

MATH 470: Communications and Cryptography**Homework 2***Due date: 7 September 2023**Name: Huy Lai*

Problem 1. For each of the $\gcd(a, b)$ values in Exercise 1.9, use the extended Euclidean algorithm (Theorem 1.11) to find integers u and v such that $au + bv = \gcd(a, b)$. Let $a = 291$ and $b = 252$

Solution:

q	r	u	v
	291	1	0
	252	0	1
1	39	1	-1
6	18	-6	7
2	3	13	-15
	0	u	v

Table 1: Extended Euclidean Algorithm

$$u = 13, v = -15$$

Problem 2. Let a_1, a_2, \dots, a_k be integers with $\gcd(a_1, a_2, \dots, a_k) = 1$ i.e., the largest positive integer dividing all of a_1, a_2, \dots, a_k is 1. Prove that the equation

$$a_1u_1 + a_2u_2 + \dots + a_ku_k = 1$$

has a solution in integers u_1, u_2, \dots, u_k . (*Hint.* Repeatedly apply the extended Euclidean algorithm, Theorem 1.11. You may find it easier to prove a more general statement in which $\gcd(a_1, \dots, a_k)$ is allowed to be larger than 1.)

Solution:

Proof by Induction

Proof. Base case: $k = 1$

$$a_1 \cdot 1 = \gcd(a_1)$$

$k = 2$

This is proven by the Extended Euclidean Algorithm

Inductive Hypothesis: Assume $\forall k \geq 3$ that

$$a_1u_1 + a_2u_2 + \dots + a_{k-1}u_{k-1} = \gcd(a_1, a_2, \dots, a_{k-1})$$

Let $b = \gcd(a_1, \dots, a_{k-1})$.

Apply the Extended Euclidean algorithm to b and a_k , this gives the solution

$$bu + a_kv = \gcd(b, a_k)$$

Multiplying the Inductive Hypothesis by v results in

$$\begin{aligned} a_1u_1v + a_2u_2v + \dots + a_{k-1}u_{k-1}v &= \gcd(a_1, a_2, \dots, a_{k-1})v \\ &= b \text{ by the definition of } b \\ &= -a_kv + \gcd(b, a_k) \text{ by rearranging the EEA} \end{aligned}$$

Adding a_kv to both sides of this equation results in

$$a_1u_1 + a_2u_2 + \dots + a_{k-1}u_{k-1} + a_kv = \gcd(b, a_k)$$

Since $b = \gcd(a_1, \dots, a_{k-1})$,

$$\begin{aligned} \gcd(b, a_k) &= \gcd(\gcd(a_1, \dots, a_{k-1}), a_k) \\ &= \gcd(a_1, a_2, \dots, a_{k-1}, a_k) \end{aligned}$$

□

Problem 3. Find all values of x between 0 and $m - 1$ that are solutions of the following congruences. (*Hint.* If you can't figure out a clever way to find the solution(s), you can just substitute each value $x = 1, x = 2, \dots, x = m - 1$ and see which ones work.)

Subproblem 1. $x^2 \equiv 3 \pmod{11}$

Solution:

The squares modulo 11 are $\{0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1\}$

Therefore, $5^2 \equiv 3 \pmod{11}$ and $6^2 \equiv 3 \pmod{11}$

Subproblem 2. $x^2 \equiv 2 \pmod{13}$

Solution:

The squares modulo 13 are $\{0, 1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1\}$

Therefore, $x^2 \equiv 2 \pmod{13}$ has no solutions

Problem 4. Suppose that $g^a \equiv 1 \pmod{m}$ and that $g^b \equiv 1 \pmod{m}$. Prove that

$$g^{\gcd(a,b)} \equiv 1 \pmod{m}$$

Solution:

According to the Extended Euclidean Algorithm, $\exists u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a, b)$. Then

$$g^{\gcd(a,b)} = g^{au+bv} = (g^a)^u \cdot (g^b)^v \equiv 1^u \cdot 1^v \equiv 1 \pmod{m}$$

Since $g^a \equiv 1 \pmod{m}$ and $g^b \equiv 1 \pmod{m}$, the above equation holds.

