Name:
Student ID number:

prob.	score
1	
2	
3	
4	
5	
6	
7	
8	
9	
total	

1. Suppose $f : A \to B$. Define the inverse set as

$$f^{-1}(b) = \{a \in A \mid f(a) = b\} \quad \text{for } b \in B.$$

Note that $f^{-1}(b)$ is a *set*. Prove that the collection of these inverse sets

$$\{f^{-1}(b) \mid b \in B\}$$

is a partition of A. *Hint:* You need to show two properties. First, prove that for all $a \in A$, there is some b such that $a \in f^{-1}(b)$. Second, show that each $a \in A$ belongs to *only one* set $f^{-1}(b)$ (and hence the sets $f^{-1}(b)$ must be disjoint).

Proof: to show that the collection of sets $f^{-1}(b)$ is a partition of A we must show that ① the union of all sets $f^{-1}(b)$ forms all of A, and ② these sets are all mutually disjoint.

① $A = \bigcup_{b \in B} f^{-1}(b)$: (i.e. A = the union of all sets $f^{-1}(b)$)

$A \subseteq \bigcup_{b \in B} f^{-1}(b)$:

let $x \in A$. Then since f is a f'n, $\exists b' \in B$ st $f(x) = b'$. so $x \in f^{-1}(b')$, and is thus in the union of all such sets.

$\bigcup_{b \in B} f^{-1}(b) \subseteq A$:

let $x \in \bigcup_{b \in B} f^{-1}(b)$. By def union, $\exists b \in B$ st. $x \in f^{-1}(b)$. By def'n, $f^{-1}(b) = \{x' \in A \mid f(a) = b\}$. so $f^{-1}(b) \subseteq A$, and so $x \in A$.

② $f^{-1}(b_i) \cap f^{-1}(b_j) = \emptyset \quad \forall i \neq j,\ b_i, b_j \in B$

Since f is a f'n, $\forall a \in A$, f maps a to a single element, call it $b \in B$ So a is only in one set $f^{-1}(b)$. And $f^{-1}(b) \subseteq A$, so it is only made of elements of A. Since we showed any $a \in A$ can only ... they are mutually disjoint. ∎

2. Suppose A is countable and B is uncountable. Is $A \cap B$ countable? Is $A \cup B$ countable? Why?

$A \cap B \subseteq A$. A is countable. Therefore $A \cap B$ is countable because any subset of a countable set is countable.

$B \subseteq A \cup B$. B is uncountable. Therefore $A \cup B$ is uncountable because any set with an uncountable subset is uncountable.

3. Prove by induction that

$$\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3} \quad \text{for } n \geq 1.$$

Define $P(n)$: $\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$

Proof: $\boxed{\text{Base case.}}$ Prove $P(1)$.

[wts. $\sum_{i=1}^{1} i(i+1) = \frac{1(1+1)(1+2)}{3} = 2$]

$$\sum_{i=1}^{1} i(i+1) = 1(2) = 2.$$

$\frac{n(n+1)(n+2)}{3} = 2$ when $n = 1$.

The two sides are equal so the base case holds.

$\boxed{\text{Inductive Hypothesis}}$ let $k \geq 1$, [a fixed, arbitrary k] and assume $P(k)$ holds.

That is $\sum_{i=1}^{k} i(i+1) = \frac{k(k+1)(k+2)}{3}$.

$\boxed{\text{Inductive Step}}$ we must prove $P(k+1)$ holds.

[wts $\sum_{i=1}^{k+1} i(i+1) = \frac{(k+1)(k+1+1)(k+1+2)}{3}$].

$$\sum_{i=1}^{k+1} i(i+1) = \sum_{i=1}^{k} i(i+1) + (k+1)(k+2) \quad \text{by separating terms.}$$

$$= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2) \quad \text{by applying I.H. to first term.}$$

$$= \frac{k(k+1)(k+2) + 3(k+1)(k+2)}{3} \quad \text{algebra}$$

$$= \frac{(k+1)(k+2)(k+3)}{3} \quad \text{— " —}$$

and this is what we wanted to show. □

4. Define the *fibonacci* sequence as

$$f_1 = 1$$
$$f_2 = 1$$
$$f_i = f_{i-1} + f_{i-2} \quad \text{for } i \geq 3.$$

Using induction, prove that f_{3k} is even for all $k \geq 1$ (*e.g.* f_3 is even, f_6 is even, *etc.*).

