Math 251W: Foundations of Advanced Mathematics

Portfolio problems from sections 6.4, 5.1, & 5.2

Problem 6.3.11: Prove the following

proposition:

$$P(n): \qquad \prod_{i=2}^{n}\left(1-\frac{1}{i^2}\right)=\frac{n+1}{2n} \qquad \forall n \geq 2$$

proof (PMI-I) Let n be an arbitrary natural number such that $n \geq 2$. Consider the base-case where $n = 2$. By substituting,

$$\prod_{i=2}^{n}\left(1-\frac{1}{i^2}\right)=\left(1-\frac{1}{2^2}\right)=\frac{3}{4}=\frac{2+1}{2(2)}=\frac{n+1}{2n}.$$

Thus, the base case is true.
Suppose $k \geq 2$ is an arbitrary natural number such that

$$\prod_{i=2}^{k}\left(1-\frac{1}{i^2}\right)=\frac{k+1}{2k}.$$

Consider $k + 1$. By the associative, communitative, and distributive properties of real numbers, and substitution,

$$\prod_{i=2}^{k+1}\left(1-\frac{1}{i^2}\right)=\prod_{i=2}^{k}\left(1-\frac{1}{i^2}\right)\left(1-\frac{1}{(k+1)^2}\right)=\frac{k+1}{2k}\left(1-\frac{1}{(k+1)^2}\right)$$

$$=\frac{k+1}{2k}-\frac{1}{2k(k+1)}=\frac{(k+1)^2-1}{2k(k+1)}=\frac{(k+1)+1}{2(k+1)}.$$

Hence $P(k + 1)$ holds. Since k is an arbitrary natural number such that $k \geq 2$, $P(k)$ implies $P(k + 1)$ for all natural numbers greater than two. Thus, by way of induction,

$$P(n): \qquad \prod_{i=2}^{n}\left(1-\frac{1}{i^2}\right)=\frac{n+1}{2n} \qquad \forall n \geq 2.$$

Problem 6.3.12: Prove the following

proposition: For all $(n \geq 2) \in \mathbb{N}$,

$$\sum_{i=1}^{n} \frac{1}{\sqrt{i}} > \sqrt{n}.$$

proof: For proof by induction, consider the case where $n = 2$. Hence we have

$$\left(\sum_{i=1}^{2} \frac{1}{\sqrt{i}} = 1 + \frac{1}{\sqrt{2}} = \frac{\sqrt{2}+1}{\sqrt{2}} \right) > \left(\frac{2}{\sqrt{2}} = \sqrt{2} \right).$$

Thus, the base case holds.

Now suppose the statement holds for some particular $(n \geq 2) \in \mathbb{N}$, such that

$$\sum_{i=1}^{n} \frac{1}{\sqrt{i}} > \sqrt{n}.$$

By the associative property of addition,

$$\sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} = \sum_{i=1}^{n} \frac{1}{\sqrt{i}} + \frac{1}{\sqrt{1+n}}.$$

By induction hypothesis,

$$\sum_{i=1}^{n} \frac{1}{\sqrt{i}} + \frac{1}{\sqrt{1+n}} > \sqrt{n+1}$$

. By way of induction, it follows that for all $(n \geq 2) \in \mathbb{N}$,

$$\sum_{i=1}^{n} \frac{1}{\sqrt{i}} > \sqrt{n}.$$

Problem Irreducible Polynomials: Prove the following

proposition: Every reducible polynomial can be written as a product of irreducible polynomials. (AKA) for all $n \in \mathbb{N}$, reducible polynomials of degree n can be written as the product of irreducible polynomials.

proof (Strong Induction) The lowest possible degree for a polynomial to be reducible is degree $n = 2$.

For proof by induction, consider the base case $n = 2$. Let p be an arbitrary reducible polynomial of degree 2. By definition of reducible polynomials, $p_2 = q_a r_b$, where q_a and r_b are polynomials of degrees a and b, such that $a, b < 2$. Furthermore, since $a, b < 2$, q_a and r_b are either of degree 1 or 0, both of which are degrees at which all polynomials are irreducible. Thus, since p_2 is arbitrary, all polynomials of degree 2 can be written as a product of irreducible polynomials, hence the base case holds.

