MCS 150 Final Exam Solutions

1. (10 pts) Prove that $\sqrt[3]{2}$ is irrational.

   First, we prove a

   Lemma. *Let n be an integer. If n^3 is even then n is even.*

   Proof: We will prove the contrapositive: if n is not even then n^3 is not even. So let n be an integer. Suppose n is not even. Then n is odd and $n = 2q + 1$ for some $q \in \mathbb{Z}$. So

   $$n^3 = (2q+1)^3 = 8q^3 + 12q^2 + 6q + 1 = 2(4q^3 + 6q^2 + 3q) + 1.$$

   Since q is an integer, $4q^3$, $6q^2$, and $3q$ are also integers, and so is their sum $4q^3 + 6q^2 + 3q$. Hence n^3 is odd and therefore n^3 is not even. □

   Now, suppose the $\sqrt[3]{2}$ is rational. Then $\sqrt[3]{2} = m/n$ for some $m, n \in \mathbb{Z}$ such that $n \neq 0$. We can always reduce the fraction to lowest terms, so assume that m and n have no nontrivial common factor. Now,

   $$2 = \left(\frac{m}{n}\right)^3 = \frac{m^3}{n^3} \implies n^3 = 2m^3.$$

   Since $2m^3$ is even, n^3 must be even as well. Therefore n is also even by the lemma above. So $n = 2k$ for some $k \in \mathbb{Z}$. Now

   $$2m^3 = n^3 = (2k)^3 = 8k^3 \implies m^3 = 4k^3 = 2(2k^3).$$

   Since the $2(2k^3)$ is even, m^3 must be even as well. Therefore m is also even by the lemma. But if m and n are both even, then 2 is a common factor of m and n. This contradicts the assumption we made earlier about m/n being a fraction in lowest terms. So $\sqrt[3]{2}$ must be rational.

2. (10 pts) Let A and B be arbitrary nonempty sets. Under what conditions is $(A \times B) \cap (B \times A)$ empty? Do not forget to fully justify your answer.

   We will show that $(A \times B) \cap (B \times A)$ is empty if and only if A and B are disjoint, that is $A \cap B$ is empty. First, we prove if $(A \times B) \cap (B \times A) = \emptyset$ then $A \cap B = \emptyset$ by proving the contrapositive: if $A \cap B \neq \emptyset$ then $(A \times B) \cap (B \times A) \neq \emptyset$. So suppose $A \cap B \neq \emptyset$. Then there is some element x that is both in A and B. Hence the ordered pair (x, x) is both in $A \times B$ and $B \times A$. Therefore $(A \times B) \cap (B \times A)$ is nonempty.

   We will now prove if $A \cap B = \emptyset$ then $(A \times B) \cap (B \times A) = \emptyset$ by proving the contrapositive: if $(A \times B) \cap (B \times A) \neq \emptyset$ then $A \cap B \neq \emptyset$. So suppose $(A \times B) \cap (B \times A) \neq \emptyset$. Then there is an ordered pair (x, y) that is in both $A \times B$ and $B \times A$. Since $(x, y) \in A \times B$, x must be in A and y must be in B. But (x, y) is also in $B \times A$, so x must be in B and y must be in A. Thus $x \in A \cap B$, and hence $A \cap B$ is nonempty. (Now, y could be another element in $A \cap B$, or y could be the same thing as x, but it does not matter since we already showed that $A \cap B$ has at least one element.)

3. (10 pts) Given any arbitrary integers a, b, and c, show that if $a|c$, $b|c$, and $\gcd(a, b) = 1$ then $ab|c$.

   Suppose $a|c$, $b|c$, and $\gcd(a, b) = 1$. Since $a|c$ and $b|c$, there exist $q, r \in \mathbb{Z}$ such that $c = qa = rb$. Because $\gcd(a, b) = 1$, we also know $1 = sa + tb$ for some $s, t \in \mathbb{Z}$. Hence

   $$c = c(sa + tb) = sac + tbc = sarb + tbqa = (sr + tq)(ab).$$

   Since s, r, t and q are all integers, so is $sr + tq$. Therefore $ab|c$.

4. (10 pts) Recall that we defined the Fibonacci numbers $\{F_n\}_{n=0}^{\infty}$ by $F_0 = 0$, $F_1 = 1$ and the recurrence relation

$$F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 2.$$

Use induction to prove that

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

for every positive integer n.

If $n = 1$ then

$$F_{1+1}F_{1-1} - F_1^2 = F_2F_0 - F_1^2 = 1(0) - 1^2 = -1 = (-1)^1,$$

which establishes the base case for the induction.

