)

$= 1 = 423 + 191(-4) + 423(9) + 191(-18)$
$+ 191(-1) + 41(4)$
$= 1 = 423(10) + 191(-23) + 41(4)$
$= 1 = 423(10) + 191(-23) + ((423 + 191)(-2))(4)$
$= 1 = 423(10) + 191(-23) + 423(4) + 191(-8)$
$= 1 = 423(\underline{\underline{14}}) + 191(-31)$

$\underline{\underline{M_2^{-1} = 14}}$ } used SageMath for calculation

⑥ Substitute values in equation to solve x:

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M$
$x = (137 \cdot 191 \cdot -31 + 87 \cdot 423 \cdot 14) \bmod 80{,}793$
$x = (-811{,}177 + 515{,}214) \bmod 80{,}793$
$x = (-295{,}963) \bmod 80{,}793$
$x = 27{,}209$

$\boxed{\text{Answer: } 27{,}209 \pmod{80{,}793}}$ } used SageMath for calculation

check work:

$27{,}209 \equiv 137 \bmod 423$ ✓
$27{,}209 \equiv 87 \bmod 191$ ✓

Problem 5C :

Equations : $X \equiv 133 \mod 451$
$X \equiv 237 \mod 697$

① check modulus are relatively prime :

↳ GCD(451, 697)

↳ $697 = 451(1) + (246)$

↳ $451 = 246(1) + (205)$

↳ $246 = 205(1) + (\underline{41}) \rightarrow GCD = 41$

↳ $205 = 41(5) + (0)$

Answer : No solution. According to properties of the Chinese Remainder Theorem, the GCD amongst all equations must be 1 (relatively prime). As the GCD (451, 697) is 41, this equation has no solution.

Problem 5d :

Equations : $x \equiv 5 \mod 9$
$x \equiv 6 \mod 10$
$x \equiv 7 \mod 11$

① Check modulus are relatively prime :

↳ GCD (9, 10) , GCD (10, 11) , GCD (9, 11)

↳ GCD (9, 10)

$10 = 9(1) + (\underline{\underline{1}}) \rightarrow GCD = 1$

$9 = 1(9) + (0)$

↳ GCD (10, 11)

$11 = 10(1) + (\underline{\underline{1}}) \rightarrow GCD = 1$

$10 = 1(10) + (0)$

↳ GCD (9, 11)

$11 = 9(1) + (2)$

$9 = 2(4) + (\underline{\underline{1}}) \rightarrow GCD = 1$

$2 = 1(2) + (0)$

Euclidean Algorithm

② Solve for X using CRT equation :

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \mod M$$

where $\underset{a_1}{x \equiv 5} \mod \underset{m_1}{9}$; $\underset{a_2}{x \equiv 6} \mod \underset{m_2}{10}$; $\underset{a_3}{x \equiv 7} \mod \underset{m_3}{11}$

$$M = m_1 \cdot m_2 \cdot m_3 \; ; \; M_1 = \frac{M}{m_1} \; ; \; M_2 = \frac{M}{m_2} \; ; \; M_3 = \frac{M}{M_3}$$

③ Calculate value for M:

↳ $M = m_1 \cdot m_2 \cdot m_3$

$M = 9 \cdot 10 \cdot 11$

$\underline{\underline{M = 990}}$

Used SageMath for calculation

④ Calculate values for M_1, M_2, M_3:

↳ $M_1 = \frac{M}{m_1} = \frac{990}{9} = \underline{\underline{110}}$

↳ $M_2 = \frac{M}{m_2} = \frac{990}{10} = \underline{\underline{99}}$

↳ $M_3 = \frac{M}{m_2} = \frac{990}{11} = \underline{\underline{90}}$

used SageMath for calculation

⑤ Calculate values for $M_1^{-1}, M_2^{-1}, M_3^{-1}$:

↳ $M_1^{-1} = M_1 \cdot M_1^{-1} \equiv 1 \bmod m_1$

$= 110 \cdot M_1^{-1} \equiv 1 \bmod 9$

$= 110x \equiv 1 \bmod 9$ (let $M_1^{-1} = x$)

$= 110x + 9y = 1$

(see next page)

$= 110x + 9y = 1$

$= 110 = 9(12) + (2)$

$= 9 = 2(4) + (1)$

$= 2 = 1(2) + (0)$

$= 1 = 9 + 2(-4)$

$= 1 = 9 + (110 + 9(-12))(-4)$

$= 1 = 9 + 110(-4) + 9(48)$

$= 1 = 9(49) + 110(\underline{-4})$

Extended Euclidean Algorithm

$M_1^{-1} = -4$

$M_2^{-1} = M_2 \cdot M_2^{-1} \equiv 1 \bmod m_2$

$= 99 \cdot M_2^{-1} \equiv 1 \bmod 10$

$= 99x \equiv 1 \bmod 10$ (let $M_2^{-1} = x$)