Define $P(k)$: f_{3k} is even.

Proof:

Basis step

Base case $k=1$. Want to show $P(1)$, ie that f_3 is even.

By def of sequence

$f_3 = f_2 + f_1$ (because $3 \geq 3$). by def sequence.

$= 1 + 1$

$= 2$

2 is even because $2 = 2 \cdot 1$, $1 \in \mathbb{Z}$, so $P(1)$ holds.

Inductive Hypothesis

Let $k \geq 3$ be a fixed but arbitrary k, and assume $P(j)$ holds for all $1 \leq j \leq k$. That is f_{3j} is even.

Inductive Step: Want to show $P(k+1)$, that is $f_{3(k+1)}$ is even.

$f_{3(k+1)} = f_{3k+3}$ by expanding subscript.

By def of sequence, $f_{3k+3} = f_{3k+2} + f_{3k+1}$.

$= f_{3k+1} + f_{3k} + f_{3k+1}$ by def seq.

$= f_{3k} + 2f_{3k+1}$ by grouping terms

$= f_{3k} + 2(f_{3k} + f_{3k-1})$ by def seq

since $k, k-1 \leq k$, can apply inductive hypothesis, so $\exists\, m, n \in \mathbb{Z}$ s.t.

$f_{3k+3} = 2m + 2(2m + 2n) = 2(m + 2m + 2n)$. Since $(m + 2m + 2n) \in \mathbb{Z}$, f_{3k+3} even by def even. $\square$

5. Let d and k be positive integers. Define a relation R on $\mathbb{Z}$ as

$$(x, y) \in R \text{ if } d \mid (x^k - y^k).$$

Prove that R is an equivalence relation.

Proof:

R is an equivalence relation iff and only if it is reflexive, symmetric, and transitive.

Let $d, k \in \mathbb{Z}^+$ be fixed but arbitrary positive integers.

Reflexive: [wts. $\forall x \in \mathbb{Z}$, xRx]

Let $x \in \mathbb{Z}$. Then $x^k = x^k$, so $x^k - x^k = 0$.

And $d \mid 0$ b/c $0 = d \cdot 0$.

so $d \mid (x^k - x^k)$ so xRx by def R. $\square$

Symmetric [wts $\forall x, y \in \mathbb{Z}$, if xRy then yRx]

let $x, y \in \mathbb{Z}$ s.t. xRy.

By def. of R, $d \mid (x^k - y^k)$

By def. divisibility, $x^k - y^k = dl$ for some $l \in \mathbb{Z}$.

multiplying by (-1) on both sides,

$$y^k - x^k = -dl.$$

$$y^k - x^k = d(-l).$$

Since $-l \in \mathbb{Z}$, $d \mid (y^k - x^k)$ by def. divisibility.

so yRx by def. R. $\square$

Transitive [wts $\forall x, y, z \in \mathbb{Z}$, if xRy and yRz, then xRz].

let $x, y, z \in \mathbb{Z}$ st. xRy and yRz.

By def R, $d \mid (x^k - y^k)$ and $d \mid (y^k - z^k)$.

Note that $(x^k - y^k) + (y^k - z^k) = x^k - z^k$. (+)

By def divisibility, $x^k - y^k = ld$ for $l \in \mathbb{Z}$ and $y^k - z^k = md$ for $l \in \mathbb{Z}$.

So $(x^k - y^k) + (y^k - z^k) = md + ld = d(m + l)$. Since $m + l \in \mathbb{Z}$, $d \mid (x^k - y^k) + (y^k - z^k)$ by def divis.

Subbing in from (+), $d \mid (x^k - z^k)$.

So xRz by def R. $\square$

[NOTE: since it is not specified in the problem, you could also pv. the equality algebraically].

6. Prove that for any sets A, B, C

$$(A - B) \cap (A - C) = A - (B \cup C).$$

To prove equality we will prove both subset relations.

