E. Dummit's Math 1465 ~ Intensive Mathematical Reasoning, Fall 2024 ~ Midterm 2 Solutions (Form E)

---

1. Each part was worth 3 points.

   (a) By Euclid we see that $31 = 6 \cdot 5 + 1$, so $1 = 31 - 6 \cdot 5$. Reducing mod 31 yields $1 \equiv (-6) \cdot 5 \pmod{31}$, so that $\overline{1} = \overline{-6} \cdot \overline{5}$. This means $\boxed{\overline{5}^{-1} = \overline{-6} = \overline{25}}$.

   (b) Many options. A simple one is $R = \{(1,1),(2,2),(3,3),(1,2)\}$ which is not symmetric since it does not contain $(2,1)$.

   (c) The ordered pairs are those involving any two elements in the same equivalence class: the union of $\{1,5\} \times \{1,5\}$, $\{2\} \times \{2\}$, $\{3,4\} \times \{3,4\}$. The full list is $\boxed{\{(1,1),(1,5),(5,1),(5,5),(2,2),(3,3),(3,4),(4,3),(4,4)\}}$.

   (d) Many options. A simple one is to take $f(1) = f(2) = a$, $f(3) = b$, $f(4) = c$.

   (e) For $y = f(x)$ we have $y = 5x - 3$. Solving for x in terms of y yields $x = \dfrac{y+3}{5}$, so $\boxed{f^{-1}(y) = \dfrac{y+3}{5}}$.

---

2. Each part was worth 1.5 points.

   (a) Since the pair $(2,2)$ is missing from R, $\boxed{R \text{ is not reflexive}}$.

   (b) Reversing the pairs yields $(1,1),(2,1),(1,2),(3,3)$, all of which are in R, so $\boxed{R \text{ is symmetric}}$.

   (c) Since $(2,1),(1,2)$ are in R but $(2,2)$ is not in R, $\boxed{R \text{ is not transitive}}$.

   (d) Since R is not reflexive or transitive, $\boxed{R \text{ is not an equivalence relation}}$.

   (e) Since $(1,2) \in R$ and $(2,1) \in R$ but $1 \neq 2$, $\boxed{R \text{ is not antisymmetric}}$.

   (f) Since R is not antisymmetric, $\boxed{R \text{ is not a partial ordering}}$.

   (g) Since 1 is the first element of two different pairs, $\boxed{R \text{ is not a function}}$ from A to A.

---

3. Part (a) was worth 7 points and (b) was worth 3 points.

   (a) We must show that R is reflexive, symmetric, and transitive.

   - Reflexive: We have $a^2 \equiv a^2 \pmod 7$, so $\overline{a}\, R\, \overline{a}$ for any a.
   - Symmetric: If $a^2 \equiv b^2 \pmod 7$ then $b^2 \equiv a^2 \pmod 7$, so if $\overline{a}\, R\, \overline{b}$ then $\overline{b}\, R\, \overline{a}$.
   - Transitive: If $a^2 \equiv b^2 \pmod 7$ and $b^2 \equiv c^2 \pmod 7$ then $a^2 \equiv c^2 \pmod 7$, so if $\overline{a}\, R\, \overline{b}$ and $\overline{b}\, R\, \overline{c}$ then $\overline{a}\, R\, \overline{c}$.

   (b) The equivalence classes are $\{\overline{0}\}$, $\{\overline{1},\overline{6}\}$, $\{\overline{2},\overline{5}\}$, and $\{\overline{3},\overline{4}\}$. (Other descriptions are possible here, such as $[\overline{a}] = \{\overline{a}, -\overline{a}\}$ for each residue class $\overline{a}$.)

---

4. We can either show f is one-to-one and onto separately, or do them together by showing f is a bijection directly.

   - Solution 1: First, f is one-to-one: if $f(a) = f(b)$, then applying f to both sides yields $f(f(a)) = f(f(b))$ so that $-a = -b$ hence $a = b$.
   - Also, f is onto: for any $b \in \mathbb{Z}$, if we take $a = f(-b)$ then $f(a) = f(f(-b)) = -(-b) = b$.
   - Solution 2: Let $g(x) = f(f(f(x)))$. We claim that $f^{-1}(x) = g(x)$: to see this, note (as suggested by the hint) that $f(f(f(f(x)))) = f(f(-x)) = -(-x) = x$. Therefore, we have $(f \circ g)(x) = f(f(f(f(x)))) = x$ and also $(g \circ f)(x) = f(f(f(f(x)))) = x$ as well. Thus, since f is invertible, it is one-to-one and onto.

