hw6-proofs-cardinality-relations: Sample Solutions

CSE20S24

Due: 6/6/24 at 5pm (no penalty late submission until 8am next morning)

In this assignment, you will work with binary relations and prove properties about them, practicing proof strategies and applications.

Relevant class material: Weeks 9,10.

You will submit this assignment via Gradescope (https://www.gradescope.com) in the assignment called "hw6-proofs-cardinality-relations".

In your proofs and disproofs of statements below, justify each step by reference to a component of the following proof strategies we have discussed so far, and/or to relevant definitions and calculations.

- A counterexample can be used to prove that $\forall x P(x)$ is **false**.
- A witness can be used to prove that $\exists x P(x)$ is **true**.
- **Proof of universal by exhaustion**: To prove that $\forall x\, P(x)$ is true when P has a finite domain, evaluate the predicate at **each** domain element to confirm that it is always T.
- **Proof by universal generalization**: To prove that $\forall x\, P(x)$ is true, we can take an arbitrary element e from the domain and show that $P(e)$ is true, without making any assumptions about e other than that it comes from the domain.
- To prove that $\exists x P(x)$ is **false**, write the universal statement that is logically equivalent to its negation and then prove it true using universal generalization.
- **Strategies for conjunction**: To prove that $p \wedge q$ is true, have two subgoals: subgoal (1) prove p is true; and, subgoal (2) prove q is true. To prove that $p \wedge q$ is false, it's enough to prove that p is false. To prove that $p \wedge q$ is false, it's enough to prove that q is false.
- **Proof of Conditional by Direct Proof**: To prove that the implication $p \rightarrow q$ is true, we can assume p is true and use that assumption to show q is true.

- **Proof of Conditional by Contrapositive Proof**: To prove that the implication $p \to q$ is true, we can assume $\neg q$ is true and use that assumption to show $\neg p$ is true.
- **Proof by Cases**: To prove q when we know $p_1 \vee p_2$, show that $p_1 \to q$ and $p_2 \to q$.
- **Proof by Structural Induction**: To prove that $\forall x \in X\, P(x)$ where X is a recursively defined set, prove two cases:

  Basis Step: Show the statement holds for elements specified in the basis step of the definition.

  Recursive Step: Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.
- **Proof by Mathematical Induction**: To prove a universal quantification over the set of all integers greater than or equal to some base integer b:

  Basis Step: Show the statement holds for b.

  Recursive Step: Consider an arbitrary integer n greater than or equal to b, assume (as the **induction hypothesis**) that the property holds for n, and use this and other facts to prove that the property holds for $n + 1$.
- **Proof by Strong Induction** To prove that a universal quantification over the set of all integers greater than or equal to some base integer b holds, pick a fixed nonnegative integer j and then:

  Basis Step: Show the statement holds for b, $b + 1$, $\ldots$, $b + j$.

  Recursive Step: Consider an arbitrary integer n greater than or equal to $b + j$, assume (as the **strong induction hypothesis**) that the property holds for **each of** b, $b + 1$, $\ldots$, n, and use this and other facts to prove that the property holds for $n + 1$.
- **Proof by Contradiction**

  To prove that a statement p is true, pick another statement r and once we show that $\neg p \to (r \wedge \neg r)$ then we can conclude that p is true.

  Informally The statement we care about can't possibly be false, so it must be true.

Assigned questions

1. Binary relations. In the review quiz, we considered the binary relation on $\mathbb{Z}^+$ defined by

$$\{(a, b) \mid \exists c \in \mathbb{Z}(b = ac)\}$$

Let's call that relation R_1. Consider the following other binary relations on $\mathbb{Z}^+$:

$$R_2 = \{(a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid gcd(\ (a, b)\ ) = 1\}$$

$$R_3 = \{(a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid a + b \leq 2024\}$$

Sample response that can be used as reference for the detail expected in your answer: To prove that R_1 is not symmetric we need to find a counterexample to

$$\forall x \in \mathbb{Z}^+ \forall y \in \mathbb{Z}^+ \; (\; (x, y) \in R_1 \rightarrow (y, x) \in R_1 \;)$$

Consider $x = 2$ and $y = 4$. Then $(x, y) \in R_1$ because $\exists c \in \mathbb{Z}(y = xc)$ is witnessed by the integer $c = 2$, since $4 = 2 \cdot 2$. However, $\exists c \in \mathbb{Z}(x = yc)$ is not true: to prove this, we consider an arbitrary integer c and consider the two (exhaustive) cases $c \geq 1$ and $c < 1$. In case 1, assume $c \geq 1$, and then $yc = 4c \geq 4 > 3$ so $yc \neq 2 = x$. In case 2, assume $c < 1$ so $c \leq 0$, and then $yc = 4c \leq 0$ so is not equal to 2, which is x. Thus, we've found positive integers x and y where $(x, y) \in R_1$ and $(y, x) \notin R_1$ so R_1 is not symmetric.