For the inductive hypothesis, suppose

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

for some positive integer n. We will prove that

$$F_{(n+1)+1}F_{(n+1)-1} - F_{n+1}^2 = (-1)^{n+1}.$$

First,

$$F_{(n+1)+1}F_{(n+1)-1} - F_{n+1}^2 = F_{n+2}F_n - F_{n+1}^2.$$

Since $F_{n+2} = F_{n+1} + F_n$,

$$F_{n+2}F_n = (F_{n+1} + F_n)F_n = F_{n+1}F_n + F_n^2.$$

Since $F_{n+1} = F_n + F_{n-1}$,

$$F_{n+1}^2 = F_{n+1}F_{n+1} = (F_n + F_{n-1})F_{n+1} = F_nF_{n+1} + F_{n-1}F_{n+1}.$$

Hence

$$\begin{aligned} F_{n+2}F_n - F_{n+1}^2 &= F_{n+1}F_n + F_n^2 - F_nF_{n+1} - F_{n-1}F_{n+1} \\ &= F_n^2 - F_{n-1}F_{n+1} \\ &= -(F_{n+1}F_{n-1} - F_n^2) \\ &= -(-1)^n \\ &= (-1)^{n+1}. \end{aligned}$$

by the inductive hypothesis. It follows by induction that

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

for all $n \in \mathbb{Z}^+$.

5. (10 pts) Let S be a finite set. Prove that the cardinality of the power set of S is

$$|\mathcal{P}(S)| = 2^{|S|}.$$

We gave several proofs of this. Here is the shortest of them. Since $\mathcal{P}(S)$ is the set of all subsets of S, the cardinality of $\mathcal{P}(S)$ is the number of different subsets of S. To form any subset T of S, we can decide for each element $x \in S$ whether to include it in T or not. That is two possible choices for each element of S. The choice for each element of S is independent of the choices for the other elements. Therefore this gives us $2 \cdot 2 \cdots 2$ choices for constructing the subset T, where the number of 2s in the product is exactly the number of elements of S. Hence $|\mathcal{P}(S)| = 2^{|S|}$.

For some reason, the popular choice among you was another proof we gave which uses induction. It is a good example of using induction, but it is not the most efficient proof that $|\mathcal{P}(S)| = 2^{|S|}$. But here it is to show you how the correct argument goes.

Let $n = |S|$. We want to prove $|\mathcal{P}(S)| = 2^n$. We will induct on n. For the base case, let $n = 0$. So S has no elements, that is $S = \emptyset$. Then the only subset of S is $\emptyset$, so

$$\mathcal{P}(S) = \{\emptyset\} \implies |\mathcal{P}(S)| = 1 = 2^0,$$

exactly as it should be.

For the inductive hypothesis, assume that it is true for some $n \in \mathbb{Z}^{\geq 0}$ that for any set S such that $|S| = n$, $|\mathcal{P}(S)| = 2^n$.

We now want to prove that if S is any set such that $|S| = n + 1$ then $|\mathcal{P}(S)| = 2^{n+1}$. Pick any element $x \in S$. Let T be set that consists of all of the elements of S except for x, that is $T = S - \{x\}$. It is clear that $|T| = n$ and hence $|\mathcal{P}(T)| = 2^n$ by the inductive hypothesis. So T has 2^n different subsets $T_1, T_2, \ldots, T_{2^n}$. Since $T \subseteq S$, each of these is also a subset of S. Now, add x to each of the T_i, that is consider the sets

$$T_1 \cup \{x\}, T_2 \cup \{x\}, \ldots, T_{2^n} \cup \{x\}.$$

Since $x \in S$, these are also subsets of S. There are 2^n of them. It is easy to see that

$$T_1, T_2, \ldots, T_{2^n}, T_1 \cup \{x\}, T_2 \cup \{x\}, \ldots, T_{2^n} \cup \{x\}$$