Problem 5. Let $m \in \mathbb{Z}$

Subproblem 1. Suppose that m is odd. What integer between 1 and $m - 1$ equals $2^{-1} \pmod{m}$?

Solution:

Since m is odd, then $\frac{m+1}{2}$ must also be an integer, since $m+1$ is an even number. Therefore

$$2 \cdot \frac{m+1}{2} = m+1 \equiv 1 \pmod{m}$$

Therefore $\frac{m+1}{2} = 2^{-1} \pmod{m}$

Subproblem 2. More generally, suppose that $m \equiv 1 \pmod{b}$. What integer between 1 and $m - 1$ is equal to $b^{-1} \pmod{m}$?

Solution:

The assumption that $m \equiv 1 \pmod{b} \rightarrow b \mid (m - 1)$ by proposition.

By the definition of division, $b \mid (m - 1) \rightarrow \exists x \in \mathbb{Z}$ such that $m - 1 = bx$. This requires that $\frac{m-1}{b} \in \mathbb{Z}$

Multiplying this fraction by b results in

$$b \cdot \frac{m-1}{b} = m-1 \equiv -1 \pmod{m}$$

Multiplying this result by -1 results in

$$b \cdot \frac{1-m}{b} = 1-m \equiv 1 \pmod{m}$$

However, $\frac{1-m}{b}$ is negative, but we can add multiples of m without effecting the value of modulo m . As a result,

$\frac{1-m}{b} + m = \frac{1+(b-1)m}{b}$ is an integer and more importantly is congruent to $1 \pmod{m}$.

Therefore, $\frac{1+(b-1)m}{b} = b^{-1} \pmod{m}$

Problem 6. Consider the congruence

$$ax \equiv c \pmod{m}$$

Prove that there is a solution if and only if $\gcd(a, m) \mid c$.

Solution:

First we prove that if $ax \equiv c \pmod{m}$ has a solution, then $\gcd(a, m) \mid c$

Proof. Let $g = \gcd(a, m)$.

According to the definition of divisors, $\exists p, q \in \mathbb{Z}$ such that $a = gp$ and $m = gq$

We can take this definition and substitute it into the congruence which results in.

$$gpx \equiv c \pmod{gq}$$

Since g divides both sides of the congruence, we can divide by g

$$px \equiv \frac{c}{g} \pmod{q}$$

$\frac{c}{g}$ must be an integer in order for the congruence to hold.

This implies that $\gcd(a, m) \mid c$

This proves that if $ax \equiv c \pmod{m}$ then $\gcd(a, m) \mid c$ □

Next we prove that if $\gcd(a, m) \mid c$, then $ax \equiv c \pmod{m}$ has a solution

Proof. According to the Extended Euclidean Algorithm, $\exists u, v \in \mathbb{Z}$ such that

$$au + mv = \gcd(a, m)$$

$$\gcd(a, m) \mid c \rightarrow (au + mv) \mid c$$

By definition of divisibility, $\exists y \in \mathbb{Z}$ such that $c = (au + mv)y$

Rearranging this equation results in $mvy = c - auy \Rightarrow -mvy = auy - c$ or equivalently $mY = aX - c$ where $X = uy, Y = -vy$

Since $X, Y \in \mathbb{Z}$, the definition of divisibility implies that $m \mid (aX - c)$.

By one of the modular propositions, $m \mid (aX - c) \rightarrow aX \equiv c \pmod{m}$.

This proves that if $\gcd(a, m) \mid c$, then $ax \equiv c \pmod{m}$ has a solution □

$$a = 123456789012345678901234567890123456789012345678901234567890123456789,$$
$$b = 23456789012345678901234567890123456789012345678901234567890123456789$$

Solution:

6



```
pineapple@Pineapple: /mnt/c  x + v
pineapple@Pineapple: /mnt/c/MrPineapple/TAMU/MATH 470/Homework 2$ python3 modInverse.py
a(-1) mod b = 99353031097916192520417712888739223382820736393198081539055480041500162181280
a*a(-1)==1 mod b? True
b(-1) mod a = 711657180071165718007116571800711657180071165718007116571800711657180071165618
b*b(-1)==1 mod a? True
pineapple@Pineapple: /mnt/c/MrPineapple/TAMU/MATH 470/Homework 2$
```

Figure 1: Output