$= 99x + 10y = 1$

$= 99 = 10(9) + (9)$

$= 10 = 9(1) + (1)$

$= 9 = 1(9) + (0)$

$= 1 = 10 + 9(-1)$

$= 1 = 10 + (99 + 10(-9))(-1)$

$= 1 = 10 + 99(-1) + 10(9)$

$= 1 = 10(10) + 99(\underline{-1})$

Extended Euclidean Algorithm

$M_2^{-1} = -1$

$$M_3^{-1} = M_3 \cdot M_3^{-1} \equiv 1 \bmod m_3$$
$$= 90 \cdot M_3^{-1} \equiv 1 \bmod 11$$
$$= 90x \equiv 1 \bmod 11 \quad (\text{let } M_3^{-1} = x)$$
$$= 90x + 11y = 1$$

$$= 90 = 11(8) + (2)$$
$$= 11 = 2(5) + (\underline{1})$$
$$= 2 = 1(2) + (0)$$

$$= 1 = 11 + 2(-5)$$
$$= 1 = 11 + (90 + 11(-8))(-5)$$
$$= 1 = 11 + 90(-5) + 11(40)$$
$$= 1 = 11(41) + 90(\underline{\underline{-5}})$$

Extended Euclidean Algorithm

$$\underline{\underline{M_3^{-1} = -5}}$$

(6) Substitute values in equation to solve X:

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$
$$X = (5 \cdot 110 \cdot -4 + 6 \cdot 99 \cdot -1 + 7 \cdot 90 \cdot -5) \bmod 990$$
$$X = ((-2200) + (-594) + (-3150)) \bmod 990$$
$$X = (-5944) \bmod 990$$
$$X = 986$$

$$\boxed{\text{Answer: } 986 \pmod{990}}$$

used SageMath

check work:

$986 \equiv 5 \bmod 9$ ✓

$986 \equiv 6 \bmod 10$ ✓

$986 \equiv 7 \bmod 11$ ✓

Problem 5e :

Equations : $x \equiv 37 \bmod 43$
$x \equiv 22 \bmod 49$
$x \equiv 18 \bmod 71$

① Check modulus are relatively prime :

↳ GCD(43,49) , GCD(49,71) , GCD(43,71)

↳ GCD(43,49)

$49 = 43(1) + (6)$
$43 = 6(7) + (1) \rightarrow GCD = 1$
$6 = 1(6) + (0)$

↳ GCD(49,71)

$71 = 49(1) + (22)$
$49 = 22(2) + (5)$
$22 = 5(4) + (2)$
$5 = 2(2) + (1) \rightarrow GCD = 1$
$2 = 1(2) + (0)$

↳ GCD(43,71)

$71 = 43(1) + (28)$
$43 = 28(1) + (15)$
$28 = 15(1) + (13)$
$15 = 13(1) + (2)$
$13 = 2(6) + (1) \rightarrow GCD = 1$
$2 = 1(2) + (0)$

Euclidean Algorithm

② Solve for x using CRT equation:

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

where $\underset{a_1}{x \equiv 37} \bmod \underset{m_1}{43}$; $\underset{a_2}{x \equiv 22} \bmod \underset{m_2}{49}$; $\underset{a_3}{x \equiv 18} \bmod \underset{m_3}{71}$

$M = m_1 \cdot m_2 \cdot m_3$; $M_1 = \frac{M}{m_1}$; $M_2 = \frac{M}{m_2}$; $M_3 = \frac{M}{m_3}$

③ Calculate value for M:

$$\left.\begin{aligned} \hookrightarrow M &= m_1 \cdot m_2 \cdot m_3 \\ M &= 43 \cdot 49 \cdot 71 \\ M &= \underline{\underline{149{,}597}} \end{aligned}\right\} \text{used SageMath for calculation}$$

④ Calculate values for M_1, M_2, M_3:

$$\left.\begin{aligned} \hookrightarrow M_1 &= \frac{M}{m_1} = \frac{149{,}597}{43} = \underline{\underline{3{,}479}} \\ \hookrightarrow M_2 &= \frac{M}{m_2} = \frac{149{,}597}{49} = \underline{\underline{3{,}053}} \\ \hookrightarrow M_3 &= \frac{M}{m_3} = \frac{149{,}597}{71} = \underline{\underline{2{,}107}} \end{aligned}\right\} \text{Used SageMath}$$

⑤ Calculate values for $M_1^{-1}, M_2^{-1}, M_3^{-1}$:

$\hookrightarrow M_1^{-1} = M_1 \cdot M_1^{-1} \equiv 1 \bmod m_1$

$= 3479 \cdot M_1^{-1} \equiv 1 \bmod 43$

$= 3479x \equiv 1 \bmod 43$ (let $M_1^{-1} = x$)