(a) (*Graded for completeness*) [1] Give example positive integers that are related according to each of these three relations. In other words, give example values (a_1, b_1), (a_2, b_2), and (a_3, b_3) such that $(a_i, b_i) \in R_i$ for each $i = 1, 2, 3$.

Sample Solution: Let $a_1 = 1, b_1 = 2$ (both positive integers). $(a_1, b_1) \in R_1$ as $c = 2$ witnesses $\exists c \in \mathbb{Z} b_1 = a_1 \cdot c$.

Let $a_2 = 3, b_2 = 5$ (both positive integers). The positive factors of a_2 form the set $\{1, 3\}$, and the positive factors of b_2 form the set $\{1, 5\}$, so $gcd((a_2, b_2)) = 1$ and thus $(a_2, b_2) \in R_2$.

Let $a_3 = 1, b_3 = 1$ (both positive integers). $a_3 + b_3 = 2 \leq 2024$, so $(a_3, b_3) \in R_3$.

(b) (*Graded for correctness*) [2] Prove that R_2 is not transitive.

Solution: To prove that R_2 is not transitive we need to find a counterexample to

$$\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ \forall c \in \mathbb{Z}^+ \quad ((a, b) \in R_2 \wedge (b, c) \in R_2) \rightarrow (a, c) \in R_2$$

Consider $a = 2, b = 3, c = 4$ (all of which are positive integers). Then $(a, b) \in R_2$ as $gcd((2, 3)) = 1$, and $(b, c) \in R_2$ as $gcd((3, 4)) = 1$. However, $(a, c) \notin R_2$ as $gcd((2, 4)) = 2 \neq 1$. Hence, we have found positive integers a, b, c where $(a, b) \in R_2$ and $(b, c) \in R_2$ but $(a, c) \notin R_2$, so R_2 is not transitive.

[1] This means you will get full credit so long as your submission demonstrates honest effort to answer the question. You will not be penalized for incorrect answers. To demonstrate your honest effort in answering the question, we expect you to include your attempt to answer *each* part of the question. If you get stuck with your attempt, you can still demonstrate your effort by explaining where you got stuck and what you did to try to get unstuck.

[2] This means your solution will be evaluated not only on the correctness of your answers, but on your ability to present your ideas clearly and logically. You should explain how you arrived at your conclusions, using mathematically sound reasoning. Whether you use formal proof techniques or write a more informal argument for why something is true, your answers should always be well-supported. Your goal should be to convince the reader that your results and methods are sound.

(c) (*Graded for correctness*) Prove that R_3 is not reflexive.

Solution: To prove that R_3 is not reflexive we need to find a counterexample to

$$\forall a \in \mathbb{Z}^+ \quad (a, a) \in R_3$$

Consider $a = 2000$, $a + a = 4000 > 2024$, so $(a, a) \notin R_3$. Hence, we have found positive integer a where $(a, a) \notin R_3$, so R_3 is not reflexive.

(d) (*Graded for correctness*) Prove that R_2 is symmetric.

Solution: To prove that R_2 is symmetric we need to prove

$$\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ \quad (a, b) \in R_2 \rightarrow (b, a) \in R_2$$

Let a, b be arbitrary positive integers. Towards a direct proof, assume $(a, b) \in R_2$, which implies $gcd((a, b)) = 1$. By the definition of gcd (because the set of common divisors of two integers can be thought of as the intersection of the separate sets of divisors, and set intersection is commutative), $gcd((a, b)) = gcd((b, a))$. Hence, $gcd((b, a)) = 1$ and $(b, a) \in R_2$.

(e) (*Graded for correctness*) Prove that R_3 is not anti-symmetric.

