UWO CS2214

Tutorial #7

**Problem 1** Let $a, b, c, m$ be four positive integers with $m > 1$. Assume that $a$ has an inverse modulo $m$. Prove that if each of $b$ and $c$ is an inverse of $a$ modulo $m$ then we have: $b \equiv c \mod m$ .

**Solution 1** Let us assume that each of $b$ and $c$ is an inverse of $a$ modulo $m$. Thus, we have

$$ab \equiv 1 \mod m \text{ and } ac \equiv 1 \mod m.$$

This implies

$$ab \equiv ac \mod m.$$

That is:

$$a(b-c) \equiv 0 \mod m.$$

In other words, $m$ divides $a(b-c)$. Since $a$ has an inverse modulo $m$, we have:

$$\gcd(a, m) = 1.$$

Therefore, $m$ divides $b - c$, that is:

$$b \equiv c \mod m.$$

**Problem 2** Let $a, b, m$ be three positive integers with $m > 1$. Consider the function $f$ from $\mathbb{Z}_m$ to $\mathbb{Z}_m$ defined by

$$f(p) = ap + b \mod m$$

1. Prove that $f$ is injective if and only if $a$ and $m$ are relatively prime.
2. Prove that if $a$ and $m$ are relatively prime, then $f$ is surjective. Is the converse true?
3. When $a$ and $m$ are relatively prime, what is the inverse function of $f$?

**Solution 2**

1. $f$ injective means that for all $p, q \in \mathbb{Z}_m$ we have

$$f(p) = f(q) \quad \longrightarrow \quad p \equiv q \mod m.$$

The equation $f(p) = f(q)$ is equivalent to:

$$ap + b \equiv aq + b \mod m,$$

that is:

$$a(p - q) \equiv 0 \mod m.$$

Therefore, $f$ injective means that for all $p, q \in \mathbb{Z}_m$ we have

$$a(p - q) \equiv 0 \mod m \quad \longrightarrow \quad p \equiv q \mod m.$$

In other words:

$$m \text{ divides } a(p - q) \quad \longrightarrow \quad m \text{ divides } (p - q)$$

This proves that if $a$ and $m$ are relatively prime, then $f$ is injective. Now, suppose that $f$ is not injective. Then, there exists $p, q \in \mathbb{Z}_m$, with $p \neq q$ and $m$ divides $a(p - q)$. Because $0 < p - q < m$ holds, we cannot have $\gcd(a, m) = 1$, otherwise $m$ would divide $p - q$.

2. Assume that $a$ and $m$ are relatively prime and let us prove that $f$ is surjective. Since $a$ and $m$ are relatively prime, we know that $f$ is injective. Now observe that the domain and the codomain of $f$ are the same finite set $\mathbb{Z}_m$. Since $f$ is injective, the images $f(p)$ for all $p \in \mathbb{Z}_m$ are disctint and thus there are $m$ of them. Since the codomain of $f$ is $\mathbb{Z}_m$, necessarily, every element of $\mathbb{Z}_m$ must have a pre-image in $\mathbb{Z}_m$ by $f$, thus $f$ is surjective.
   The converse is true and this can be proved by a similar reasoning: if $a$ and $m$ are not relatively prime, then $f$ is not injective and two different elements $p, q \in \mathbb{Z}_m$ have the same image. Hence, at least one element of $\mathbb{Z}_m$ does not have a pre-image by $f$ in $\mathbb{Z}_m$, that is, $f$ is not surjective. The key point here is that the domain and the codomain of $f$ are the same finite set $\mathbb{Z}_m$.
3. Assume that $a$ and $m$ are relatively prime. Then, there exists $c \in \mathbb{Z}_m$ such that $ac \equiv 1 \mod m$. The inverse function $f^{-1}$ of $f$ is given by

$$f^{-1}(q) = c(q - b) \mod m.$$

**Problem 3** Find $s, t$, and $\gcd(a, b)$ such that $s\,a + t\,b = \gcd(a, b)$ holds in the following cases:

1. $a = 2$ and $b = 3$,
2. $a = 11$ and $b = 12$,
3. $a = 12$ and $b = 15$,

4. $a = 3$ and $b = 7$,

**Solution 3**

1. $-1 \times 2 + 1 \times 3 = 1 = \gcd(a, b)$,
2. $-1 \times 11 + 1 \times 12 = 1 = \gcd(a, b)$,
3. $-1 \times 12 + 1 \times 15 = 3 = \gcd(a, b)$,
4. $-2 \times 3 + 1 \times 7 = 1 = \gcd(a, b)$,.

**Problem 4**

1. Find all integers $x$ such that $0 \leq x < 21$ and $4x + 9 \equiv 13 \mod 21$. Justify your answer.
2. Find all integers $x$ and $y$ such that $0 \leq x < 21$, $0 \leq y < 21$, $x + 2y \equiv 4 \mod 21$ and $3x - y \equiv 10 \mod 21$. Justify your answer.
3. Find all integers $x$ such that $0 \leq x < 21$, $x \equiv 2 \mod 3$ and $x \equiv 6 \mod 7$.