$= 3479x + 43y = 1$

$= 3479 = 43(80) + (39)$

$= 43 = 39(1) + (4)$

$= 39 = 4(9) + (3)$

$= 4 = 3(1) + (\underline{1})$

$= 3 = 1(3) + (0)$

$= 1 = 4 + 3(-1)$

$= 1 = (43 + 39(-1)) + (39 + 4(-9))(-1)$

$= 1 = 43 + 39(-1) + 39(-1) + 4(9)$

$= 1 = 43 + 39(-2) + (43 + 39(-1))(9)$

$= 1 = 43 + 39(-2) + 43(9) + 39(-9)$

$= 1 = 43(10) + 39(-11)$

$= 1 = 43(10) + (3479 + 43(-80))(-11)$

$= 1 = 43(10) + 3479(-11) + 43(880)$

$= 1 = 43(890) + 3479\underline{(-11)}$

Extended Euclidean Algorithm

$\underline{M_1^{-1} = -11}$

$\hookrightarrow M_2^{-1} = M_2 \cdot M_2^{-1} \equiv 1 \bmod m_2$

$= 3053 \cdot M_2^{-1} \equiv 1 \bmod 49$

$= 3053x \equiv 1 \bmod 49$ (let $M_2^{-1} = x$)

$= 3053x + 49y = 1$

$= 3053 = 49(62) + (15)$

$= 49 = 15(3) + (4)$

$= 15 = 4(3) + (3)$

$= 4 = 3(1) + \underline{(1)}$

$= 3 = 1(3) + (0)$

$= 1 = 4 + 3(-1)$

$= 1 = (49 + 15(-3)) + (15 + 4(-3))(-1)$

$= 1 = 49 + 15(-3) + 15(-1) + 4(3)$

$= 1 = 49 + 15(-4) + (49 + 15(-3))(3)$

$= 1 = 49 + 15(-4) + 49(3) + 15(-9)$

$= 1 = 49(4) + 15(-13)$

$= 1 = 49(4) + (3053 + 49(-62))(-13)$

$= 1 = 49(4) + 3053(-13) + 49(806)$

$= 1 = 49(810) + 3053\,\underline{(-13)}$

$\underline{M_2^{-1} = -13}$

Extended Euclidean Algorithm

$$M_2^{-1} = M_3 \cdot M_3^{-1} \equiv 1 \bmod m_3$$

$$= 2107 \cdot M_3^{-1} \equiv 1 \bmod 71$$

$$= 2107\,x \equiv 1 \bmod 71 \quad (\text{let } M_3^{-1} = x)$$

$$= 2107x + 71y = 1$$

$$= 2107 = 71(29) + (48)$$

$$= 71 = 48(1) + (23)$$

$$= 48 = 23(2) + (2)$$

$$= 23 = 2(11) + \underline{(1)}$$

$$= 2 = 1(2) + (0)$$

$$= 1 = 23 + 2(-11)$$

$$= 1 = (71 + 48(-1)) + (48 + 23(-2))(-11)$$

$$= 1 = 71 + 48(-1) + 48(-11) + 23(22)$$

$$= 1 = 71 + 48(-12) + (71 + 48(-1))(22)$$

$$= 1 = 71 + 48(-12) + 71(22) + 48(-22)$$

$$= 1 = 71(23) + 48(-34)$$

$$= 1 = 71(23) + (2107 + 71(-29))(-34)$$

$$= 1 = 71(23) + 2107(-34) + 71(986)$$

$$= 1 = 71(1009) + 2107\underline{(-34)}$$

$$\underline{\underline{M_3^{-1} = -34}}$$

Extended Euclidean Algorithm

⑥ Substitute values in equation to solve x:

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

$$X = (37 \cdot 3479 \cdot -11 + 22 \cdot 3053 \cdot -13 + 18 \cdot 2107 \cdot -34) \bmod 149{,}597$$

$$X = ((-1{,}415{,}953) + (-873{,}158) + (-1{,}289{,}484)) \bmod 149{,}597$$

$$X = (-3{,}578{,}595) \bmod 149{,}597$$

$$X = 11{,}733$$

$\boxed{\text{Answer: } 11{,}733 \pmod{149{,}597}}$ } used SageMath for calculations

---

check work:

$11{,}733 \equiv 37 \bmod 43$ ✓

$11{,}733 \equiv 22 \bmod 49$ ✓

$11{,}733 \equiv 18 \bmod 71$ ✓

References

Student Discussions

- Chidanand Bangalore
- Satya Srinivas
- Naphi Tang
- Iyioluwa Ojo-Aromokudu
- Nick Keith
- Jyotsna Sharma

Tools and Resources

- Hoffstein textbook
- Async video (module 2)
- Google searches
- Youtube
- Wikipedia
- Stack Exchange
- Brilliant.org
- Sage Math
- Wolfram Alpha