Exercises for Module 1: Proofs

1. Prove De Morgan's Laws for propositions: $\neg(P \wedge Q) = \neg P \vee \neg Q$ and $\neg(P \vee Q) = \neg P \wedge \neg Q$ (Hint: use truth tables).

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$
T	T	F	F	T	F	F
T	F	F	T	F	T	T
F	T	T	F	F	T	T
F	F	T	T	F	T	T

P	Q	$\neg P$	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$
T	T	F	F	T	F	F
T	F	F	T	T	F	F
F	T	T	F	T	F	F
F	F	T	T	F	T	T

2. Write the following statements and their negations using logical quantifier notation and then prove or disprove them:
(i) Every odd integer is divisible by three.

$$\forall x \in \mathbb{Z},\ (\exists n \in \mathbb{Z} \text{ s.t. } x = 2n+1) \Rightarrow (\exists k \in \mathbb{Z} \text{ s.t } x = 3k)$$

negation:

$$\exists x \in \mathbb{Z} \text{ s.t. } (\exists n \in \mathbb{Z} \text{ s.t } x = 2n+1) \wedge (\forall k \in \mathbb{Z},\ x \neq 3k)$$

This statement is false.

Take $x = 11$.

(ii) For any real number, twice its square plus twice itself plus six is greater than or equal to five. *(You may assume knowledge of calculus.)*

$\forall x \in \mathbb{R}, \; 2x^2 + 2x + 6 \geq 5$

Negation: $\exists x \in \mathbb{R}$ s.t $2x^2 + 2x + 6 < 5$

This is true. $f(x) = 2x^2 + 2x + 6$ is an upward-facing parabola that attains its minimum at 5.5.

$\min_x 2x^2 + 2x + 6 \Rightarrow 0 = 4x + 2 \Rightarrow x = -1/2 \Rightarrow f(-1/2) = \frac{1}{2} - 1 + 6 = 5.5$

(iii) Every integer can be written as a unique difference of two natural numbers.

$\forall z \in \mathbb{Z} \; \exists! \, n_1, n_2$ s.t. $z = n_1 - n_2$

$\exists z \in \mathbb{Z}$ s.t. $(\exists n_1, n_2, n_3, n_4$ s.t $z = n_1 - n_2 = n_3 - n_4) \vee$
$(\forall n_1, n_2 \in \mathbb{N}, \; z \neq n_1 - n_2)$

This is false. ex. 1 can be written as the difference of natural numbers in infinite ways, ex. $1 = 3 - 2 = 4 - 3$

3. Prove the following statements:
(i) If $a|b$ and $a, b \in \mathbb{N}$ (positive integers), then $a \leq b$.

Suppose $a|b$ & $a, b \in \mathbb{N}$.
Then $\exists j \in \mathbb{N}$ s.t. $b = aj$. ($j > 0$ since $a, b > 0$)
Since $j \geq 1$, $b \geq a$. ∎

(could also use contradiction)

(ii) If $a|b$ and $a|c$, then $a|(xb+yc)$, where $x, y \overset{a,b,c}{\wedge} \in \mathbb{Z}$.

Let $a,b,c,x,y \in \mathbb{Z}$.

Let $a|b$ and $a|c$. By definition, this means that

$\exists j,k \in \mathbb{Z}$ s.t. $b = aj$ & $c = ak$.

$$\text{Then } xb + yc = xaj + yak = a(\underbrace{xj + yk}_{\in \mathbb{Z}})$$

Thus $a|(xb+yc)$ by definition. ∎

(iii) Let $a, b, n \in \mathbb{Z}$. If n does not divide the product ab, then n does not divide a and n does not divide b.

We prove the contrapositive, i.e.

$$n|a \vee n|b \Rightarrow n|ab.$$

Let $a,b,n \in \mathbb{Z}$.

Suppose $n|a$. Then $\exists j \in \mathbb{Z}$ s.t $a = nj$

$$\Rightarrow ab = njb = n(\underbrace{jb}_{\in \mathbb{Z}})$$

$\therefore n|ab$.

Suppose $n|b$. The proof that $n|ab$ is the same with the roles of a & b interchanged. ∎

4. Prove that for all integers $n \geq 1$, $3|(2^{2n} - 1)$.

We proceed by induction on n.

Base case: $n = 1$. Then $2^{2n} - 1 = 4 - 1 = 3$, which is divisible by 3.

Inductive hypothesis: Suppose $3 | 2^{2k} - 1$ for some $k \in \mathbb{N}$.

We show $3 | 2^{2(k+1)} - 1$.

$3 | 2^{2k} - 1$ means $\exists j \in \mathbb{Z}$ s.t $2^{2k} - 1 = 3j$.

$$\begin{aligned} \text{We see that } 2^{2(k+1)} - 1 &= 2^2 2^{2k} - 1 \\ &= 4(2^k) - 4 + 3 \\ &= 4(2^k - 1) + 3 \\ &= 4(3j) + 3 \\ &= 3(4j + 1) \end{aligned}$$

Thus $3 | 2^{2(k+1)} - 1$. The claim holds by induction.

5. Prove the Fundamental Theorem of Arithmetic, that every integer $n \geq 2$ has a unique prime factorization (i.e. prove that the prime factorization from the last proof is unique).

We have already shown (in lecture) that each integer $n \geq 2$ has a prime factorization. It remains to show that this factorization is unique.

Suppose in order to derive a contradiction that the prime factorization is not unique. Then there exists a least integer $n \geq 2$ such that

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell \quad \text{where } p_i, q_j, \; 1 \leq i \leq k, \; 1 \leq j \leq \ell \text{ are prime numbers}$$

This equality gives us that the p_i divide $q_1 q_2 \cdots q_\ell$. Without loss of generality, we focus on p_1.

$p_1 | q_1 q_2 \cdots q_\ell$ implies that p_1 divides one of $q_1, q_2, \ldots, q_\ell$, since they are prime.

Without loss of generality, $p_1 | q_1$. Since both are prime, this means $p_1 = q_1$.

Thus $\cancel{p_1} p_2 \cdots p_k = \cancel{q_1} q_2 \cdots q_\ell \Rightarrow p_2 \cdots p_k = q_2 \cdots q_\ell$

This contradicts our assumption that n was the <u>least</u> integer that could be written as the product of two sets of primes.

Therefore there does not exist such a $n \Rightarrow$ prime factorizations are unique.