MATH 273 Assignment 2

Instructor: Thi Ngoc Dinh
UCID: 30063828

Fall 2018

1

a Use the Euclidean Algorithm to find $gcd(65, 18)$ and use that to find integers x and y so that $gcd(65, 18) = 65x + 18y$.

From Euclidean Algorithm: If $a = qb + r$ where $a, q, b, r \in \mathbb{Z}$. Then $gcd(a, b) = gcd(b, r)$.

a	q	b	r
65	3	18	11
18	1	11	7
11	1	7	4
7	1	4	3
4	1	3	1
3	3	1	0

$gcd(65, 18) = 1$.

x	y	65x+19y
1	-3	11
-1	4	7
2	-7	4
-3	11	3
5	-18	1

$gcd(65, 18) = 1 = 65(5) \times 18(-18)$.

b Is it true that for all integers $a, b,$ and c, if $a \mid bc$ then $a \mid b$ or $a \mid c$? Prove your answer.

It is true. Proof by contradiction: Suppose $a, b, c \in \mathbb{Z}$, such that $a \mid bc$ and $a \nmid b$ and $a \nmid c$. This means $b = ad+i$ and $c = ae+j$ where $d, e, i, j \in \mathbb{Z}$ and $a \nmid i$ and $a \nmid j$. So $bc = (ad+i)(ae+j) = a^2de+iae+jad+ij = a(ade + ie + jd) + ij$. Because $(ade + ie + jd), ij \in \mathbb{Z}$ and $a \nmid ij$, $a \nmid bc$ as $bc = a(ade + ie + jd) + ij$. Which contradicts the assumption that $a \mid bc$. Therefore the statement can not be false.

c Is it true that for all integers x, if $18 \mid 65x$ then $18 \mid x$? Prove your answer.

It is true. Proof: Let $a = 18, b = 65$ and $c = x$ where $c, x \in \mathbb{Z}$, such that $a \mid bc$. Because $18 \nmid 65, a \nmid b$. From 1.(b): $\forall a, b, c \in \mathbb{Z}$ if $a \mid bc$ then $a \mid b$ or $a \mid c$. $a \mid c$ because $a \nmid b$. So $18 \mid x$.

d Is it true that for all integers $a, b,$ and c, if $a \mid bc$ and $gcd(a, b) = 1$ then $a \mid c$? Prove your answer.

It is true. Proof: Let $a, b, c \in \mathbb{Z}$ so that $a \mid bc$ and $gcd(a, b) = 1$. Case 1: $a \nmid b$ Then $a \mid c$ because $a \mid bc$ and becasue 1.is true. Case 2: $a \mid b$ If $a \mid b$ then $gcd(a, b) = a$ since $b = da + 0$ where $d \in \mathbb{Z}$, so $gcd(a, b) = gcd(a, 0) = a$ for $a \neq 0$. Because $a \mid b$ and $gcd(a, b) = 1$, $a = 1$. $1 \mid c, \forall c \in \mathbb{Z}$. So $a \mid c$. Therefore $a \mid c$ in all cases.

2 Let $\mathbb{Z}^+$ be the set of all positive integers and let R be the relation on $\mathbb{Z}^+ \times \mathbb{Z}^+$ defined by: For any $(a, b), (c, d) \in \mathbb{Z}^+ \times \mathbb{Z}^+, (a, b)R(c, d)$ if and only if $a + 2b = c + 2d$.

a Prove that R is an equivalence relation on $\mathbb{Z}^+ \times \mathbb{Z}^+$.

Proof for Reflictive: Let $(a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+$. $a + 2b = a + 2b$, so $(a, b)R(a, b)$.
Proof for Symmetric: Let $(a, b), (c, d) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ such that $(a, b)R(c, d)$. $c+2d = a+2b$ because $a+2b = c+2d$. So $(c, d)R(a, b)$.
Proof for Transitive: Let$(a, b), (c, d), (e, f) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ such that $(a, b)R(c, d)$ and $(c, d)R(e, f)$. $a+2b = c+2d$ because $(a, b)R(c, d)$. $c + 2d = e + 2f$ because $(c, d)R(e, f)$. $a + 2b = c + 2d = e + 2f$, so $(a, b)R(e, f)$. R is an equivalence relation because it is reflecctive, symmetric and transitive.

b List all elements of $[(3, 3)]$, the equivalence class of $(3, 3)$.

$[(1, 4), (3, 3), (5, 2), (7, 1)]$

c Is there an equivalence class that has exactly 13 elements? If there is one, list all elements of that class.

Yes. $[(1, 13), (3, 12), (5, 11), (7, 10), (9, 9), (11, 8), (13, 7), (15, 6), (17, 5), (19, 4), (21, 3), (23, 2), (25, 1)]$

d Is there an equivalence class that has exactly 273 element? Prove your answer.

