# MA014G
# Algebra and Discrete Mathematics
# Suggested Solutions to Assignment 4

**Question 1**

(a) (i) $R$ is reflexive if $(a, a) \in R$ for all $a \in S$;

(ii) $R$ is symmetric if whenever $(a, b) \in R$ then $(b, a) \in R$ also, for all $a, b \in S$;

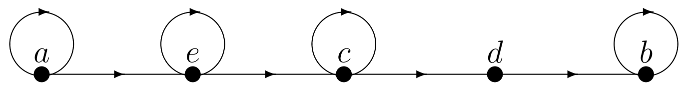
(iii) $R$ is transitive if whenever $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$ also, for all $a, b, c \in S$;

(iv) $R$ is anti-symmetric if whenever both $(a, b) \in R$ and $(b, a) \in R$ then $a = b$, for all $a, b \in S$.

(b) $R$ is the following relation on $S = \{a, b, c, d, e\}$.

$$R = \{(a, a),\ (b, b),\ (c, c),\ (e, e),\ (a, e),\ (e, c),\ (d, b),\ (c, d)\}$$

(i) It has the relation digraph




(ii) To make $R$ symmetric you have to add the following set of pairs:

$$R = \{(e, a),\ (c, e),\ (d, c),\ (b, d)\}.$$

(iii) To make $R$ reflexive, you have to add the following set of pairs:

$$\{(d, d)\}.$$

(iv) To make $R$ transitive, first notice that you have to add $(a, c)$ as $(a, e) \in R$ and $(e, c) \in R$. Next you have to add $(a, d)$ as $(a, c) \in R$ and $(c, d) \in R$. Then you have to add $(a, b)$ as $(a, d) \in R$ and $(d, b) \in R$. Similarly you have to add $(e, d)$, $(e, b)$ and $(c, b)$. Hence the set of pairs which has to be added is

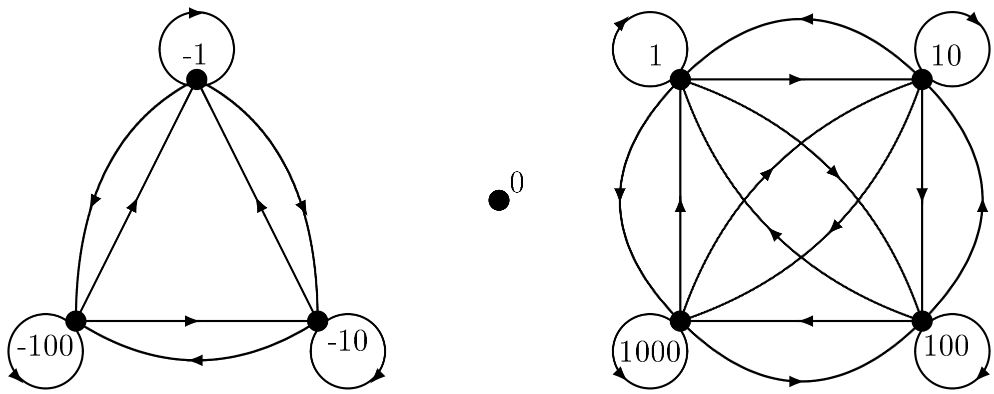
$$\{(a, c),\ (a, d),\ (a, b),\ (e, d),\ (e, b),\ (c, b)\}.$$

(v) The relationen $R$ is anti-symmetric as the relation digraph has no 'double-arrows' between any pair of distinct points, i.e. $(x, y) \in R$ and $(y, x) \in R$ only when $x = y$.

**Question 2**

(a) $R = \{(1000, 1000),\ (1000, 100),\ (1000, 10),\ (1000, 1),$
$(100, 1000),\ (100, 100),\ (100, 10),\ (100, 1),$
$(10, 1000),\ (10, 100),\ (10, 10),\ (10, 1),$
$(1, 1000),\ (1, 100),\ (1, 10),\ (1, 1),$
$(-1, -1),\ (-1, -10),\ (-1, -100),$
$(-10, -1),\ (-10, -10),\ (-10, -100),$
$(-100, -1),\ (-100, -10),\ (-100, -100)\}$

(b) The relation digraph, of the relation $R$ on $X = \{-100, -10, -1, 0, 1, 10, 100, 1000\}$ defined by $(x, y) \in R$ if $xy > 0$, is




(c) No, $R$ is not an equivalence relation as $(0, 0) \notin R$ so $R$ is not reflexive.