For the induction hypothesis, suppose all reducible polynomials of a particular degree i can be written as the product of reducible polynomials for all $i \leq n$ for some particular $n \in \mathbb{N}$.
Consider an arbitrary polynomial of degree $i+1$, p_{i+1}, such that p_{i+1} is reducible. By definition of reducible polynomials, $p_{i+1} = q_a r b$, where q_a and r_b are polynomials of degree a and b respectively, where a and b are natural numbers less than $i+1$. By the induction hypothesis, these polynomials can be written as a product of irreducible polynomials. Furthermore, by substitution and the associative property, p_{i+1} can be written as the product of irreducible polynomials. Since p_{i+1} is arbitrary, this applies to all reducible polynomials of degree $i + 1$.

Thus, by way of strong induction, all reducible polynomials can be written as a product of irreducible polynomials.

Problem 6.4.6: Prove the following

proposition: For all $n \in \mathbb{N}$ such that $n > 5$, $F_n = 5F_{n-4} + 3F_{n-5}$.

proof For proof by induction, consider the base case where $n = 6$. By definition of the Fibonacci sequence, $F_6 = 8$, $F_2 = 1$, and $F_1 = 1$. By substitution $F_6 = 5(1) + 3(1) = 8$. Thus the base case hold.

Suppose by way of strong induction that $F_i = 5F_{i-4} + 3F_{i-5}$ for all $i \leq n$ for some particular $(n > 6) \in \mathbb{N}$. Consider F_{i+1}. By definition of the Fibonacci sequence, $F_{i+1} = F_i + F_{i-2}$. By the induction hypothesis,

$$F_{i+1} = 5F_{i-4} + 3F_{i-5} + F_{i-2} = 5F_{i-4} + 3F_{i-5} + F_{i-2} + F_{i-3}$$

$$= 5F_{i-4} + 3F_{i-5} + F_{i-3} + F_{i-4} + F_{i-3}$$

$$= (3F_{i-4} + 3F_{i-5}) + 2F_{i-3} + 3F_{i-4}$$

$$F_{i+1} = 5F_{(i+1)-4} + 3F_{(i+1)-5}.$$

Thus, by way of strong induction, for all $n \in \mathbb{N}$ such that $n > 6$, $F_n = 5F_{n-4} + 3F_{n-5}$.

Problem 6.4.14(1i): Prove the following

Given $P_1 = 1$, $P_{n+1} = P_n + (3n+1)$, $T_1 = 1$, $T_{n+1} = T_n + (n+1)$, $L_1 = 1$, and $L_{n+1} = L_n + 1$ for all $n \in \mathbb{N}$,

proposition: $P_n = 3T_n - 2L_n$ for all $n \in \mathbb{N}$

proof For proof by induction consider the base case where $n = 1$. It is given that $P_1 = 1$, and that $T_1 = 1$, and that $L_1 = 1$. Thus, $P_1 = 1 = 3(1) - 2(1) = 3T_1 - 2T_1$.

For our induction hypothesis, suppose that $P_n = 3T_n - 2L_n$ for for some particular $n \in \mathbb{N}$. Consider P_{n+1}. By definition of P, $P_{n+1} = P_n + (3n + 1)$. By the induction hypothesis and by definition of T and L,

$$P_{n+1} = 3T_n - 2L_n + (3n + 1) = 3(T_{n+1} - (n + 1)) - 2(L_{n+1} - 1) + (3n + 1)$$

$$= 3T_{n+1} - 3n - 3 - 2L_{n+1} + 2 + 3n + 1$$

$$P_{n+1} = 3T_{n+1} - 2L_{n+1}.$$

Thus, by way of induction, $P_n = 3T_n - 2L_n$ for all $n \in \mathbb{N}$.

Problem 5.1.8

Let A be a set. Let $\{R_i\}_{i \in I}$ be a family of relations on A indexed by the nonempty set I.

a Prove each of the following propositions:

i If R_i is reflexive for all $i \in I$ then $\bigcap_{i \in I} R_i$ is reflexive

ii If R_i is symmetric for all $i \in I$ then $\bigcap_{i \in I} R_i$ is symmetric

iii If R_i is transitive for all $i \in I$ then $\bigcap_{i \in I} R_i$ is transitive

proof Let A be an arbitrary set, and let $\{\mathcal{R}_i\}_{i \in I}$ be a family of relations on A indexed by the nonempty set I.

i Suppose $\mathcal{R}_i$ is reflexive for all $i \in I$. Let x be an arbitrary element A. By supposition and the definition of reflexive relations, $(x, x) \in \mathcal{R}_i$ for all $i \in I$. By definition of the intersection of an indexed family of sets, $(x, x) \in \bigcap_{i \in I} \mathcal{R}_i$. Since x is an arbitrary element in A, for all $x \in A$, $(x, x) \in \bigcap_{i \in I} \mathcal{R}_\rangle$. Thus, by definition of reflexive relations, $\bigcap_{i \in I} \mathcal{R}_i$ is reflexive.

