Steven Rosendahl
Proofs Homework

1. (a) Let a, b and c be natural numbers with a odd. Prove that if $a|(b-c)$ and $a|(b+c)$, then $a|b$ and $a|c$.

   Proof: Let $a|(b-c)$ and $a|(b+c)$. Then $b-c = ax$ and $b+c = ay$ for some $x, y \in \mathbb{N}$. We have that $b = ax + c$. Then

$$\begin{gathered} ax + c + c = ay \\ ax + 2c = ay \\ 2c = ay - ax \\ 2c = a(y - x). \end{gathered}$$

   Since a is odd, $y - x$ must be even since $2c$ is even. Then $2|(y-x)$, and we have $c = a\frac{y-x}{2}$, or $c = az$ for $z \in \mathbb{N}$. Therefore $a|c$. If we let $c = b - ax$, we have

$$\begin{gathered} b + b - ax = ay \\ 2b - ax = ay \\ 2b = ay + ax \\ 2b = a(y + x) \end{gathered}$$

   Since $2b$ is even and a is odd, $y - x$ must be even, or $2|(y+x)$. Therefore $b = a\frac{y+x}{2}$, or $b = aj$ for $j \in \mathbb{N}$. Therefore $a|b$.

   $\triangle$

   (b) Using a truth table, show that $\neg(P \wedge Q)$ and $(\neg P \vee \neg Q)$ are logically equivalent.

P	Q	$\neg(P \wedge Q)$	$(\neg P \vee \neg Q)$
0	0	1	1
0	1	1	1
1	0	1	1
1	1	0	0

2. (a) Establish the following identity using induction.

$$\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$$

Proof:
Base Case: $n = 1$

$$\sum_{i=1}^{1} i^3 = \left(\frac{1(1+1)}{2}\right)^2$$
$$1^3 = \left(\frac{2}{2}\right)^2$$
$$1 = 1$$

Assume:

$$\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$$

Prove:

$$\sum_{i=1}^{n+1} i^3 = \left(\frac{(n+1)(n+2)}{2}\right)^2$$

$$\begin{aligned}
\therefore \sum_{i=1}^{n} i^3 + \sum_{i=n+1}^{n+1} i^3 &= \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 \quad \text{By the Induction Hypothesis} \\
&= \frac{n^2(n+1)^2}{4} + (n+1)^3 \\
&= \frac{n^2(n+1)^2}{4} + \frac{4(n+1)^3}{4} \\
&= \frac{n^2(n+1)^2 + 4(n+1)^3}{4} \\
&= \frac{(n+1)^2(n^2+4n+4)}{4} \\
&= \frac{(n+1)^2(n+2)^2}{2^2} \\
&= \left(\frac{(n+1)(n+2)}{2}\right)^2
\end{aligned}$$

$\triangle$

(b) Prove that if n^3 is odd, then n is odd.

Proof: Assume the contrapositive: if n is even, then n^3 is even. Then $n = 2k$ for $k \in \mathbb{Z}$, which mean that $n^3 = (2k)^3$. $(2k)^3 = 2(2^2k^3)$ where $(2^2k^3) \in \mathbb{Z}$. Therefore n^3 is even.

$\triangle$

3. (a) Using the definition, prove that $f : \mathbb{Q} \to \mathbb{Q}$ given by $f(x) = 3x + 2$ is bijective.

Proof: Let $x, y \in \mathbb{Q}$ such that $f(x) = f(y)$. Then

$$\begin{aligned} 3x + 2 &= 3y + 2 \\ 3x &= 3y \\ x &= y \end{aligned}$$

Therefore f is injective.
Let $y \in \mathbb{Q}$ such that $y = \frac{x-2}{3}$. Then

$$\begin{aligned} f(y) &= 3\left(\frac{x-2}{3}\right) + 2 \\ &= x - 2 + 2 \\ &= x \end{aligned}$$

Therefore f is surjective.
Therefore f is bijective.

$\triangle$

(b) Define a relation on $\mathbb{N} \times \mathbb{N}$ by $(a, b) \sim (c, d)$ if $a + d = b + c$. Prove that $\sim$ is an equivalence relation.

Symmetric: Let $(a, b) \sim (c, d)$. Then

$$\begin{aligned} a + d &= b + c \\ -b - c &= -a - d \\ (-1)(b + c) &= (-1)(a + d) \\ b + c &= a + d \end{aligned}$$

Therefore $(c, d) \sim (a, b)$, and $\sim$ is symmetric.

Reflexive: Let $(a, b) \in \mathbb{N} \times \mathbb{N}$. If $(a, b) \sim (a, b)$, then $a + b = a + b$. Therefore $(a, b) \sim (a, b)$, and $\sim$ is reflexive.

Transitive: Let $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $a + d = b + c$ and $c + f = d + e$. Solving for c yields $c = d + e - f$, and substituting gives us $a + d = b + d + e - f$. Then $a + f = e + b$, and $(a, b) \sim (e, f)$. Therefore, $\sim$ is transitive.

