Sets and Modular Arithmetic Tutorial Problems

1. Congruence classes of perfect squares
   a) Compute \{[x^2]_4 \mid x \in \mathbb{Z}\}. (That is, rewrite the set into a simpler form that lists all the elements explicitly.)

   b) Notice that, for any \(k\), \([a]_k \neq [b]_k\) implies \(a \neq b\). (Do you see why this is true?) Using this fact and the result from part (a), prove that for all integers \(x\) and \(y\), \(x^2 + y^2 \neq 4000003\). (Do not use a calculator.)

2. Sets warmup
   Consider the following sets: \(A = \{2\}\), \(B = \{A, \{4, 5\}\}\), \(C = B \cup \emptyset\), \(D = B \cup \{\emptyset\}\).
   a) Which of the sets have more than two elements?
   b) Which of the following are true:
      \[2 \in A, \{2\} \in A, \{2\} \in B, \emptyset \in C, \emptyset \in D, \]
      \[\emptyset \subseteq A, \{2\} \subseteq A, \{2\} \subseteq B\]

3. Cross product
   a) Find an example of sets \(A\) and \(B\) such that \(A \times B = B \times A\). Then find a second such pair of sets; try to make this second example feel different from your first, e.g. don’t just rename some elements.
   b) Consider the following incomplete statement:
      \[\text{For sets } A \text{ and } B, \text{ if } \underline{\text{____________________}} \text{ then } A \times B \neq B \times A.\]

      Create a true claim by filling in the blank with a statement about \(A\) and \(B\) that does not mention Cartesian products. Try to make the strongest possible claim, i.e. ideally your statement should still be true even if we replaced the “if-then” by an “if and only if”. If you have extra time, also prove your claim. Hint: two sets are not-equal if and only if there exists an element that is in one but not the other.

Solutions

1. Congruence classes of perfect squares
   We will use \([\cdot]_4\) as shorthand for \([\cdot]_4\).
a) For any even integer \( y = 2k \), \( y^2 = (2k)^2 = 4 \cdot k^2 \), so \( [y^2] = [4 \cdot k^2] = [0] \). For any odd integer \( z = 2m + 1 \), \( z^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 4 \cdot (m^2 + m) + 1 \), so \( [z^2] = [4 \cdot (m^2 + m) + 1] = [1] \). Every integer \( x \) is either even or odd, so \( \{ [x^2] \mid x \in \mathbb{Z} \} = \{ [0], [1] \} \).

Commentary: My scratch paper starts with small examples:
\[ [0^2] = [0], \quad [1^2] = [1], \quad [2^2] = [4] = [0], \quad [3^2] = [9] = [1]. \] At this point (or perhaps after a few more) you can guess the even-odd pattern, and write the proof accordingly.

b) Let \( x, y \) be integers. By part (a), each of \( [x^2] \) and \( [y^2] \) is either \( [0] \) or \( [1] \).
Thus, since \( x^2 + y^2 = [x^2] + [y^2] \), \( x^2 + y^2 \) is either \( [0] \), \( [1] \), or \( [2] \). However \( [4000003] = [3] \) (since \( 4000003 = 4 \cdot 1000000 + 3 \)), so \( x^2 + y^2 \neq [4000003] \). Therefore, \( x^2 + y^2 \neq 4000003 \).

2. Sets warmup
a) Only \( D \) has more than two elements: its three elements are
\[ \bullet \{ 2 \} \]
\[ \bullet \{ 4, 5 \} \]
\[ \bullet \emptyset \]

Commentary: Note that \( \{ 4, 5 \} \) is itself only one element, and that \( C = B \), so \( B \) and \( C \) each only have \( 2 \) elements.

b) These are true: \( 2 \in A \), \( \{ 2 \} \in B \), \( \emptyset \in D \), \( \emptyset \subseteq A \), \( \{ 2 \} \subseteq A \); the remaining statements are false. (Notice that for any object \( x \) and set \( Y \), \( x \in Y \) will always have the same truth value as \( \{ x \} \subseteq Y \).)