**Question 3**

(a) The multiplication table for $\mathbb{Z}_{12}$ is:

| $\odot$ | [0] | [1] | [2] | [3] | [4] | [5] | [6] | [7] | [8] | [9] | [10] | [11] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [0] | [0] | [0] | [0] | [0] | [0] | [0] | [0] | [0] | [0] | [0] | [0] | [0] |
| [1] | [0] | [1] | [2] | [3] | [4] | [5] | [6] | [7] | [8] | [9] | [10] | [11] |
| [2] | [0] | [2] | [4] | [6] | [8] | [10] | [0] | [2] | [4] | [6] | [8] | [10] |
| [3] | [0] | [3] | [6] | [9] | [0] | [3] | [6] | [9] | [0] | [3] | [6] | [9] |
| [4] | [0] | [4] | [8] | [0] | [4] | [8] | [0] | [4] | [8] | [0] | [4] | [8] |
| [5] | [0] | [5] | [10] | [3] | [8] | [1] | [6] | [11] | [4] | [9] | [2] | [7] |
| [6] | [0] | [6] | [0] | [6] | [0] | [6] | [0] | [6] | [0] | [6] | [0] | [6] |
| [7] | [0] | [7] | [2] | [9] | [4] | [11] | [6] | [1] | [8] | [3] | [10] | [5] |
| [8] | [0] | [8] | [4] | [0] | [8] | [4] | [0] | [8] | [4] | [0] | [8] | [4] |
| [9] | [0] | [9] | [6] | [3] | [0] | [9] | [6] | [3] | [0] | [9] | [6] | [3] |
| [10] | [0] | [10] | [8] | [6] | [4] | [2] | [0] | [10] | [8] | [6] | [4] | [2] |
| [11] | [0] | [11] | [10] | [9] | [8] | [7] | [6] | [5] | [4] | [3] | [2] | [1] |

(b) From the table in (a) you can see that the equation $[8] \odot [x] = [4]$ has the four solutions $[x] = [2], [x] = [5], [x] = [8]$ and $[x] = [11]$ in $\mathbb{Z}_{12}$.

(c) From the table in (a) you can see that the equation $[8] \odot [x] = [2]$ has no solutions in $\mathbb{Z}_{12}$.

**Uppgift 4**

In Question 3 of Assignment 3 we found that $\gcd(3571, 1753) = 1$ and that

$$1 = (-863) \cdot 3571 + (1758) \cdot 1753,$$

so the multiplicative inverse of $[1753] \in \mathbb{Z}_{3571}$ is $[1758]$ and the equation has precisely one solution in $\mathbb{Z}_{3571}$, which you can find by multiplying the equation through by $[1758]$ to get

$$[x] = [1758] \odot [3] = [5274] = [1703].$$

**Uppgift 5**

(a) To solve the equation $[14] \odot [x] = [4]$ in $\mathbb{Z}_{150}$:

(i) $\gcd(14, 150) = 2$, so there are two solutions in $\mathbb{Z}_{150}$ and we need to solve the reduced equation $[7] \odot [x] = [2]$ in $\mathbb{Z}_{75}$.

(ii) Now the multiplicative inverse of $[7]$ in $\mathbb{Z}_{75}$ is $[43]$ as $43 \times 7 = 301$. Hence the reduced equation has the solution

$$[x] = [43] \odot [2] = [86] = [11] \text{ in } \mathbb{Z}_{75},$$

(iii) and the original equation has the two solutions

$$[x] = [11] \text{ and } [x] = [86] \text{ in } \mathbb{Z}_{150}.$$

(b) To solve the equation $[14] \odot [x] = [4]$ in $\mathbb{Z}_{151}$:

(i) We use Euclid's algorithm to find $\gcd(14, 151)$ :

$$\begin{aligned}
151 &= 10 \cdot 14 + 11; \\
14 &= 1 \cdot 11 + 3; \\
11 &= 3 \cdot 3 + 2; \\
3 &= 1 \cdot 2 + 1; \\
2 &= 2 \cdot 1 + 0.
\end{aligned}$$

Hence $\gcd(151, 14) = 1$ because the last non-zero remainder is 1.

This means that the equation has precisely one solution in $\mathbb{Z}_{151}$ and the reduced equation is the same as the original equation.

(ii) To find the multiplicative inverse of $[14]$ in $\mathbb{Z}_{151}$, work backwards through Euclid's algorithm to find

$$\begin{aligned}
1 &= 3 - 2 = 3 - (11 - 3 \cdot 3) = 4 \cdot 3 - 11 \\
&= 4(14 - 11) - 11 = 4 \cdot 14 - 5 \cdot 11 \\
&= 4 \cdot 14 - 5(151 - 10 \cdot 14) \\
&= 54 \cdot 14 + (-5)151
\end{aligned}$$

so the multiplicative inverse of $[14] \in \mathbb{Z}_{151}$ is $[54]$. Hence the equation has the solution

$$[x] = [54] \odot [4] = [216] = [65] \text{ in } \mathbb{Z}_{151}.$$