Solution: To prove that R_3 is not anti-symmetric we need to find a counterexample to

$$\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ \quad ((a, b) \in R_3 \wedge (b, a) \in R_3) \rightarrow a = b$$

Consider $a = 1, b = 2$. Then $a+b = b+a = 3 \leq 2024$, which implies $(a, b) \in R_3 \wedge (b, a) \in R_3$. However, $a \neq b$. Hence, we have found positive integers a, b, c where $((a, b) \in R_3 \wedge (b, a) \in R_3) \rightarrow a = b$ is false, so R_3 is not anti-symmetric.

(f) (*Graded for completeness*) Give an example relation on $\mathbb{Z}^+$ that is both symmetric and anti-symmetric. Briefly justify your example.

Sample solution 1: The identity relation $R = \{(a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid a = b\}$ is both symmetric and anti-symmetric. It is symmetric because equals is symmetric, so $\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ \ (a = b \rightarrow b = a)$. It is anti-symmetric because, if we consider arbitrary positive integers a and b and assume that $(a, b) \in R$ and $(b, a) \in R$,the definition of R guarantees that $a = b$ as required.

Sample solution 2: The empty relation $R = \emptyset$ is both symmetric and anti-symmetric. The universal claim $\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ \ ((a, b) \in R \rightarrow (b, a) \in R)$ evaluates to true because the hypothesis is always false. Similarly $\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ \ ((a, b) \in R \wedge (b, a) \in R \rightarrow a = b)$ also evaluates to true because the hypothesis is always false. Hence, R is both symmetric and anti-symmetric.

2. Equivalence relations. Recall that we say a is **congruent to** b **mod** n means $(a, b) \in R_{(\mathbf{mod}\ n)}$, that is ($a$ **mod** $n = b$ **mod** n). A common notation is to write this as $a \equiv b (\mathbf{mod}\ n)$.

A **modular inverse** of an integer x relative to modulus n (where n is a positive number and x is an integer between 0 and $n - 1$, inclusive) is defined to be an integer y between 0 and $n - 1$ (inclusive) such that $xy \equiv 1 (\mathbf{mod}\ n)$.

(a) (*Graded for completeness*) Fill in the multiplication table below so that each cell in row labelled a and column labelled b is an integer p in the set $\{0, 1, 2, 3, 4\}$ satisfying $ab \equiv p(\textbf{mod } 5)$. Then, use this multiplication table to find the **modular inverse** of each number in $\{0, 1, 2, 3, 4\}$ or to explain why it does not exist.

Solution:

	0	1	2	3	4
0	0	0	0	0	0
1	0	**1**	2	3	4
2	0	2	4	**1**	3
3	0	3	**1**	4	2
4	0	4	3	2	**1**

Modular inverse of 0 does not exist because there's no y to make $0 \cdot y \equiv 1 \pmod 5$.
Modular inverse of 1 is 1 (looking at the 1 in the second row and second column).
Modular inverse of 2 is 3 (looking at the 1 in the third row and fourth column).
Modular inverse of 3 is 2 (looking at the 1 in the fourth row and third column).
Modular inverse of 4 is 4 (looking at the 1 in the fifth row and fifth column).

(b) (*Graded for correctness*) Find an example n and integer x between 1 and $n-1$ (inclusive) so that there is no modular inverse of x relative to n. Justify your example by exhausting through all the possible values of y between 0 and $n-1$ and showing that none of them have $xy \equiv 1(\textbf{mod } n)$. *Note: 0 does not have a modular inverse relative to n. In this question, you're looking for a value of n where some nonzero number also doesn't have a modular inverse relative to n.*

Idea: Consider $d = gcd((n, x))$. Let $r = xy$ **mod** n, $q = xy$ **div** n. By definition of mod and div, $r = x \cdot y - q \cdot n$. By definition of gcd, $d \mid n$ and $d \mid x$, which implies $d \mid x \cdot y$ and $d \mid q \cdot n$, and hence $d \mid r = x \cdot y - q \cdot n$. Therefore, if we can have xy **mod** $n = 1$, then $d \mid 1$ and only possible choice for d is that $d = 1$. The contrapositive of the previous result is that if $d = gcd(n, x) > 1$, then for all allowed values of y, xy **mod** $n \neq 1$. In other words, x doesn't have a modular inverse relative to n.

