CISC 1100: HW 4

SOLUTIONS

1) a) Write the set of all numbers $x \in \mathbb{Z}$ such that $x \equiv 4 (mod\, 5)$ in set builder notation.

$\{x \in \mathbb{Z} : x = 5k + 4, k \in \mathbb{Z}\}$

b) State the equivalence classes for the relation "$x \equiv y (mod\, 5)$" on $S = \mathbb{Z}$

$[0], [1], [2], [3], [4]$

c) Find all solutions to $2x \equiv 3 (mod\, 5)$. Hint: you only need to test one element from each equivalence class.

Any $x \in [4]$ works; this is because $2(4) = 8 \equiv 3 (mod\, 5)$. This can be found by observation by running through the equivalence classes.

d) Find all solutions to $5x \equiv 4 (mod\, 6)$ and $2x \equiv 4 (mod\, 7)$. (Notice you have different equivalence classes now.)

$x \in [2]$ for the first and $x \in [2]$ in the latter as well, although these are different equivalence classes. Interestingly, this does mean that $x = 2$ works as a solution to either question, although for instance 8 will satisfy the first and not the second, while 9 will satisfy the second and not the first.

e) Generally we are looking at equations of the form $ax \equiv b(mod\, n)$. What pattern do you notice is emerging between a, n? This condition is necessary to guarantee a solution; for example $2x \equiv 1(mod\, 4)$ has no solution.

The pattern is that a, n have no common divisors, or are "coprime." We will see that when this happens, a has an "inverse" that allows us to "undo" multiplication. (Which is also the shortcut to finding the answer.)

2) Modular arithmetic has many applications. One is determining powers of $i = \sqrt{-1}$, the imaginary number.

a) Write out the powers of $i^0, i^1, i^2, ..., i^7$.

$i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1, i^5 = i, i^6 = -1, i^7 = -i$

b) Notice that the powers of i 'reset' every 4; for instance $i = i^5$. Therefore $i^k = i^0, i^1, ..., i^3$ depending on what k is equal to $(mod\, 4)$. Using this fact, find i^{107}, i^{-22}

$107 \equiv 3(mod\, 4)$, so $i^{107} = i^3 = -i$. $-22 \equiv 2(mod\, 4)$ so $i^{-22} = i^2 = -1$.

c) Another application is the 'last digit' problem. Find $12(mod\, 10), -28(mod\, 10), 217(mod\, 10)$

2,8,7 respectively.

d) What pattern do you notice emerging?

$(mod\, 10)$ reads off the units digit of an integer.

e) If $a \equiv a'(mod\, n)$ and $b \equiv b'(mod\, n)$, then $ab \equiv a'b'(mod\, n)$. Using this fact and your observation in (d), find the last digit of $(22)^{17}$.

First notice $22 \equiv 2(mod\, 10)$. This tells us that $22^{17} \equiv 2^{17}(mod\, 10)$ by the given property. But notice that $2^5 \equiv 2(mod\, 10)$, so that $2^{17} = 2^5 \cdot 2^5 \cdot 2^5 \cdot 2^2 \equiv 2 \cdot 2 \cdot 2 \cdot 2^2 \equiv 2^5 \equiv 2(mod\, 10)$. So the last digit of 22^{17} is 2.

3) Suppose that X is a set and let $S = P(X)$, the power set. Consider the relation $r = \{(A, B) \in S \times S | A \subset B\}$.

a) Prove that r is irreflexive.

Let $A \in S$. $A \not\subset A$ because we are using strict subsets, and $A = A$ by definition. So $\forall A \in S, (A, A) \notin r$.

b) Prove that r is antisymmetric.

Let $A, B \in r$ with $A \neq B$. If $A \subset B$, we cannot have $B \subset A$ as this would imply $A = B$, contrary to assumption. So $\forall A, B \in S, A \neq B, (A, B) \in r \Rightarrow (B, A) \notin r$.

c) Prove that r is transitive.

Let $A, B, C \in S$. Then $A \subset B$ and $B \subset C$ implies that $A \subset C$. Therefore for all $A, B, C \in S$ such that $(A, B) \in r, (B, C) \in r$, $(A, C) \in r$.

d) Why isn't it necessary to show that r is reflexive or symmetric?

To show that something is not reflexive, we need to provide only one counterexample of an element that is not reflexive. In fact we showed that every element is not reflexive, so our work is done.

Same goes for symmetric.

As we learned in class, these properties make r an 'inequality relation.' An important aspect of inequality relations is that, for any finite set S with inequality relation r, S contains a 'least element,' that is, $\exists x \in S, xRy\ \forall y \in S$. (Think of this as $0 < n$ for any natural number$n \in \mathbb{N}$).

e) Assume X is finite. What is the least element for this relation r on $S = P(X)$?

First notice that if X is finite, so is $S = P(X)$. So we know that there will be a least element. (You didn't have to provide this in your hw.)

Next we look for a set A such that $A \subset B$ for all $B \in P(X)$. There is a set which is the subset of every set–it is the empty set! So $A = \emptyset$ is the least element.

In retrospect there might have been some confusion since $\emptyset \not\subset \emptyset$ and should not be in the relation as defined; this is all based off of a more complex example, so my apologies for any confusion.

Another important aspect of the relation $<$ is called the 'well-ordering principle.' This is: $\forall x, y \in S, x \neq y, xRy$ or yRx. (E.g., given any two distinct numbers, one is always larger than the other.)

f) Is the relation r on $S = P(X)$ well ordered? Why or why not?

It is not well ordered. Given any two arbitrary sets, it is possible that they are disjoint (so neither is a subset of the other). For example if $X = \{1, 2\}$ then $\{1\}, \{2\} \in P(X)$ but $(\{1\}, \{2\})$ is not in the relation.

4) Consider the relation: $S = \{a, b, c\}; r = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, c)\}$

a) Write the diagram for this relation (with nodes at elements of S and arrows representing 'is related to').

Ask for picture.

b) By use of your diagram, classify this relation (reflexive/irreflexive/neither, symmetric/anti... etc.).

This is reflexive and transitive but neither symmetric nor antisymmetric.