ii Suppose $\mathcal{R}_i$ is symmetric for all $i \in I$. Let x and y be arbitrary elements in A such that $(x, y) \in \mathcal{R}_i$ for all $i \in I$. Let $\mathcal{R}_i$ be an arbitrary element in $\{R_i\}_{i \in I}$. Since $\mathcal{R}_i$ is symmetric, $(y, x) \in \mathcal{R}$. Since $\mathcal{R}_\rangle$ is arbitrary, this applies to the entire family $\{\mathcal{R}_i\}_{i \in I}$. By definition of the intersection of an indexed family of sets, $(y, x) \in \bigcap_i \mathcal{R}_i$. Furthermore, since (x, y) is an arbitrary element in $A \times A$, by definition of a symmetric relation, $\bigcap_{i \in I} \mathcal{R}_\rangle$ is symmetric.

iii Suppose R_i is transitive for all $i \in I$. Let a, b and c be arbitrary elements in A such that $(a, b), (b, c) \in \bigcap_{i \in I} R_i$. Let i be an arbitrary element in I. By definition of the intersection of an indexed family of sets, $(a, b), (b, c) \in \mathcal{R}_i$. Since R_i is transitive, $(a, c) \in \mathcal{R}_i$. Since i is an arbitrary element in I, $(a, c)]in\mathcal{R}_i)$ for all $i \in I$. By definition of the intersection of an indexed family of sets, $(a, c) \in \bigcap_{i \in I} \mathcal{R}_i$. Since a, b and c are arbitrary elements in A, $\bigcap_{i \in I} \mathcal{R}_i$ is transitive.

b Find a counterexample to the proposition: If R_i is transitive for all $i \in I$ then $\bigcup_{i \in I} R_i$ is transitive

counterexample Consider the relation $\mathcal{F}_1$ on the set of all people, $\mathcal{P}$, defined $a\mathcal{F}_1 b$ if and only if a is friends with b. Let Fred and Sal be people such that Sal is friends with Fred, that is $Fred\mathcal{F}Sal$. Consider another relation, $\mathcal{F}_2$ on the set of all people defined, $a\mathcal{F}_2 b$ if and only if a is dating b. Suppose Fred goes to some far away place and begins dating someone Sal has never heard of. However, as Sal has never heard of Jen, and vice versa, it follows that $Jen \not\mathcal{F}Sal$. Consider the union $\mathcal{F}_1 \cup \mathcal{F}_2$, that is, $a(\mathcal{F}_1 \cup \mathcal{F}_2)b$ if a is either friends with or dating b. By definition of unions, $Sal(\mathcal{F}_1 \cup \mathcal{F}_2)Fred$ and $Fred(\mathcal{F}_1 \cup \mathcal{F}_2)Jen$ and $Sal \not(\mathcal{F}_1 \cup \mathcal{F}_2)Jen$. Thus, the union is not transitive. That is, if I am either dating or friends with person A, and person A is either dating or friends with person B, it does not follow that I am friends with or dating person B.

Problem 5.1.11

3 proposition: If $\mathcal{R}$ is a transitive relation on the set A and $x\mathcal{R}y$ then $[y] \subseteq [x]$

proof Let A be an arbitrary set and let $\mathcal{R}$ be an arbitrary relation on A. Suppose $\mathcal{R}$ is a transitive. Let x and y be arbitrary elements of A such that $x\mathcal{R}y$. Let a be an arbitrary element of the relation class $[y]$. By definition of the relation class, $y\mathcal{R}a$. Since $x\mathcal{R}y$ and $y\mathcal{R}a$, by definition of transitivity, $x\mathcal{R}a$. By definition of the relation class, $a \in [x]$. Since a is an arbitrary element of $[y]$, by definition of subsets, $[y] \subseteq [x]$.

Problem 5.2.4

proposition: Let $n, q \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. Suppose $a \equiv b \pmod{n}$ and that $q|n$. Then $a \equiv b \pmod{q}$.

proof Let n and q be arbitrary natural numbers and a and b be arbitrary integers. Suppose that $a \equiv b \pmod{q}$ and $q|n$. By definition of modular congruence, $n|a - b$. Furthermore, by definition of divides, there exists integers x and y such that $xn = a - b$ and $yq = n$. By substitution, $xyq = a - b$. By the closure property of integers under multiplication, xy is an integer, hence there exists some integer $k = xy$ such that $kq = a - b$. By definition of divides, $q|a - b$. By definition of modular congruence, $a \equiv b \pmod{q}$.