3. Cross product
a) Here are a few examples:
\[ \bullet A = \emptyset \text{ and } B = \{ 3 \}. \quad (\text{Then } A \times B = B \times A = \emptyset.) \]
\[ \bullet A = B = \{ 1, 2 \}. \quad (\text{Then } A \times B = B \times A = \{ (1, 1), (1, 2), (2, 1), (2, 2) \}.) \]

Commentary: It’s often worth starting a search for examples from simple “edge cases” like the empty set or sets being equal. In this case those happen to be the only examples that will work here.

b) Claim:

For sets \( A \) and \( B \), if the sets are non-empty and \( A \neq B \) then \( A \times B \neq B \times A \).

Proof: Let \( A \) and \( B \) be sets, and suppose they are non-empty and \( A \neq B \). Since the sets are not equal, there is at least one element that appears in one set but not the other, so without loss of generality, let \( x \) be an element where \( x \in A \) and \( x \notin B \). Since \( B \) is non-empty, let \( y \) be an element such that \( y \in B \). Then by the definition of Cartesian product, \( (x, y) \in A \times B \) (because \( x \in A \) and \( y \in B \)), but \( (x, y) \notin B \times A \) (because \( x \notin B \)), so \( A \times B \neq B \times A \).
Discussion Manual Solutions

2.1 Modular arithmetic

a) A few answers that keep it small are \([-31, -16, -1, 14, 29, 44]\). \((You can also create arbitrarily large answers, like [1500000014]).\)


c) 
\[
\begin{align*}
\end{align*}
\]

d) 
\[
\begin{align*}
\end{align*}
\]


3.1 Set Builder Notation

a) \{ (0, 3), (1, 2), (2, 1), (3, 0) \}

b) \{ -19, -12, -5, 2, 9, 16 \}

c) \{ 0, 1, 2, 3, 4, 5, 6, 7 \}

d) \{ (2\sqrt{2}, 2\sqrt{2}), (-2\sqrt{2}, -2\sqrt{2}) \}

3.2 Concrete Subset Proof

Let \(z\) be an (arbitrary) element of \(A\). Then by the definition of \(A\), \(z = (i, j)\) for some real numbers \(i\) and \(j\) where \(i^2 + j^2 \leq 1\). Since squares are non-negative, this gives us \(i^2 \leq 1\) and \(j^2 \leq 1\), which in turn gives us \(|i| \leq 1\) and \(|j| \leq 1\). Finally, this means that \(z = (i, j) \in B\). Since \(z\) was an arbitrary element of \(A\), we have shown that every element of \(A\) is an element of \(B\), so \(A \subseteq B\).
3.3b Abstract Subset Proof

Proof of the claim: Let \( z \) be an element of \((A - C) - (B - C)\). Then by the definition of set subtraction, \( z \in (A - C) \) and \( z \notin (B - C) \). From \( z \in (A - C) \), we get \( z \in A \) and \( z \notin C \). From \( z \notin (B - C) \), we get \( z \notin B \) OR \( z \in C \). Since we have established \( z \notin C \), the OR statement gives us \( z \notin B \). That, combined with our \( z \in A \), gives us \( z \in (A - B) \). Since \( z \) was arbitrary, this means that every element of \((A - C) - (B - C)\) is also an element of \((A - B)\), so \((A - C) - (B - C) \subseteq (A - B)\).

Proof the reverse containment does not hold: Consider the case where \( A = C = \{42\} \) and \( B = \emptyset \). Then \((A - C) - (B - C) = \emptyset\) and \((A - B) = \{42\}\), so \((A - B) \nsubseteq (A - C) - (B - C)\).

Commentary: Once again, sets being empty or equal to each other turned out to be a great place to find counterexamples. It won’t always work, but it’s always worth a try.