**Solution 4**

1. We have $4 \times 5 \equiv -1 \mod 21$. Thus, we have $4 \times 16 \equiv 1 \mod 21$, since $5 \equiv -16 \mod 21$. That is, 16 is the inverse of 4 modulo 21. We multiply by 16 each side of:
$$4x + 9 \equiv 13 \mod 21,$$
leading to:
$$x + 9 \times 16 \equiv 16 \times 13 \mod 21,$$
that is:
$$x \equiv 16(13 - 9) \mod 21,$$
which finally yields: $x \equiv 1 \mod 21$.
2. We eliminate $y$ in order to solve for $x$ first. Multiplying $3x - y \equiv 10 \mod 21$ by 2 yields $6x - 2y \equiv 20 \mod 21$. Adding this equation side-by-side with $x + 2y \equiv 4 \mod 21$ yields $7x \equiv 3 \mod 21$. Since $3 \times 7 \equiv 0 \mod 21$, we have $0\,x \equiv 9 \mod 21$, which is false. Therefore, the input problem has no solutions for $x$ and consequently no solutions for $y$.
3. We apply the Chinese Remainder Theorem. We have $m = 3$, $n = 7$, $a = 2$, $b = 6$. We need $s$ and $t$ such that $s\,m + t\,n = 1$, hence we can choose $s = -2$ and $t = 1$. Then, we have
$$c \equiv a + (b - a)\,s\,m \equiv 2 + (6 - 2) \times -2 \times 3 \equiv 20 \mod 21.$$

**Problem 5 (Modular exponentiation)** When dealing with congruences, an important question is that of *modular exponentiation*, that is, computing an expression of the form $a^n \mod m$ where $a$ is an integer and $m, n$ are positive integers.

1. Assume that $n$ is even and at least equal to 2. Let $r$ be the remainder of the division of $a^{\frac{n}{2}}$ by $m$. Prove that we have $a^n \equiv r^2 \mod m$.

2. Assume that $n$ is odd and at least equal to 3. Let $r$ be the remainder of the division of $a^{\frac{n-1}{2}}$ by $m$. Prove that we have $a^n \equiv (ar^2) \mod m$.

3. Use the previous questions in order to compute $4^{43} \mod 60$ without using any computer.

**Solution 5**

1. Indeed, using Tutorial 6, we have

$$a^n \equiv a^{\frac{n}{2}} \times a^{\frac{n}{2}} \equiv r \times r \equiv r^2 \mod m.$$

2. Indeed, using again Tutorial 6, we have

$$a^n \equiv a^{\frac{n-1}{2}} \times a^{\frac{n-1}{2}} \times a \equiv r \times r \times a \equiv (ar^2) \mod m.$$

3. We have

$$\begin{array}{lcll}
4^{43} & \equiv & (4^{21})^2 4 \mod 60 & \text{applying}(2) \\
4^{43} & \equiv & ((4^{10})^2 4)^2 4 \mod 60 & \text{applying}(1) \\
4^{43} & \equiv & (((4^5)^2)^2 4)^2 4 \mod 60 & \text{applying}(1) \\
4^{43} & \equiv & ((((4^2)^2 4)^2)^2 4)^2 4 \mod 60 & \text{applying}(2) \\
4^{43} & \equiv & ((((16)^2 4)^2)^2 4)^2 4 \mod 60 & \text{using} 4^2 \equiv 16 \mod 60 \\
4^{43} & \equiv & (((16 \times 4)^2)^2 4)^2 4 \mod 60 & \text{using} 4^3 \equiv 4 \mod 60 \\
4^{43} & \equiv & (((4)^2)^2 4)^2 4 \mod 60 & \text{using} 4^2 \equiv 16 \mod 60 \\
4^{43} & \equiv & ((16)^2 4)^2 4 \mod 60 & \text{using} 4^3 \equiv 4 \mod 60 \\
4^{43} & \equiv & (4)^2 4 \mod 60 & \text{using} 4^3 \equiv 4 \mod 60xs \\
4^{43} & \equiv & 4 \mod 60. &
\end{array}$$

**Problem 6 (RSA)** Let us consider an RSA Public Key Crypto System. Alice selects 2 prime numbers: $p = 5$ and $q = 13$. Alice selects her public exponent $e = 7$ and sends it to Bob. Bob wants to send the message $M = 4$. to Alice.