Sample solution: Consider $x = 2$ and $n = 4$. $x \cdot 0 = 0 \equiv 0 \pmod 4$; $x \cdot 1 = 2 \equiv 2 \pmod 4$; $x \cdot 2 = 4 \equiv 0 \pmod 4$; $x \cdot 3 = 6 \equiv 2 \pmod 4$. Hence, $x = 2$ does not have a modular inverse relative to $n = 4$.

3. (*Graded for correctness*) Partial orders. Recall the recursive definition of the set of linked lists of natural numbers (from class)

Basis Step:	$[] \in L$
Recursive Step:	If $l \in L$ and $n \in \mathbb{N}$, then $(n, l) \in L$

and the definition of the function which gives the length of a linked list of natural numbers

$length : L \to \mathbb{N}$

Basis Step:	$length(\ [])$	$= 0$
Recursive Step: If $l \in L$ and $n \in \mathbb{N}$, then	$length(\ (n, l)\ )$	$= 1 + length(l)$

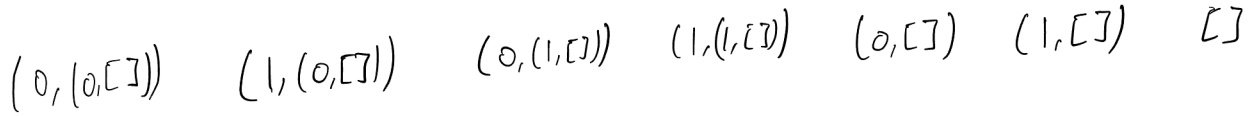
For this question, we'll restrict our attention to just linked lists with data in the set $\{0, 1\}$ which have length 0, 1, or 2. Let's call this restricted set of lists L'.

Note: L' has 7 distinct elements.

Define two different partial orders with domain L'. For each of the partial orders, you can specify its definition by listing the set of ordered pairs with roster method, giving a set builder definition, giving a recursive definition, or using a clear and precise English description of which lists are related to one another. Then, draw the Hasse diagram for each of the two partial orders you defined.

Sample solution 1: The simplest partial order is $R = \{(a, a) \mid a \in L'\}$. It is reflexive as $(a, a) \in R$ for each element a in L' (we can test this by exhaustion). It is anti-symmetric because, for arbitrary a and b in L', if we assume that $(a, b) \in R \wedge (b, a) \in R$, that guarantees (in particular) that $(a, b) \in R$, which by definition means $a = b$, as desired. It is transitive because for arbitrary a, b, c in L', if $((a, b) \in R \wedge (b, c) \in R)$ the definition of R gives $a = b \wedge b = c$ and since $=$ is transitive, we get $a = c$, or in other words, $(a, c) \in R$ (as required). Hence, R is a partial order.

The Hasse diagram would have no edges (as we omit self-loops):

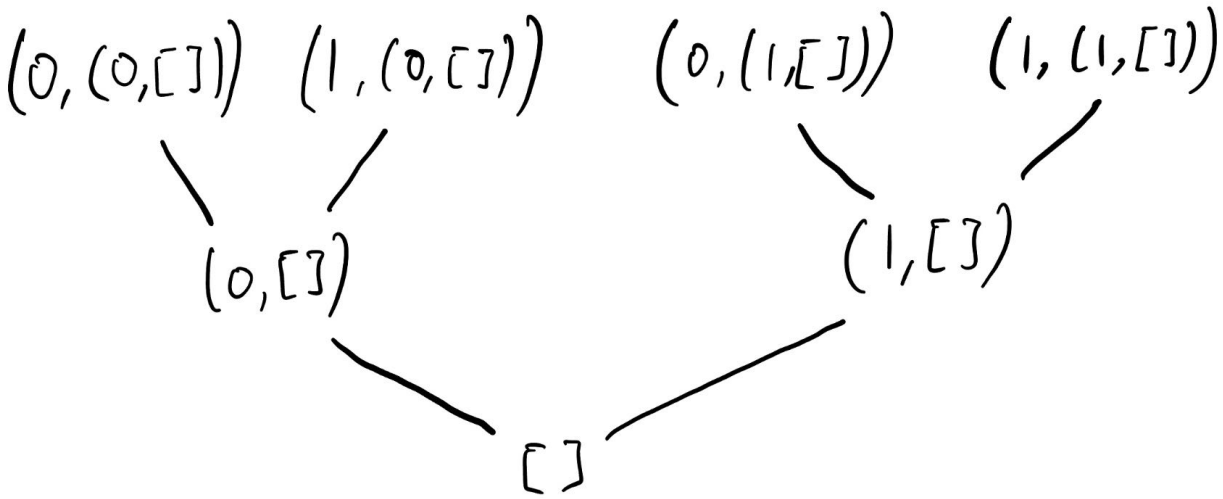


Sample Solution 2: Another partial order can be defined by

$R_2 = \{(a, b) \in L' \times L' \mid$ we can change a to b by prepending data to a non-negative many times$\}$