Yes. $\forall n \in \mathbb{Z}^+, \exists$ an equivalence class of size n for the relation R. Proof: Let $x \in \mathbb{Z}^+$, choose (1,x). The equivalence class of (1,x) has the size of x. Proof by example: [(1, 273), (3, 272), (5, 271), (7, 270), (9, 269), (11, 268), (13, 267), (15, 266), (17, 265), (19, 264), (21, 263), (23, 262), (25, 261), (27, 260), (29, 259), (31, 258), (33, 257), (35, 256), (37, 255), (39, 254), (41, 253), (43, 252), (45, 251), (47, 250), (49, 249), (51, 248), (53, 247), (55, 246), (57, 245), (59, 244), (61, 243), (63, 242), (65, 241), (67, 240), (69, 239), (71, 238), (73, 237), (75, 236), (77, 235), (79, 234), (81, 233), (83, 232), (85, 231), (87, 230), (89, 229), (91, 228), (93, 227), (95, 226), (97, 225), (99, 224), (101, 223), (103, 222), (105, 221), (107, 220), (109, 219), (111, 218), (113, 217), (115, 216), (117, 215), (119, 214), (121, 213), (123, 212), (125, 211), (127, 210), (129, 209), (131, 208), (133, 207), (135, 206), (137, 205), (139, 204), (141, 203), (143, 202), (145, 201), (147, 200), (149, 199), (151, 198), (153, 197), (155, 196), (157, 195), (159, 194), (161, 193), (163, 192), (165, 191), (167, 190), (169, 189), (171, 188), (173, 187), (175, 186), (177, 185), (179, 184), (181, 183), (183, 182), (185, 181), (187, 180), (189, 179), (191, 178), (193, 177), (195, 176), (197, 175), (199, 174), (201, 173), (203, 172), (205, 171), (207, 170), (209, 169), (211, 168), (213, 167), (215, 166), (217, 165), (219, 164), (221, 163), (223, 162), (225, 161), (227, 160), (229, 159), (231, 158), (233, 157), (235, 156), (237, 155), (239, 154), (241, 153), (243, 152), (245, 151), (247, 150), (249, 149), (251, 148), (253, 147), (255, 146), (257, 145), (259, 144), (261, 143), (263, 142), (265, 141), (267, 140), (269, 139), (271, 138), (273, 137), (275, 136), (277, 135), (279, 134), (281, 133), (283, 132), (285, 131), (287, 130), (289, 129), (291, 128), (293, 127), (295, 126), (297, 125), (299, 124), (301, 123), (303, 122), (305, 121), (307, 120), (309, 119), (311, 118), (313, 117), (315, 116), (317, 115), (319, 114), (321, 113), (323, 112), (325, 111), (327, 110), (329, 109), (331, 108), (333, 107), (335, 106), (337, 105), (339, 104), (341, 103), (343, 102), (345, 101), (347, 100), (349, 99), (351, 98), (353, 97), (355, 96), (357, 95), (359, 94), (361, 93), (363, 92), (365, 91), (367, 90), (369, 89), (371, 88), (373, 87), (375, 86), (377, 85), (379, 84), (381, 83), (383, 82), (385, 81), (387, 80), (389, 79), (391, 78), (393, 77), (395, 76), (397, 75), (399, 74), (401, 73), (403, 72), (405, 71), (407, 70), (409, 69), (411, 68), (413, 67), (415, 66), (417, 65), (419, 64), (421, 63), (423, 62), (425, 61), (427, 60), (429, 59), (431, 58), (433, 57), (435, 56), (437, 55), (439, 54), (441, 53), (443, 52), (445, 51), (447, 50), (449, 49), (451, 48), (453, 47), (455, 46), (457, 45), (459, 44), (461, 43), (463, 42), (465, 41), (467, 40), (469, 39), (471, 38), (473, 37), (475, 36), (477, 35), (479, 34), (481, 33), (483, 32), (485, 31), (487, 30), (489, 29), (491, 28), (493, 27), (495, 26), (497, 25), (499, 24), (501, 23), (503, 22), (505, 21), (507, 20), (509, 19), (511, 18), (513, 17), (515, 16), (517, 15), (519, 14), (521, 13), (523, 12), (525, 11), (527, 10), (529, 9), (531, 8), (533, 7), (535, 6), (537, 5), (539, 4), (541, 3), (543, 2), (545, 1)]

3 Let $A = \{1, 2, 3, 4\}$. Let $\mathcal{F}$ be the set of all functions from A to A. Let R be the relation on $\mathcal{F}$ defined by: For any $f, g \in \mathcal{F}, fRg$ if and only if $f(i) = g(i)$ for some $i \in A$.

a Is R reflictive? symmetric? transitive? Prove your answer.

It is reflictive. Proof: Let $f \in \mathcal{F}$. Let $i \in A$. $f(i) = f(i)$.
It is symmetric. Proof: Let $f, g \in \mathcal{F}$ such that fRg. Let $i \in A$. $g(i) = f(i)$ because $f(i) = g(i)$, so gRf.
It is transitive. Proof: Let $f, g, h \in \mathcal{F}$ such that fRg, gRh. Let $i \in A$. $f(i) = g(i)$ because fRg. $g(i) = h(i)$ because gRh. $f(i) = g(i) = h(i)$, so fRh

b Is it true that for all functions $f \in \mathcal{F}$, there exists a function $g \in \mathcal{F}$ so that fRg? Prove your answer.

Yes. Proof: Let $f \in \mathcal{F}$. Choose $g = f$. Becasue R is reflective from 3.(a), fRg.

c Is it true that there exists a function $g \in \mathcal{F}$ so that for all functions $f \in \mathcal{F}, fRg$? Prove your answer.

No. Proof by contradiction: Suppose $\exists g \in \mathcal{F}$ so that $\forall f \in \mathcal{F}, fRg$. Because R is reflective, symmetric, and transitive from 3.(a), it is an equivalence relation. Because $\forall f \in \mathcal{F}, fRg$ and R is an equivalence relation, R has only one equivalence class. Let $i \in A$. Let $h, p \in \mathcal{F}$, defined as: $h(i) = 1, p(i) = 2$. $h(i) = 1 \neq 2 = g(i)$, therefore $(h, g) \notin R$. This means R has more then one equivalence class. This contradicts the fact that it has only one equivalence class. Therefore the assumption cannot be true, and there exists no such g.