are all distinct. Clearly, $T_i \neq T_j$ for $i \neq j$ since $T_1, T_2, \ldots, T_{2^n}$ were distinct subsets of T to begin with. It is also true that if $i \neq j$ then $T_i \cup \{x\} \neq T_j \cup \{x\}$. This is because either T_i has an element y that is not in T_j and since $y \neq x$, y is not in $T_j \cup \{x\}$ either, but obviously, $y \in T_i \cup \{x\}$, so $T_i \cup \{x\} \neq T_j \cup \{x\}$; or T_j has an element y that is not in T_i and then $T_i \cup \{x\} \neq T_j \cup \{x\}$ by an analogous argument. Finally, $T_i \neq T_j \cup \{x\}$ for any $1 \leq i, j \leq 2^n$, because $x \notin T_i$ but $x \in T_j \cup \{x\}$. So we have found $2(2^n) = 2^{n+1}$ different subsets of S. The only thing that remains to show is that if A is any subset of S then A is one of these 2^{n+1} subsets. Either $x \notin A$, in which case $A \subseteq T$ and hence $A = T_i$ for some $1 \leq i \leq 2^n$, or $x \in A$, in which case $A - \{x\} \subseteq T$ and hence $A - \{x\} = T_i$ for some i and so $A = T_i \cup \{x\}$. Therefore the 2^{n+1} subsets we listed above are all of the subsets of S. We can now conclude that $|\mathcal{P}(S)| = 2^{n+1}$. By induction, $|\mathcal{P}(S)| = 2^{|S|}$ must be true for a finite set S of any size.

6. Let $n \in \mathbb{Z}^+$.

   (a) (3 pts) Define congruence of integers, that is what

   $$a \equiv b \pmod{n}$$

   means for integers a and b.

   For $a, b \in \mathbb{Z}$, we say a is *congruent* to b modulo n, or

   $$a \equiv b \pmod{n}$$

   if $n|(a - b)$.

   (b) (7 pts) Let $a, b, c, d \in \mathbb{Z}$ such that

   $$a \equiv b \pmod{n}$$
   $$c \equiv d \pmod{n}.$$

   Prove that

   $$a - c \equiv b - d \pmod{n}.$$

   We want to prove

   $$a - c \equiv b - d \pmod{n},$$

that is $n|[(a-c)-(b-d)]$. Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, we know that $n|(a-b)$ and $n|(c-d)$. Therefore

$$(a-c)-(b-d) = a-c-b+d = (a-b)-(c-d)$$

is also divisible by n (by Theorem 5.3.2(3)).

7. (10 pts) **Extra credit problem.** We have seen in class that the Principle of Induction and the Well-Ordering Principle are logically equivalent. Therefore where one can be used in a proof, so can the other. Prove the identity

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

for Fibonacci numbers from problem 4 by using the Well-Ordering Principle instead of induction. (Hint: Prove by contradiction that the set of positive integers for which the identity does not hold must be empty.)

Let S be the set of all positive integers k for which

$$F_{n+1}F_{n-1} - F_n^2 \neq (-1)^n.$$

We will show that S is the empty set and hence

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

for all positive integers n. Suppose S is not empty. As we already noted in problem 4,

$$F_2F_0 - F_1^2 = 1(0) - 1^2 = -1 = (-1)^1,$$

so the identity holds for $n = 1$, and therefore $1 \notin S$.

Since S is a nonempty subset of $\mathbb{Z}^+$, S has a least element k by the Well-Ordering Principle. We know $1 \notin S$, so $k \geq 2$. Since k is the least element of S, $k-1 \notin S$. Therefore

$$F_{(k-1)+1}F_{(k-1)-1} - F_{k-1}^2 = (-1)^{k-1} \implies F_kF_{k-2} - F_{k-1}^2 = (-1)^{k-1}$$

holds. Since $k \geq 2$, we know that

$$F_k = F_{k-1} + F_{k-2} \quad \text{and} \quad F_{k+1} = F_k + F_{k-1}$$

Hence, much like in our solution to problem 4,

$$\begin{aligned}
F_{k+1}F_{k-1} - F_k^2 &= (F_k + F_{k-1})F_{k-1} - F_k^2 && \text{since } F_{k+1} = F_k + F_{k-1} \\
&= F_kF_{k-1} + F_{k-1}^2 - F_k^2 \\
&= F_{k-1}^2 + F_k(F_{k-1} - F_k) \\
&= F_{k-1}^2 - F_kF_{k-2} && \text{since } F_k = F_{k-1} + F_{k-2} \implies F_{k-1} - F_k = -F_{k-2} \\
&= -(F_kF_{k-2} - F_{k-1}^2) \\
&= -(-1)^{k-1} \\
&= (-1)^k.
\end{aligned}$$

But this contradicts the fact that $k \in S$ and so

$$F_{k+1}F_{k-1} - F_k^2 \neq (-1)^k.$$

Assuming that $S \neq \emptyset$ led to a contradiction, so S must be empty, which is what we wanted to prove.