MATHEMATICS 271 L01 FALL 2007
ASSIGNMENT 5 SOLUTION

1. Let $f : A \to B$ be a function and let $\mathcal{S}$ be a relation on B. Let $\mathcal{R}$ be the relation on A defined by "For all $x, y \in A$, $(x, y) \in \mathcal{R}$ if and only if $(f(x), f(y)) \in \mathcal{S}$." Prove or disprove each of the following statement.

(a) If $\mathcal{S}$ is an equivalence relation on B then $\mathcal{R}$ is an equivalence relation on A.

Solution:

The statement is true. Suppose that $\mathcal{S}$ is an equivalence relation on B. We prove that $\mathcal{R}$ is an equivalence relation on A.

First, we prove that $\mathcal{R}$ is reflexive. Let $x \in A$. Since $f(x) \in B$ and $\mathcal{S}$ is reflexive on B, we have $f(x) \mathcal{S} f(x)$ and so $x \mathcal{R} x$.

Next, we prove that $\mathcal{R}$ is symmetric. Let $x, y \in A$ and suppose that $x \mathcal{R} y$. Since $x \mathcal{R} y$, $f(x) \mathcal{S} f(y)$, and by symmetry of $\mathcal{S}$, we get $f(y) \mathcal{S} f(x)$, and so $y \mathcal{R} x$.

Lastly, we prove that $\mathcal{R}$ is transitive. Let $x, y, z \in A$ and suppose that $x \mathcal{R} y$ and $y \mathcal{R} z$. Since $x \mathcal{R} y$ and $y \mathcal{R} z$, $f(x) \mathcal{S} f(y)$ and $f(y) \mathcal{S} f(z)$ and by transitivity of $\mathcal{S}$, we get $f(x) \mathcal{S} f(z)$, and so $x \mathcal{R} z$.

Since $\mathcal{R}$ is reflexive, symmetric and transitive, $\mathcal{R}$ is an equivalence relation on A.

(b) If $\mathcal{R}$ is an equivalence relation on A then $\mathcal{S}$ is an equivalence relation on B.

Solution:

The statement is false. For example, let $A = \{1\}$, $B = \{1, 2\}$, $f = \{(1, 1)\}$ and $\mathcal{S} = \{(1, 1)\}$. Then $\mathcal{R} = \{(1, 1)\}$ is an equivalence relation on A, but $\mathcal{S}$ is not an equivalence relation on B since it is not reflexive (for $(1, 1) \notin \mathcal{S}$).

(c) If $\mathcal{S}$ is antisymmetric then $\mathcal{R}$ is antisymmetric.

Solution:

The statement is false. For example, let $A = \{1, 2\}$, $B = \{1\}$, $f = \{(1, 1)\}$ and $\mathcal{S} = \{(1, 1)\}$. Then $\mathcal{R} = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$. We note that $\mathcal{S}$ is antisymmetric but $\mathcal{R}$ is not antisymmetric since $1 \mathcal{R} 2$ and $2 \mathcal{R} 1$ but $1 \neq 2$.

(d) If f is one-to-one and $\mathcal{S}$ is antisymmetric then $\mathcal{R}$ is antisymmetric.

Solution:

The statement is true. Suppose that f is one-to-one and $\mathcal{S}$ is antisymmetric. We prove that $\mathcal{R}$ is antisymmetric. Let $x, y \in A$ and suppose that $x \mathcal{R} y$ and $y \mathcal{R} x$. Since $x \mathcal{R} y$ and $y \mathcal{R} x$, $f(x) \mathcal{S} f(y)$ and $f(y) \mathcal{S} f(x)$ and by antisymmetry of $\mathcal{S}$, we get $f(x) = f(y)$, and since f is one-to-one we get $x = y$. Thus, $\mathcal{R}$ is antisymmetric.

2. Let $n \geq 1$ be an integer. Let $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and $a \in \mathbb{Z}$. Let $\mathcal{R}$ be the relation on A defined by "For all $x, y \in A$, $(x, y) \in \mathcal{R}$ if and only if $ax \equiv ay \pmod{n}$."

(a) Prove that $\mathcal{R}$ is an equivalence relation on A. Note that you may want to use some result in question 1.