It is reflexive as, for arbitrary a in L', we can change a to a by prepending data zero many times, which means $(a, a) \in R_2$. To formally prove that R_2 is anti-symmetric, we could prove a lemma that, for all $(a, b) \in R_2$, $length(a) \leq length(b)$. Once we have that, we can show that, for arbitrary a and b in L', if $(a, b) \in R_2 \wedge (b, a) \in R_2$, we $length(a) \leq length(b)$ and $length(a) \geq length(b)$ so $length(a) = lenght(b)$ and the only way to have that while the relation holds is to have $a = b$. It is transitive because for arbitrary a, b, c in L', if we assume that $((a, b) \in R_2 \wedge (b, c) \in R_2)$, that means we can change a to b and b to c by prepending, therefore we can also change a to c by combining those operations. So $(a, c) \in R_2$ as desired. Hence, R_2 is a partial order.

The Hesse diagram would look like:



4. Equivalence classes and partitions. Recall that in a movie recommendation system, each user's ratings of movies is represented as a n-tuple (with the positive integer n being the number of movies in the database), and each component of the n-tuple is an element of the collection $\{-1, 0, 1\}$. Assume there are five movies in the database, so that each user's ratings can be represented as a 5-tuple. We call Rt_5 the set of all ratings 5-tuples. Consider the binary relation on the set of all 5-tuples where each component of the 5-tuple is an element of the collection $\{-1, 0, 1\}$:

   $$G = \{(u, v) \in Rt_5 \times Rt_5 \mid \text{the number of 1s in } u \text{ is the same as the number of 1s in } v\}$$

   This is an equivalence relation (you do not need to prove this).

   Recall that the **equivalence class** of an element $x \in X$ for an equivalence relation $\sim$ on the set X is the set $\{s \in X | (x, s) \in \sim\}$. We write this as $[x]_\sim$.

   (a) (*Graded for correctness*) Find a ratings 5-tuple v such that $[v]_G = \{v\}$. Justify your choice of v.

   Solution: $[v]_G = \{v\}$ means that the only element in the equivalence relation is the element itself. If there are any elements other than 1 in the 5-tuple v, another element in that equivalence relation could have the same 5-tuple but swap out one non-1 number element with the other number not equal to 1. For example, if we have $v = (1, 1, 1, 1, 0)$, the tuple $v' = (1, 1, 1, 1, -1)$ would also be in the equivalence relation set and v cannot be the only element in $[v]_G$. Hence, the only possible v is $(1, 1, 1, 1, 1)$. For all $u \in Rt_5$, $(u, v) \in G$ means the number of 1s in u is also fives, which guarantees that $u = (1, 1, 1, 1, 1)$. Hence, the only

member in $[v]_G$ is v itself.

(b) (*Graded for completeness*) Find distinct ratings 5-tuples u_1, u_2 ($u_1 \neq u_2$) whose equivalence classes $[u_1]_G$ and $[u_2]_G$ have the same size.

Note: We know that elements of the domain of an equivalence relation that are related by the equivalence relation have the same equivalence class.

Sample solution: All we need is to find $u_1 \neq u_2$ such that $(u_1, u_2) \in G$. One example would be $u_1 = (1, 0, 0, 0, 0)$ and $u_2 = (0, 1, 0, 0, 0)$. They have the same number of 1s and thus $(u_1, u_2) \in G$. By the note above, $[u_1]_G = [u_2]_G$ and thus they have the same size.

(c) (*Graded for completeness*) Find distinct ratings 5-tuples w_1, w_2 ($w_1 \neq w_2$) whose equivalence classes $[w_1]_G$ and $[w_2]_G$ have different sizes.

Sample Solution: Let $w_1 = (1, 0, 0, 0, 0)$ and $w_2 = (1, 1, 1, 1, 1)$. From (a) we know $[w_2]_G = \{w_2\}$ has size 1, and from (b) we know that $(0, 1, 0, 0, 0)$ is another element in $[w_1]_G$ other than w_1, which means $[w_1]_G$ has size at least 2. Hence, $[w_1]_G$ and $[w_2]_G$ have different sizes.

