Homework 6

1. **Chinese Remainder Theorem.** Let p and q be distinct prime number. Let $\alpha \in \{0, 1, \dots, p-1\}$ and $\beta \in \{0, 1, \dots, q-1\}$. Then, we have seen earlier that there exists an integer x such that it simultaneously satisfies $x = \alpha \mod p$ and $x = \beta \mod q$. For brevity, we shall refer to this as $x = (\alpha, \beta) \mod (p, q)$.

   In this problem, we shall prove a few interesting properties of the result and the fact that there exists a unique $x \in \{0, 1, \dots, N-1\}$, where $N = p\dot{q}$, that simultaneously satisfies the two equation.

   (a) (5 points) Suppose that the integers x and y satisfy $x = (\alpha, \beta) \mod (p, q)$ and $y = (\alpha', \beta') \mod (p, q)$. Prove that the integer $x - y = (\alpha - \alpha', \beta - \beta') \mod (p, q)$.

   Solution.

(b) (5 points) Suppose that the integers x and y satisfy $x = (\alpha, \beta) \mod (p, q)$ and $y = (\alpha', \beta') \mod (p, q)$. Prove that the integer $x \cdot y = (\alpha \cdot \alpha', \beta \cdot \beta') \mod (p, q)$.

Solution.

(c) (5 points) Suppose x and x' are integers such that $x = (\alpha, \beta) \mod (p, q)$ and $x' = (\alpha, \beta) \mod (p, q)$. Prove that N divides $(x - x')$, where $N = p \cdot q$.

Solution.

(d) (5 points) Prove that for every $\alpha \in \{0, 1, \ldots, p-1\}$ and $\beta \in \{0, 1, \ldots, q-1\}$ there exists a unique $x \in \{0, 1, \ldots, N-1\}$ such that $x = (\alpha, \beta) \mod (p, q)$.

Solution.

(e) (5 points) Prove that for every element $x \in \{0, 1 \ldots, N-1\}$ there exists unique (α, β) where $\alpha \in \{0, 1, \ldots, p-1\}$ and $\beta \in \{0, 1, \ldots, q-1\}$ such that $x = (\alpha, \beta) \bmod (p, q)$.

Solution.

2. **Proving $\mathbb{Z}_N^*$ is a group.** Let p and q be two prime numbers, and $N = p \cdot q$. Define

$$\mathbb{Z}_N^* = \left\{x \colon 0 \leqslant x < N, \gcd(x, N) = 1\right\}$$

Let $\times$ be integer multiplication $\mod N$. We shall prove that $(\mathbb{Z}_N^*, \times)$ is a group.

Our starting point is the result of Problem 1.e. that shows that every integer $x \in \{0, 1, \dots, N-1\}$ has a unique (α, β) associated with it, such that $\alpha \in \{0, \dots, p-1\}$, $\beta \in \{0, \dots, q-1\}$, and $x = (\alpha, \beta) \mod (p, q)$.

(a) (5 points) Prove that $x \in \mathbb{Z}_N^*$ if and only if $x = (\alpha, \beta) \mod (p, q)$, such that $\alpha \in \{1, \dots, p-1\}$ and $\beta \in \{1, \dots, q-1\}$. Remark: This result proves that $\left|\mathbb{Z}_N^*\right| = (p-1)(q-1)$. **Solution.**

(b) (5 points) (Closure) Suppose $x = (\alpha, \beta) \mod (p, q)$ and $y = (\alpha', \beta') \mod (p, q)$. Prove that $x \times y \in \mathbb{Z}_N^*$.

Solution.

(c) (8 points) (Existence of identity) Find an element $e \in \mathbb{Z}_N^*$ such that $e = (\alpha, \beta) \bmod (p, q)$ and for all $x \in \mathbb{Z}_N^*$ we have $e \times x = x$. (That is, e is the identity element)

Solution.

(d) (8 points) (Multiplicative Inverse) Suppose $x = (\alpha, \beta) \mod (p, q)$ and $x \in \mathbb{Z}_N^*$. What is the element $y \in \mathbb{Z}_N^*$ such that $x \times y = e$? **Solution.**

3. **An Observation about Solving Equations.** Let p and q be distinct primes, and $N = p \cdot q$. Suppose there exists one solution $x \in \{0, 1, \dots, N-1\}$ such that $x^2 = a \mod N$. Define

$$S(a) = \Big\{ X \colon X \in \{0, 1, \dots, N-1\}, X^2 = a \mod N \Big\}$$

That is, $S(a)$ is the set of all solutions of $X^2 = a \mod N$, where $X \in \{0, 1, \dots, N-1\}$.

(a) (8 points) If $a \in \mathbb{Z}_N^*$ then prove that $\big| S(a) \big| = 4$.
Solution.

(b) (8 points) If a is divisible by p or q, then prove that we have $\left|S(a)\right| = 2$.

Solution.

(c) (8 points) If $a = 0$, then prove that we have $\left|S(a)\right| = 1$.

Solution.

4. **Proving Bijection of X^i.** (25 points) Suppose p and q are primes, and $N = p \cdot q$. We define $\times$ as integer multiplication $\mod N$. The objective of this problem is to prove that the function $X^i \colon \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ is a bijection, if i is relatively prime to $(p-1)$ and $(q-1)$.

   Suppose $X \in \mathbb{Z}_N^*$ such that $X = (\alpha, \beta) \mod (p, q)$, $\alpha \in \mathbb{Z}_p^*$, and $\beta \in \mathbb{Z}_q^*$. Suppose Y is a different element $\in \mathbb{Z}_N^*$ such that $Y = (\gamma, \delta) \mod (p, q)$.

   If possible let i be relatively prime to $(p-1)$ and $(q-1)$, and $X^i = Y^i$. If this condition is true, then we have $(\alpha^i, \beta^i) = (\gamma^i, \delta^i) \mod (p, q)$. This statement is equivalent to $0 = (\alpha^i - \gamma^i, \beta^i - \delta^i) \mod (p, q)$. By problem 3.c. we know that this equation has a unique solution $\alpha^i = \gamma^i \mod p$ and $\beta^i = \delta^i \mod q$.

   Now, all that remains is to prove the following result. Suppose α, γ are distinct elements in $\mathbb{Z}_p^*$. If $\gcd(i, p-1) = 1$, then it is impossible to have $\alpha^i = \gamma^i \mod p$. In your proof, you can assume that $\mathbb{Z}_p^* = \{g^0, g^1, \ldots, g^{p-2}\}$, for some $g \in \mathbb{Z}_p^*$.

   Solution.

Collaborators :