By the way: the midterm is CLOSED BOOK – no notes etc. are allowed.

Answers to the questions

Ex 1. (i) Denote by \([a]_n\) the set of all integers congruent to \(a\) modulo \(n\). Show that

\[ [a]_n + [b]_n = [a + b]_n \]

is well defined.

**Explanation:** To say that an (binary) operation \(*\) on \(X\) is well defined means that to each pair \(x, y\) in \(X\) one can associate an unambiguously defined element \(x \ast y\). So if \(x = [a]_n\) and \(y = [b]_n\), we want to define \(x \ast y\) unambiguously as \([a + b]_n\). But what if we chose the element \(a' \in [a]_n\) instead of \(a\), and \(b' \in [b]_n\) instead of \(b\), we’d then define \(x \ast y\) to be \([a' + b']_n\). For the expression for \(x \ast y\) to be unambiguous, we need to know \([a + b]_n = [a' + b']_n\) when \([a']_n = [a]_n\) and \([b']_n = [b]_n\). This is the content of Prop 2.23.

**Answer** To show that the operation is well defined, we must prove that if \([a']_n = [a]_n\) and \([b']_n = [b]_n\) then \([a + b]_n = [a' + b']_n\). But \([a']_n = [a]_n\) means there is \(k \in \mathbb{Z}\) such that \(a' = a + kn\), and similarly, there is \(\ell \in \mathbb{Z}\) such that \(b' = b + \ell n\).

Therefore \(a' + b' = a + b + n(k + \ell)\), i.e. \([a + b]_n = [a' + b']_n\), as required.

(ii) Find the last digit of \(37^8\).

\(3^4 \equiv_{10} 1\) so we need to find \(7^8 \mod 4\). But \(7 \equiv_4 1\) so \(7^8 \equiv_4 1\). So we have \(3^8 \equiv_{10} 3^1 \equiv_{10} 3\).

Ex 2. Consider the statement:

\[
\left( \forall x \in \mathbb{R}, \quad (x < 0) \implies (\exists n \in \mathbb{Z}, x + n > 0) \right)
\]

(i) Write down its contrapositive, its converse and its negation in as simplified a form as you can.

**CONTRAPOSITIVE:**

\[
\left( \forall x \in \mathbb{R}, \quad \neg(\exists n \in \mathbb{Z}, x + n > 0) \implies \neg(x < 0) \right)
\]

to simplify: note that \(\neg(\exists n \in \mathbb{Z}, x + n > 0)\) is \(\forall n \in \mathbb{Z}, x + n \leq 0\). So simplified statement is:

\[
\left( \forall x \in \mathbb{R}, \quad (\forall n \in \mathbb{Z}, x + n \leq 0) \implies x \geq 0 \right)
\]

**CONVERSE:**

\[
\left( \forall x \in \mathbb{R}, \quad (\forall n \in \mathbb{Z}, x + n > 0) \implies (x < 0) \right).
\]

**NEGATION:**

\[
\left( \exists x \in \mathbb{R}, (x < 0) \land (\forall n \in \mathbb{Z}, x + n \leq 0) \right)
\]
(ii) Of these four statements, which are true, which are false? Justify your answer.

The statement is true: given \( x < 0 \) choose \( n > -x \). So contrapositive is true, and negation is false.

The converse is FALSE. eg take \( x = 1 \) then there is \( n \) (eg \( n = 1 \)) such that \( x + n > 0 \). But \( x \) is NOT \( < 0 \).

**Ex 3.** (i) Define what is meant by saying that a relation \( R \) on the set \( X \) is

a) transitive, b) symmetric, c) antisymmetric

(ii) Let \( X \) be the set of all functions \( f : [0, 1] \to \mathbb{R} \), and let \( R \) be the relation on \( X \) defined by

\[
fRg \iff f(x) = g(x) \quad \text{for some } x \in [0, 1].
\]

d) Sketch the graphs of functions \( f, g, h \in X \) such that \( fRg \) but \( f \not R h \).

\( f, g \) can be any two functions whose graphs over \([0, 1]\) intersect, while the graphs of \( f, h \) should not intersect.

e) Which of the properties (a), (b), (c) does this relation have?

It is reflexive, symmetric, NOT antisymmetric. E.g. let \( f(x) = x, g(x) = \sin x \). Then \( fRg \) since \( f(0) = g(0) \). Also \( gRf \) by symmetry. But \( f \neq g \).

NOT transitive. E.g. take \( f, g \) as above, and \( h \) defined by \( h(x) = -1 \) for \( x < 1 \) and \( h(1) = \sin(1) \). Then \( fRg, gRh \) but \( f \) is not related to \( h \) since \( f(x) > h(x) \) for all \( x \in [0, 1] \).

f) Given \( f \) describe the set \( S[f] \) of all functions \( g \) such that \( fRg \).

This is the set of all functions whose graphs over \([0, 1]\) intersect the graph of \( f \).

h) If \( S[f] = S[g] \) what can you say about \( f \) and \( g \)?

It is true that \( f = g \) in this case. Proof: assume that \( f \neq g \) so that there is \( a \in [0, 1] \) with \( f(a) \neq g(a) \) and then construct \( h \in S_g \) but not in \( S_f \).

**Ex 4.** (i) Let \( f : X \to X \) be a function. What does it mean to say that \( f \) is injective, surjective?

(ii) Show that if \( f \) is surjective so is its composite with itself \( f \circ f : X \to X \).