---

5. We must show that R is reflexive, antisymmetric, and transitive.

   - Reflexive: for any $a \in A$, we have $(f(a), f(a)) \in S$ because S is reflexive. So by definition, $(a, a) \in R$.
   - Antisymmetric: suppose $(a, b) \in R$ and $(b, a) \in R$, so that $(f(a), f(b)) \in S$ and $(f(b), f(a) \in S$. Then because S is antisymmetric, $f(b) = f(a)$, and so since f is one-to-one, $b = a$.
   - Transitive: suppose $(a, b) \in R$ and $(b, c) \in R$. Then $(f(a), f(b)) \in S$ and also $(f(b), f(c)) \in S$. Then because S is transitive, $(f(a), f(c)) \in S$, and so $(a, c) \in R$ as required.
   - Remark: The fact that f is one-to-one is required to get antisymmetry, but it is not needed for the other two properties.

---

6. Each part was worth 5 points.

   (a) The set of perfect squares is countably infinite, as is the set of prime numbers (per Euclid's proof, there are infinitely many primes). By our results on countability, we know that for any countably infinite set A there exists a bijection $f : A \to \mathbb{Z}_+$. So we have bijections $f : E \to \mathbb{Z}_+$ and $g : P \to \mathbb{Z}_+$: then the composition $f^{-1} \circ g : P \to E$ is also a bijection.

   (b) Suppose $f : \mathbb{R} \to \mathbb{Z}$ is onto, and also suppose by way of contradiction that $f : \mathbb{R} \to \mathbb{Z}$ is one-to-one. Then f would be a bijection from $\mathbb{R}$ to $\mathbb{Z}$, but such a bijection cannot exist because $\mathbb{R}$ is uncountable and $\mathbb{Z}$ is countable. This is a contradiction, so f cannot be one-to-one.

---

7. Part (a) was worth 3 points while each item in (b) was worth 1 point.

   (a) The rational numbers and even numbers are both countably infinite. The set of subsets of $\{1, 2, \ldots, 2023\}$ is very large but finite. The only uncountable set is $\boxed{\text{(i) The set of real numbers greater than 1}}$.

   (b) In order, the responses are

   i. $\boxed{\text{True}}$. We have $\overline{4} \cdot \overline{6} = \overline{24} = \overline{0} = \overline{12} = \overline{5} + \overline{7}$ mod 12.

   ii. $\boxed{\text{True}}$. Since 13 is prime, every nonzero residue class is relatively prime to it, hence has an inverse.

   iii. $\boxed{\text{False}}$. There are many more than 2 equivalence relations (in fact there are 52 in total).

   iv. $\boxed{\text{False}}$. The divisibility relation is not a partial ordering since $-1|1$ and $1|-1$ but $-1 \neq 1$.

   v. $\boxed{\text{True}}$. For real numbers x, y, if $x^3 = y^3$ then $x = y$.

   vi. $\boxed{\text{True}}$. We have $f(\sqrt[3]{x}) = x$ for every real x.

   vii. $\boxed{\text{False}}$. An one-to-one function need not be a bijection. For example, $f : \{1\} \to \{1, 2\}$ with $f(1) = 1$ is one-to-one but not onto.

   viii. $\boxed{\text{True}}$. A onto function from $\{1, 2, 3\}$ and $\{a, b, c\}$ must also be one-to-one since both sets are finite and have the same cardinality.

   ix. $\boxed{\text{False}}$. Since $\mathbb{R}$ is uncountable while $\mathbb{Q}$ is countable there cannot be a bijection between them.

   x. $\boxed{\text{True}}$. Both $\mathbb{Q}$ and $\mathbb{Z}$ are countably infinite, so there is a bijection between them.

   xi. $\boxed{\text{False}}$. As shown in class, the power set of the countable set $\mathbb{Z}_+$ is uncountable.

   xii. $\boxed{\text{False}}$. For example, the uncountable set $\mathbb{R}$ has the countable subsets $\mathbb{Q}$, $\mathbb{Z}$, $\{1\}$, and $\emptyset$.
