Problem Set 3 Solutions

Problem 1. **(a)**

$$\begin{aligned} 1386 &= 294 \cdot 4 + 210 \\ 294 &= 210 \cdot 1 + 84 \\ 210 &= 84 \cdot 2 + 42 \\ 84 &= 42 \cdot 2 \end{aligned}$$

Hence, $\gcd(1386, 294) = 42$, since 42 is the last nonzero remainder.

(b)

$$\begin{aligned} 42 &= 210 - 84 \cdot 2 \\ 42 &= 210 - (294 - 210 \cdot 1) \cdot 2 \\ 42 &= 3 \cdot 210 - 2 \cdot 294 \\ 42 &= 3 \cdot (1386 - 294 \cdot 4) - 2 \cdot 294 \\ 42 &= 3 \cdot 1386 - 14 \cdot 294 \end{aligned}$$

(c) By Theorem 5 in section 2.3 of Rosen:

$1386 \cdot 294 = \gcd(1386, 294) \cdot \mathrm{lcm}(1386, 294) \longrightarrow \mathrm{lcm}(1386, 294) = (1386 \cdot 294)/42 = 9702$

Problem 2. **(a)** Let $x > y \geq 0$. We want to show $x' + y' \leq \frac{3}{4}(x+y)$, where $x' = y$, and $y' = x \bmod y$, when the Euclidean algorithm calls itself on new arguments x' and y'. Let $x = qy + y'$, for q a positive integer. Then we have the following:

Proof. (By contradiction): Suppose $(y + y') > \frac{3}{4}(x+y)$. Then:

$$\begin{aligned} (y + y') &> \frac{3}{4}x + \frac{3}{4}y \\ &= \frac{3}{4}(qy + y') + \frac{3}{4}y \quad \longrightarrow \\ \frac{1}{4}y' &> \frac{3}{4}qy - \frac{1}{4}y \quad \longrightarrow \\ y' &> (3q - 1)y \\ &> y \qquad \text{since } q \text{ is a positive integer} \end{aligned}$$

Contradiction! y' cannot be $> y$, since $y' = x \bmod y$. ∎

(b) Let s_n be the sum of the divisor and the dividend after the Euclidean algorithm makes n recursive calls, when computing $\gcd(x, y)$. We prove by induction on n that: $s_n \leq (\frac{3}{4})^n(x+y)$.

Proof. (By Induction):
Basis Case: Clearly it is true for $n = 1$, since we proved in part (a) that $s_1 = y + (x \bmod y) \leq (\frac{3}{4})(x+y)$.
Inductive Case: Suppose $s_k \leq (\frac{3}{4})^k(x+y)$ for $1 \leq k \leq n$. We show $s_{n+1} \leq (\frac{3}{4})^{n+1}(x+y)$:

$$\begin{aligned} s_{n+1} &\leq (\frac{3}{4})s_n && \text{by part (a)} \\ &\leq (\frac{3}{4})(\frac{3}{4})^n(x+y) && \text{by the induction hypothesis} \\ &\leq (\frac{3}{4})^{n+1}(x+y) \end{aligned}$$

The smallest value s_n can take is 1. Hence, we have:

$$1 \leq (\frac{3}{4})^n(x+y) \longrightarrow (\frac{4}{3})^n \leq (x+y) \longrightarrow n \leq \log_{4/3}(x+y).$$

■

Problem 3. Translating the letters into numbers we have `0019 1900 0210`. Thus we need to compute $C = P^e \bmod n = P^{13} \bmod 43 \cdot 59 = P^{13} \bmod 2537$ for $P = 19$, $P = 1900$ and $P = 210$. The results of these calcualtions, done by fast modular multiplicaiton or a computer algebra system are 2299, 1317, and 2117, respectively. Thus the encrypted message is `2299 1317 2117`.

Problem 4. **(a)** It is possible to jump to a square if its x and y coordinates can be expressed as linear combinations of the pairs $(12, 15)$ and $(9, 12)$ respectively. That is, if we can write $x = 15a + 12b$, and $y = 12c + 9d$, for integers a, b, c, d. Furthermore, $3 = \gcd(15, 12) = 15\hat{a} + 12\hat{b}$ for some integers $\hat{a}$ and $\hat{b}$, and $3 = \gcd(12, 9) = 12\hat{c} + 9\hat{d}$ for some integers $\hat{c}$ and $\hat{d}$. Hence, $15a + 12b$ and $12c + 9d$, represent all multiples of 3. So we can always jump to any square whose x and y coordinates are multiples of 3.

(b) Let x and y denote the coordinates of the number of the square that the referee call out. Then we have the following cases:

- If $x > 0$, jump 15 squares east, then 12 squares west. Repeat this procedure $x/3$ times.

- If $x < 0$, jump 15 squares west, then 12 squares east. Repeat this procedure $|x/3|$ times.
- If $x = 0$, no jump is allowed in either east or west direction.
- If $y > 0$, jump 12 squares north, then 9 squares south. Repeat this procedure $y/3$ times.
- If $y < 0$, jump 12 squares south, then 9 squares north. Repeat this procedure $|y/3|$ times.
- If $y = 0$, no jump is allowed in either north or south direction.

Problem 5. **(a)** Set identity.