To say \( f \) surjective means that for all \( x \in X \) there is \( w \in X \) such that \( f(w) = x \). Applying this again, we have \( z \in Z \) so that \( f(z) = w \). Therefore \( f \circ f(z) = f(w) = x \). So \( f \) is surjective.

(iii) Show that if \( f \) is injective, then for any subsets \( A, B \subset X \) we have \( f(A \cap B) = f(A) \cap f(B) \).

By Definition, \( f(A) = \{ y \in X \text{ such that there is } a \in A \text{ with } f(a) = y \} \). Therefore if \( y \in f(A) \cap f(B) \) there is \( a \in A \text{ such that } f(a) = y \) and \( b \in B \text{ such that } f(b) = y \). So \( f(a) = f(b) \). By injectivity we must have \( a = b \). Therefore \( a \in A \cap B \). So \( y \in f(A \cap B) \). Hence \( f(A) \cap f(B) \subset f(A \cap B) \). The other way round is easy and is left to you.
Ex 5. Let $X = \mathbb{N}^+$. Let us say $xRy$ if $x < y + 2$ and $xSy$ if for all $n \in \mathbb{N}^+$, $2^n$ divides $x$ if and only if $2^n$ divides $y$.

(i) Is either of these relations antisymmetric?

If $xRy$ and $yRx$ then $x < y + 2$ and $y < x + 2$. So $x - y < 2$ and $y - x > -2$. We could have $x - y = 1$. i.e. $x = 3, y = 4$ satisfies these conditions. So $R$ is NOT antisymmm.

For each $x \in \mathbb{N}$ let $k(x)$ be the maximal $k$ such that $2^k$ divides $x$. Then $xSy$ implies that $k(x) = k(y)$. But for example $1S3$ and $3S1$ with $1 \neq 3$. So this is not antisymmm either.

(ii) Is either an equivalence relation?

$R$ is clearly not symm. i.e. $2R5$ but $5 \not R 2$. So this is not equiv rel.

But $S$ is reflective, symm and transitive (you should write out some details) so $S$ is equiv rel.

(iii) If one is an equivalence relation, describe the equivalence classes in as simple a way as possible.

Write $x = 2^kz$ where $z$ is odd. Then $xSy$ if $y = 2^kw$ for some odd $w$ (and same $k$.) So: There is one equiv class for each $k \geq 0$. it consists of all positive integers $\{2^ka : a \text{ odd,}\}$.

(iv) If one is antisymmetric, decide if it is a total (i.e. linear) order.

nothing to say; neither is antisymmetric

Ex 6. Let $R$ be a relation on $X$ and define $[x]_R := \{y \in X | xRy\}$.

(i) Suppose that $R$ is an equivalence relation. Show that if $[x]_R \cap [y]_R \neq \emptyset$ then $[x]_R = [y]_R$.

Proof: Let $z \in [x]_R \cap [y]_R$. Then $xRz$ and $yRz$ by definition of equivalence class. Therefore $zRx$ by symmetry. But then we have $yRz$ and $zRx$, so that $yRx$ by transitivity and then $xRy$ by symmetry.

Now suppose that $w \in [x]_R$. Then $xRw$ by definition, so that $wRx$ by symmetry. Thus we have $wRx$ and $xRy$, which implies $wRy$ and $yRw$ (by transitivity and symmetry). i.e. $w \in [y]_R$. This shows that $[x]_R \subseteq [y]_R$.

Interchanging the roles of $x, y$ above we find that $[y]_R \subseteq [x]_R$. Thus $[y]_R = [x]_R$.

(ii) Which properties of an equivalence relation did you use in your proof? Give an example of a relation $R$ that is not an equivalence relation (and not the empty relation) but yet satisfies the statement in (i).

Your proof will probably use symmetry and transitivity, NOT reflexivity. So you can take $R$ to be any relation with these properties. i.e. $X = \{a, b\}$. $R = \{(a,a)\} \subseteq X \times X$. i.e. $aRa$ but nothing else is related to anything else...
Ex 7. Let $f : X \to Y$ be a function, and consider subsets $A, B$ of $X$ and $C, D$ of $Y$. Are the following statements true or false? Give a proof or a counterexample.

(i) If $A \cup B = X$ then $f(A) \cup f(B) = Y$.
This is false because $f$ need NOT be surjective. (You could give explicit counterexample)

(ii) If $C \cup D = Y$ then $f^{-1}(C) \cup f^{-1}(D) = X$.
This is true: for all $x \in X$, $f(x) \in Y$. Since $Y = C \cup D$, $f(x)$ lies in either $C$ or $D$. Therefore $x$ lies in either $f^{-1}(C)$ or $f^{-1}(D)$.

(iii) If $A \cap B = \emptyset$ then $f(A) \cap f(B) = \emptyset$.
This is false. eg $X = \{1, 2\}$, $Y = \{1\}$, $f : X \to Y$ is the unique function and $A = \{1\}, B = \{2\}$.

(iv) If $C \cap D = \emptyset$ then $f^{-1}(C) \cap f^{-1}(D) = \emptyset$.
This is TRUE. If $f^{-1}(C) \cap f^{-1}(D) \neq \emptyset$, there is $x \in f^{-1}(C) \cap f^{-1}(D)$. But then $f(x) \in C \cap D$, contradicting the fact that $C \cap D = \emptyset$. 