① $(A-B)\cap(A-C) \subseteq A-(B\cup C)$:

Let $x \in (A-B)\cap(A-C)$. Then by def intersection, $x \in A-B$ and $x \in A-C$. So $x \in A$ and $x \notin B$ and $x \in A$ and $x \notin C$, by def set difference. In particular $x \in A$. Since $x \notin B$ and $x \notin C$, $x \in B^c$ and $x \in C^c$ by def complement. So $x \in B^c \cap C^c = (B\cup C)^c$ by def intersection, and De Morgan's Law. So $x \notin B\cup C$ by def complement. Since $x \in A$ and $x \notin B\cup C$, $x \in A-(B\cup C)$ by def set difference.

② $A-(B\cup C) \subseteq (A-B)\cap(A-C)$:

Let $x \in A-(B\cup C)$, so $x \in A$ and $x \notin B\cup C$. So $x \in (B\cup C)^c$ so $x \in B^c \cap C^c$ by De Morgan's Law. So $x \notin B$ and $x \notin C$ by def complement. Since $x \in A$ and $x \notin B$, $x \in A-B$ by def set difference. Since $x \in A$ and $x \notin C$, $x \in A-C$ by def set difference. So $x \in (A-B)\cap(A-C)$ by def intersection. ☐

Note: instead of using de morgan's laws for sets, you could have used the following logic in the appropriate places in

① since $x \notin B$ and $x \notin C$ then x is not in B or C (by the logical De Morgan's Law). So $x \notin B\cup C$ by def union.

② since $x \notin B\cup C$, i.e. x is not in $(B$ or $C)$, so x is not in B and x is not in C by the logical De Morgan's Law). So $x \notin B$ and $x \notin C$.

7. How many elements does $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$ have? ($\mathcal{P}(A)$ denotes the powerset of A).

ϕ has 0 elements.

$P(\phi) = \{\phi\}$ has one elements.

The powerset of a set containing n elements has 2^n elements, [Thm. from class].

Since $P(\phi)$ contains 1 elt, $P(P(\phi)) = \{\phi, \{\phi\}\}$ contains $2^1 = 2$ elts.

Since $P(P(\phi))$ contains 2 elts, $P(P(P(\phi)))$ contains $2^2 = \boxed{4}$ elements

Note:

Set name	Set
ϕ	$\{\}$
$P(\phi)$	$\{\phi\}$
$P(P(\phi))$	$\{\phi, \{\phi\}\}$
$P(P(P(\phi)))$	$\{\phi, \{\phi\}, \{\{\phi\}\}, \{\phi, \{\phi\}\}\}$

8. A relation R on A is *circular* if for all $x, y, z \in A$, xRy and yRz implies zRx. Show that a reflexive circular relation is an equivalence relation.

Proof.

Reflexive: This is given, as we are told the relation is a "reflexive circular relation."

symmetric: [wts $\forall x, y \in A$, if xRy then yRx]

Let $x, y \in A$ st. xRy. From reflexive, we know that yRy. From definition of circular, we have that yRx. [ie. let $y = z$ in the definition above so xRy and $yRy \rightarrow yRx$]

transitive: [wts $\forall x, y, z \in A$, if xRy and yRz then xRz]. Let $x, y, z \in A$ st. xRy and yRz. By def'n circular zRx. But we have shown above that R is symmetric, so xRz.

$\square$

9. Suppose that $f : A \to B$, $g : B \to C$ are both onto. Prove that $g \circ f$ is onto.

proof. Let $f: A \to B$, $g: B \to C$ both be onto.

[wts $g \circ f$ onto, ie $\forall c \in C$, $\exists a \in A$ st. $(g \circ f)(a) = c$].

Let $c \in C$. Since g is onto, $\exists b \in B$ st $g(b) = c$. Since f is onto, $\exists a \in A$ st. $f(a) = b$. So $g(f(a)) = g(b) = c$. since $g(f(a)) = (g \circ f)(a)$ by def composition of f'ns, we have given an a s.t. $(g \circ f)(a) = c$. Therefore $g \circ f$ is onto by definition onto. $\square$