Proof. We show that each set is a subset of the other as follows:
$\emptyset \subseteq (A - B) \cap (B - C)$, since by definition, $\emptyset$ is a subset of every set.
Also:

$$\begin{aligned}(A - B) \cap (B - C) &= \{x | x \in (A - B) \wedge x \in (B - C)\} \\ &= \{x | x \notin B \wedge x \in B\} \\ &= \{x | x \in \overline{B} \wedge x \in B\} \\ &= \emptyset\end{aligned}$$

■

(b) Not a set identity. We provide the following counterexample:
Let $A = \{1, 2, 3, 4\}$, $B = \{3, 5, 9\}$, and $C = \{1, 4, 5, 7\}$. Then:

$$\begin{aligned}(B - A) \cup (C - A) &= \{5, 9\} \cup \{5, 7\} \\ &= \{5, 7, 9\}\end{aligned}$$

But:

$$\begin{aligned}(B - (C \cup A)) \cup (C - (B \cup A)) &= \{9\} \cup \{7\} \\ &= \{7, 9\}\end{aligned}$$

(c) Set identity. We prove this by constructing the following truth table:

A	B	C	A⊕B	B⊕C	(A⊕B)⊕C	A⊕(B⊕C)
1	1	1	0	0	1	1
1	1	0	0	1	0	0
1	0	1	1	1	0	0
0	1	1	1	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	1	1
0	0	1	0	1	1	1
0	0	0	0	0	0	0

(d) Set identity. We show each set is a subset of the other as follows:

$$\begin{aligned}
&(A \cap B) \times (B \cap C) \\
&= \{(x, y) | x \in (A \cap B) \wedge y \in (B \cap C)\} \\
&= \{(x, y) | (x \in A \wedge y \in C) \cap (x \in B \wedge y \in B) \cap (x \in A \wedge y \in B) \cap (x \in B \wedge y \in C)\} \\
&= \{(x, y) | (x, y) \in (A \times C) \cap B^2 \cap (A \times B) \cap (B \times C)\}
\end{aligned}$$

Also:

$$\begin{aligned}
&(A \times C) \cap B^2 \cap (A \times B) \cap (B \times C) \\
&= \{(x, y) | (x \in A \wedge y \in C) \cap (x \in B \wedge y \in B) \cap (x \in A \wedge y \in B) \cap (x \in B \wedge y \in C)\} \\
&= \{(x, y) | x \in (A \cap B) \wedge y \in (B \cap C)\} \\
&= \{(x, y) | (x, y) \in (A \cap B) \times (B \cap C)\}
\end{aligned}$$

Problem 6. These are just the 16 different subsets of $\{(0,0), (0,1), (1,0), (1,1)\}$.

(a)

1. $\emptyset$
2. $\{(0,0)\}$
3. $\{(0,1)\}$
4. $\{(1,0)\}$
5. $\{(1,1)\}$
6. $\{(0,0), (0,1)\}$
7. $\{(0,0), (1,0)\}$
8. $\{(0,0), (1,1)\}$
9. $\{(0,1), (1,0)\}$
10. $\{(0,1), (1,1)\}$
11. $\{(1,0), (1,1)\}$
12. $\{(0,0), (0,1), (1,0)\}$
13. $\{(0,0), (0,1), (1,1)\}$
14. $\{(0,0), (1,0), (1,1)\}$
15. $\{(0,1), (1,0), (1,1)\}$
16. $\{(0,0), (0,1), (1,0), (1,1)\}$

(b) We list the relations by number as given in the solution above:
reflexive: $8, 13, 14, 16$
symmetric: $1, 2, 5, 8, 9, 12, 15, 16$
antisymmetric: $1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 13, 14$
transitive: $1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 13, 14, 16$

Problem 7. **(a)** The motions of the bracelet consists of 6 motions: rotations of 0-degree, 120-degree, and 240-degree, and three reflections, each keeping one bead fixed and interchanging the other two. The composition of any two of these operations is again one of these operations. R is reflexive since the 0-degree rotation plays the role of identity. Each operation has an inverse: reflections are their own inverses, the 0-degree rotation is its own inverse, and the 120-degree and 240-degree rotations are inverses of each other; this proves symmetry. To see that R is transitive, suppsose (B_1, B_2) and (B_2, B_3) belong to R. Taking the composition of the reflection in each case yields a composition of reflections, showing that (B_1, B_3) belongs to R.

(b) The equivalence classes are the indistinguishable bracelets. If we denote a bracelet by the colors of its beads, then these classes can be described as **RRR**, **WWW**, **BBB**, **RRW**, **RRB**, **WWR**, **WWB**, **BBR**, **BBW**, and **RWB**. Note that once we specify the colors, then any two bracelets are equivalent. This would not be the case if there were four or more beads, however. For example, in a 4-bead bracelet with two reds and two whites, the bracelet in which the red beads are adjacent is not equivalent to the one in which they are not.

Some common mistakes in your solutions

Problem 2:

- some students derived a bound, but not the one they were asked to show.
- a few did not use induction.

Problem 5: some tried to prove part (b) instead of disproving it by giving a counter example.

Problem 6:

- a few do not know what relations are.
- there seems to be a lot of confusion about properties such as reflexivity, symmetry, antisymmetry, and transitivity.

In general, most students have trouble writing down a proof in a clear and consistent way (*i.e.*, one statement follows from the previous one), without irrelevant observations and examples, and with explaining what they do when necessary.