Therefore $\sim$ is an equivalence relation.

$\triangle$

4. (a) Let $\mathcal{X}$ be a finite set with cardinality n. Prove that the power set, $\mathcal{P}(\mathcal{X})$, has cardinality 2^n.

Proof:
Base Case: A set of size 1.
Let $\mathcal{X}$ be the set $\{x\}$. Then $\mathcal{P}(\mathcal{X})$ is $\{\emptyset, \{x\}\}$, which has a cardinality of $2^{||\mathcal{X}||}$, or 2^1.

Assume: $||\mathcal{P}(\{x_0, x_1, x_2, \ldots, x_n\})|| = 2^{||\mathcal{X}||}$.

Prove: $||\mathcal{P}(\{x_0, x_1, x_2, \ldots, x_n, x_{n+1}\})|| = 2^{||\mathcal{X}||+1}$.
We know that $\mathcal{P}$ is the set of all subsets of $\mathcal{X}$. If we count the number of subsets of $\{x_0, x_1, x_2, \ldots, x_n, x_{n+1}\}$, we know that the subset will either contain x_{n+1}, or it will not contain x_{n+1}. If the subset γ does not contain x_{n+1}, then $\gamma \subseteq \{x_0, x_1, x_2, \ldots, x_n\}$, and there are $2^{||\mathcal{X}||}$ γ by the induction hypothesis. If the subset λ contains x_{n+1}, then it is the result of some set $\gamma \cup \lambda$. Since $\gamma \subseteq \{x_0, x_1, x_2, \ldots, x_n\}$, we only need $\gamma \cup \{x_{n+1}\}$ to account for all possible sets. Therefore $||\mathcal{P}(\gamma \cup \{x_{n+1}\})||$ is $||\mathcal{P}(\gamma)|| \cdot ||\mathcal{P}(\{x_{n+1}\})||$, or $2^{||\mathcal{X}||} \cdot 2^{||\{x_{n+1}\}||}$. This is equivalent to $2^{||\mathcal{X}||} \cdot 2^1$, or $2^{||\mathcal{X}||+1}$.

$\triangle$

(b) Let $n \geq 2$ be an integer. Prove that $a \equiv b (\text{mod } n)$ is an equivalence relation on $\mathbb{Z}$.

Let R be the relation $a \equiv b \ mod \ n$.
Symmetric: Let aRb. Then $a \equiv b(\text{mod } n)$, or $a - b = nk$ for $k \in \mathbb{Z}$. It follows that

$$\begin{aligned} a &= nk + b \\ -nk &= b - a \\ nj &= b - a, \in \mathbb{Z} \end{aligned}$$

Therefore $b \equiv a \ mod \ n$, and R is symmetric.

Reflexive: Let aRa. Then $a \equiv a \ mod \ n$. It follows that $n|(a-a)$, or $n|0$. Since $n \geq 2$, $n|0$, and R is reflexive.

Transitive: Let aRb and bRc. Then $a \equiv b \ mod \ n$ and $b \equiv c \ mod \ n$. By definition, $a - b = nk, \ k \in \mathbb{Z}$ and $b - c = nj, \ j \in \mathbb{Z}$. Then $a - b = a - nj - c = nk$. It follows that $a - c = nk + nj$, or $a - c = n(k + j)$. Therefore $a \equiv b \ mod \ n$, and R is transitive

Therefore R is an equivalence relation.

$\triangle$

(c) Let A and B be sets. Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Proof:
$\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: Let $x \in \overline{A \cup B}$. Then $x \notin A$ or B. Since $x \notin A$, $x \in \overline{A}$. Since $x \notin B$, $x \in \overline{B}$. Therefore $x \in \overline{A}$ and $x \in \overline{B}$, or $x \in \overline{A} \cap \overline{B}$.

$\overline{A \cup B} \supseteq \overline{A} \cap \overline{B}$: Let $x \in \overline{A} \cap \overline{B}$. Then $x \notin A$ and $x \notin B$. Therefore $x \notin A \cup B$, or $x \in \overline{A \cup B}$.

$\triangle$

(d) Prove that $\sqrt{5}$ is irrational.

Proof: Let p be a prime number, and assume that $\sqrt{p}$ is rational. Then $\sqrt{p} = \frac{n}{m}$ for $n, m \in \mathbb{N}$. It follows that $n^2 p = m^2$. We know that there are two factors of p, namely 1 and p, and that a squared number will have an even number of prime factors, since it has double the prime factors as its root. Then $n^2 p$ will have an odd number of prime factors, since its prime factors are the prime factors of n^2 and the number p. Since $n^2 p = m^2$, m^2 must also have an odd number of prime factors. However, m^2 has an even number of prime factors. Therefore, by contradiction, the root of a prime number is irrational. Therefore, since 5 is prime, $\sqrt{5}$ is irrational. $\triangle$