Solution:

The relation $\mathcal{R}$ can be defined as "For all $x, y \in A$, $(x, y) \in \mathcal{R}$ if and only if $(f(x), f(y)) \in \mathcal{S}$." where $f(x) = ax$ and $\mathcal{S}$ is the relation "congruence modulo n" which is an equivalence relation on $\mathbb{Z}$. Then by part (a) in question 1, since $\mathcal{S}$ is an equivalence relation on $\mathbb{Z}$, $\mathcal{R}$ is an equivalence relation on A.

(b) Let $n = 3$ and $a = 2$. Describe the equivalence classes of $\mathcal{R}$.

Solution:

When $n = 3$ and $a = 2$, the equivalence classes of $\mathcal{R}$ are $\{1, 4, 7, 10\}$, $\{2, 5, 8\}$ and $\{3, 6, 9\}$.

(c) Let $n = 4$ and $a = 2$. Describe the equivalence classes of $\mathcal{R}$.

Solution:

When $n = 4$ and $a = 2$, the equivalence classes of $\mathcal{R}$ are $\{1, 3, 5, 7, 9\}$ and $\{2, 4, 6, 8, 10\}$..

(d) Find some integers n and a so that $\mathcal{R}$ has exactly 5 equivalence classes.

Solution:

When $n = 5$ and $a = 1$, the five equivalence classes of $\mathcal{R}$ are $\{1, 6\}$, $\{2, 7\}$, $\{3, 8\}$, $\{4, 9\}$ and $\{5, 10\}$.

(e) Prove that for all positive integer n, there exists an integer a so that $\mathcal{R}$ has exactly 1 equivalence class.

Solution: Let n be any positive integer. Let $a = 0$. Then for any $x \in A$, $x\mathcal{R}y$ because $0x \equiv 0y \pmod{n}$. Thus $R = A \times A$ and hence $\mathcal{R}$ has exactly 1 equivalence class namely A.

3. Let $n \geq 1$ be an integer. Let $a, b, c, d \in \mathbb{Z}$.

(a) Prove that if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$ then $ab \equiv cd \pmod{n}$.

Solution:

Suppose that $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, that is, $n \mid (a - c)$ and $n \mid (b - d)$, and so there exists integers p and q so that $a - c = np$ and $b - d = nq$. Then $ab - cd = a(b - d) + d(a - c) = anp + dnq = n(ap + dq)$ which implies $n \mid (ab - cd)$ and hence $ab \equiv cd \pmod{n}$.

(b) Prove that if b is an inverse of a modulo n, and $k = b \bmod n$ then k is an inverse of a modulo n.

Solution:

Suppose that b is an inverse of a modulo n, and $k = b \bmod n$, that is $ab \equiv 1 \pmod{n}$. Since $k = b \bmod n$, $k \equiv b \pmod{n}$. We note that since congruence modulo n is reflexive, we have $a \equiv a \pmod{n}$. Since $k \equiv b \pmod{n}$ and $a \equiv a \pmod{n}$, from part (a) we get

$ak \equiv ab \pmod{n}$. Now, since $ak \equiv ab \pmod{n}$ and $ab \equiv 1 \pmod{n}$, by transitivity of congruence modulo n, $ak \equiv 1 \pmod{n}$ and hence k is an inverse of a modulo n.

(c) Use Euclid's Algorithm to find $\gcd(2007, 271)$, and find integers x and y so that $\gcd(2007, 271) = 2007x + 271y$.

Solution:

$$\begin{aligned} 2007 &= 7 \times 271 + 110 \\ 271 &= 2 \times 110 + 51 \\ 110 &= 2 \times 51 + 8 \\ 51 &= 6 \times 8 + 3 \\ 8 &= 2 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

and

2007	1	0
271	0	1
110	1	−7
51	−2	15
8	5	−37
3	−32	237
2	69	−511
1	−101	748

Thus, $\gcd(2007, 271) = 1 = 2007x + 271y$ where $x = -101$ and $y = 748$.

(d) Use the result in part (c) to find an inverse of 271 modulo 2007.

Solution:

From part (c), we have $2007 \times (-101)\, x + 271 \times 748 = 1$, and so $271 \times 748 - 1 = 2007 \times 101$, that is, $2007 \mid (271 \times 748 - 1)$ which implies $271 \times 748 \equiv 1 \pmod{n}$ and therefore, an inverse of 271 modulo 2007 is 748.

(e) Find an integer m so that $1 \leq m < 2007$ so that m is an inverse of 271 modulo 2007.

Solution: $m = 748$ as seen in part (d).