5. Modular exponentiation. Imagine you are playing the role of Alice in the Diffie Hellman key agreement (exchange) protocol. You and Bob have agreed to use the prime $p = 7$ and its primitive root $a = 3$. Your secret integer is $k_1 = 3$.

(a) (*Graded for fair effort completeness*[3]) Calculate the number you send to Bob, a^{k_1} **mod** p. Use the modular exponentiation algorithm for the calculation. Include a trace of the algorithm in your solution.

Modular Exponentation

```
1  procedure modular exponentiation(b: integer;
2                n = (a_{k-1}a_{k-2}...a_1a_0)_2, m: positive integers)
3  x := 1
4  power := b mod m
5  for i:= 0 to k-1
6     if a_i = 1 then x:= (x · power) mod m
7     power := (power · power) mod m
8  return x {x equals b^n mod m}
```

Solution:

Trace for Modular Exponentation(b=3, n=3 = $(11)_2$, m=7)				
	x	power	i	a_i
Initial Value	1	3	0	1
After 1 Iteration	3 (=1*3 mod 7)	2 (=3*3 mod 7)	1	1
After 2 Iteration	6 (=3*2 mod 7)	4 (=2*2 mod 7)		

Hence, a^{k_1} **mod** $p = 3^3$ **mod** $7 = 6$.

[3]This means you will get full credit so long as your submission demonstrates honest effort to answer the question. You will not be penalized for incorrect answers.

(b) (*Graded for fair effort completeness*) Bob sends you the number 5. Compute your shared key, $\left(a^{k_2}\right)^{k_1}$ **mod** p. Hint: a^{k_2} **mod** p is what Bob sent you. Include all relevant calculations, annotated with explanations, for full credit.

Solution: Since exponentiation is just a sequence of multiplication and by the multiplication arithmetic in modular, we have a^b **mod** $p = (a$ **mod** $p)^b$ **mod** p. Hence,

$$\begin{aligned}
&\left(a^{k_2}\right)^{k_1} \textbf{ mod } p \\
&= \left(a^{k_2} \textbf{ mod } p\right)^{k_1} \textbf{ mod } p \\
&= 5^{k_1} \textbf{ mod } 7 \\
&= 5^3 \textbf{ mod } 7 \\
&= 125 \textbf{ mod } 7 \\
&= 6
\end{aligned}$$

(c) (*Graded for fair effort completeness*) What are some possible values for Bob's secret integer? What algorithm are you using to compute them?

Sample Solution: We want to find k_2 such that 3^{k_2} **mod** $7 = 5$. We can start off by trying few small values for k_2 and try to find a pattern.

$$\begin{aligned}
&3^1 \textbf{ mod } 7 = 3 \\
&3^2 \textbf{ mod } 7 = 3 \cdot 3 \textbf{ mod } 7 = 2 \\
&3^3 \textbf{ mod } 7 = 2 \cdot 3 \textbf{ mod } 7 = 6 \\
&3^4 \textbf{ mod } 7 = 6 \cdot 3 \textbf{ mod } 7 = 18 \textbf{ mod } 7 = 4 \\
&3^5 \textbf{ mod } 7 = 4 \cdot 3 \textbf{ mod } 7 = 12 \textbf{ mod } 7 = 5 \\
&3^6 \textbf{ mod } 7 = 5 \cdot 3 \textbf{ mod } 7 = 15 \textbf{ mod } 7 = 1 \\
&3^7 \textbf{ mod } 7 = 1 \cdot 3 \textbf{ mod } 7 = 3
\end{aligned}$$

Hence, one possible value for k_2 is 5, and the other values are elements of the set $\{5 + 6 * n \mid n \in \mathbb{N}\}$.

The proof is based on the observation that 3^6 **mod** $7 = 1$, which means 3^{5+6*n} **mod** $7 = (3^5) \cdot (3^6)^n$ **mod** $7 = (3^5$ **mod** $7) \cdot ((3^6)^n$ **mod** $7) = 5 \cdot ((3^6$ **mod** $7)^n$ **mod** $7) = 5 \cdot ((1^n)$ **mod** $7) = 5 \cdot 1 = 5$.