Problem 5.2.9 proposition: Given $n \in \mathbb{N}$, one of the following is true: $n^2 \equiv 0 \mod 16$, $n^2 \equiv 1 \mod 8$, or $n^2 \equiv 4 \mod 8$

proof Let n be an arbitrary natural number. There are four cases: $n = 4q - 3$, $n = 4q - 2$, $n = 4q - 1$, $n = 4q$. Since $n = 4q$, and since q is an integer, by definition of divides $4|n$. By definition of modular congruence, $n \equiv 0 \pmod 4$. Thus, we find that the set of all n of the form $n = 41$ for some integer q is [4]. FUrhtermore, we find that the other three cases are $[1], [2], [3]$. By definition of the quotient class for congruence modulo some natural number, the set of these cases forms $\mathbb{Z}_4$. By theorem, the union of $\mathbb{Z}_4 = \mathbb{Z}$. Since $\mathbb{N} \subseteq \mathbb{Z}$, these four cases encapsulate all natural numbers.

1. Consider the case where $n = 4q-3$. Then $n^2 = 16q^2-24q+9 = 8(2q^2-3q+1)+1$. Subtracting one, $n^2 - 1 = 8(2q^2 - 3q + 1)$. By the closure property of integers over multiplication and addition, $x = 2q^2-3q+1$ is an integer, thus there exists some integer x such that $8x = n^2-1$. By definition of divides, $8|(n^2 - 1)$. By definition of modular congruence, $n^2 \equiv 1 \pmod 8$.
2. Consider the case where $n = 4q-2$. Then $n^2 = 16q^2-16q-4 = 8(2q^2-2q)+4$. Subtracting four, $n^2 - 4 = 8(2q^2 - 2q)$. By the closure property of integers over multiplication and addition, $y = 2q^2 - 2q$ is an integer. Thus there exists some integer x such that $8y = n^2 - 4$. By definition of divides, $8|(n^2 - 4)$. By definition of modular congruence, $n^2 \equiv 4 \pmod 8$.
3. Consider the case where $n = 4q - 1$. Then $n^2 = 16q^2 - 8q + 1 = 8(2q - q) + 1$. Subtracting one, $n^2 - 1 = 8(2q - q)$. Furthermore, since $z = 2q - q$ is an integer, by definition of divides, $8|n^2 - 1$. By definition of modular congruence, $n^2 \equiv 1 \pmod 8$.
4. Consider the case where $n = 4q$. Then $n^2 = 16q^2$. Since q^2 is an integer, $16|n^2$. Thus, by definition of modular congruence, $n^2 \equiv 0 \pmod{16}$.

■

Problem 5.2.10

proposition: Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. Then $\gamma(a + b) = \gamma(a) + \gamma(b)$ and $\gamma(ab) = \gamma(a) \cdot \gamma(b)$.

proof (Direct)

Let n be an arbitrary natural number and let γ be the canonical map $\gamma : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\gamma(x) = [x]$ for all $x \in \mathbb{Z}$. Since we are trying to prove two results, this proof will be divided into two parts.

- Let a and b be arbitrary integers. Consider $\gamma(a + b)$. By definition of γ, $\gamma(a + b) = [a + b]$. By properties defined on the relation class for modular congruence, $\gamma(a + b) = [a + b] = [a] + [b]$. Furthermore, since a and b are integers, $\gamma(a) = [a]$ and $\gamma(b) = [b]$. By substitution, $\gamma(a + b) = \gamma(a) + \gamma(b)$. Since a and b are arbitrary integers, $\gamma(a + b) = \gamma(a) + \gamma(b)$ for all integers a and b.
- Let a and b be arbitrary integers. Consider $\gamma(ab)$. By definition of γ, $\gamma(ab) = [ab]$. By the operations defined on congruence classes, $[ab] = [a] \cdot [b]$. Furthermore, since $[a]$ and $[b]$ are integers, $\gamma(a) = [a]$ and $\gamma(b) = [b]$. By substitution, $\gamma(ab) = \gamma(a)\dot{\gamma}(b)$. Since a and b are arbitrary integers, $\gamma(ab) = \gamma(a)\dot{\gamma}(b)$ for all integers a and b.

■