1. Compute the product $n = p\,q$



$n = pq = 65.$

$de = 1 \mod (p-1)(q-1).$

$7d = 1 \mod 4 \times 12$

$C = M^7 \mod n$

$7d = 1 \mod 48.$

$C = M^7 \mod 65.$

$\boxed{d = 7}$

2. Is this choice for of $e$ valid here?

3. Compute $d$ , the private exponent of Alice.

$C = 4^7 \mod 65.$

4. Encrypt the plain-text $M$ using Alice public exponent. What is the resulting cipher-text $C$?

5. Verify that Alice can obtain $M$ from $C$, using her private decryption exponent.

**Solution 6**

1. We have $n = pq = 55$.

2. We have $\gcd(e, (p-1)(q-1)) = \gcd(3, 40) = 1$, hence $e = 3$ is a valid choice (note that 3 is a prime number, any way).

3. Alice's private exponent $d$ satisfies $de = 1 \mod (p-1)(q-1)$, hence $3d = 1 \mod 40$, which gives $d = 27$ since $3 \times 27 = 81 = 1 + 2 \times 40$.

4. Bob sends: $C = M^e \mod n = 4^3 \mod 55 = 64 \mod 55 = 9$.

5. Alice receives C and computes $C^d \mod n = 9^{27} \mod 55 = 4$. To compute $9^{27} \mod 55$ by hand, one can proceed as in the previous problem:

$$\begin{array}{lcll}
9^{27} & \equiv & (9^{13})^2 9 \mod 55 & \text{applying } (2) \\
9^{27} & \equiv & ((9^6)^2 9)^2 9 \mod 55 & \text{applying } (2) \\
9^{27} & \equiv & (((9^2)^2 9^2)^2 9)^2 9 \mod 55 & \text{applying } (1, 2) \\
9^{27} & \equiv & (((26)^2 9^2)^2 9)^2 9 \mod 55 & \text{using } 9^2 \equiv 26 \mod 55 \\
9^{27} & \equiv & ((16 \times 9^2)^2 9)^2 9 \mod 55 & \text{using } 26^2 \equiv 16 \mod 55 \\
9^{27} & \equiv & ((16 \times 26)^2 9)^2 9 \mod 55 & \text{using } 9^2 \equiv 26 \mod 55 \\
9^{27} & \equiv & ((31)^2 9)^2 9 \mod 55 & \text{using } 16 \times 26 \equiv 31 \mod 55 \\
9^{27} & \equiv & (26 \times 9)^2 9 \mod 55 & \text{using } 31^2 \equiv 26 \mod 55 \\
9^{27} & \equiv & (14)^2 9 \mod 55 & \text{using } (26 \times 9) \equiv 14 \mod 55 \\
9^{27} & \equiv & 31 \times 9 \mod 55 & \text{using } 14^2 \equiv 31 \mod 55 \\
9^{27} & \equiv & 4 \mod 55 & \text{using } 31 \times 9 \equiv 4 \mod 55
\end{array}$$

**Problem 7 (Functions and matrices)** Consider the set of ordered pairs $(x, y)$ where $x$ are $y$ are real numbers. Such a pair can be seen as a point in the plane equipped with Cartesian coordinates $(x, y)$.

1. For each of the following functions $F_1, F_2, F_3, F_4$, determine a $(2\times 2)$-matrix $A$ so that the point of coordinates $(x \quad y)$ is sent to the point $(x' \quad y')$ when we have

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} \tag{1}$$

where

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{2}$$

   (a) $F_1(x,y) = (y,x)$
   (b) $F_2(x,y) = (\frac{x+y}{2}, \frac{x+y}{3})$
   (c) $F_3(x,y) = (x,-y)$
   (d) $F_4(x,y) = F_1(F_3(x,y))$

2. Determine which of the above functions $F_1, F_2, F_3, F_4$ is injective? surjective? Justify your answer.

**Solution 7**

1. $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. If $(y_1, x_1) = (y_2, x_2)$ holds then we have $(x_1, y_1) = (x_2, y_2)$, hence $F_1$ is injective. $F_1$ is also surjective since we have $F_1^{-1}(x', y') = (y', x')$.

2. $A = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix}$. $F_2$ is not injective. Indeed, if $x = -y$ then $F_2(x,y) = (0,0)$; thus many points like $(1,-1)$, $(2-2)$ have the same image by $F_2$. $F_2$ is not injective. Indeed, for a point $(a,b)$ to have a pre-image by $F_2$, it must satisfy $3b = 2a$; thus many points like $(1,-1)$, $(2-2)$ do not have a pre-image by $F_2$.

3. $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. If $(x_1, -y_1) = (x_2, -y_2)$ holds then we have $(x_1, y_1) = (x_2, y_2)$, hence $F_3$ is injective. $F_3$ is also surjective since we have $F_3^{-1}(x', y') = (x', y')$.

4. We have $F_4(x,y) = F_1(F_3(x,y)) = (-y, x)$ and we have $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Since $F_1$ and $F_3$ are both injective, it follows that $F_4$ is injective as well. Similarly, since $F_1$ and $F_3$ are both surjective, it follows that $F_4$ is surjective as well.