1. Direct Proof

Theorems are statements that are true.

Proof is a written verification that a theorem is true.

Definitions will help avoid ambiguity. Other terms for theorems are propositions, lemma, corollary (an immediate consequence of a theorem).

Some often used definitions:

**Def 1.** An integer $n$ is even if $n = 2a$ for some $a \in \mathbb{Z}$.

**Def 2.** An integer $n$ is odd if $n = 2a + 1$ for some $a \in \mathbb{Z}$.

**Def 3.** Two integers have the same parity if they're both even or both odd otherwise they have opposite parity.

**Def 4.** Suppose $a, b \in \mathbb{Z}$. We say $a \mid b$ (a divides b) if $b = dc$ for some $c \in \mathbb{Z}$. In this case we say that $a$ is a divisor of $b$ and $b$ is a multiple of $a$.

**Def 5.** An integer $n$ is called prime if its only divisors are 1 and $n$ (itself).

**Def 6.** An integer $n$ is composite if it factors as $n = ab$, where both $a > 1$ and $b > 1$.  

Def \( \gcd(a, b) \): greatest common divisor of \( a \) and \( b \)

\( \text{lcm}(a, b) \): least common multiple of \( a \) and \( b \)

Fact (accept w/o pf) That every \( n \in \mathbb{N}, n > 1 \) has a unique factorization into primes

Theorems of the form \( P \Rightarrow Q \)

e.g. Thm. If \( \lim_{k \to \infty} a_k \) converges then \( \lim_{k \to \infty} a_k = 0 \)

vs.

Thm. The series \( \sum_{n=1}^{\infty} \frac{1}{n} \) diverges

Outline: Thm. \( P \Rightarrow Q \)
proof Assume \( P \) is true

<table>
<thead>
<tr>
<th>( P )</th>
<th>( Q )</th>
<th>( P \Rightarrow Q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

Then \( Q \) is true

Examples

Proposition If \( x \) is odd then \( x^2 \) is odd

Proof Assume \( x \) is odd, that is, \( x = 2a + 1 \)

for some \( a \in \mathbb{Z} \)

Then \( x^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1 \)

since \( k = 2a^2 + 2a \in \mathbb{Z} \) then \( x^2 = 2k + 1 \) is an odd number
Proposition Let \( a, b, \) and \( c \) be integers
If \( ab \) and \( bc \) then \( ac \)

We want \( c = \alpha k \) for some \( k \in \mathbb{Z} \)

Proof Assume \( ab \) and \( bc \) that is we can write
\( b = \alpha d \) and \( c = \beta e \) for some integers \( d \) and \( e \).
Then \( c = (\alpha d) e = \alpha (de) \), which means \( a|c \)
(since \( de \in \mathbb{Z} \))

Proposition If \( x \) is an even integer then \( x^2 - 6x + 5 \) is odd

Proof Assume \( x \) is even, by definition we have
\( x = 2a \) for some \( a \in \mathbb{Z} \)
Then \( x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5 \)
\[ = 4a^2 - 12a + 4 + 1 \]
\[ = 2(2a^2 - 6a + 2) + 1 \]
Since \( k = 2a^2 - 6a + 2 \in \mathbb{Z} \), \( x^2 - 6x + 5 \) is odd

Claim If \( n \) is not divisible by \( 2 \), then it is odd

PF Assume \( n \neq 2a \) for all \( a \in \mathbb{Z} \), but we know
div algorithm holds \( \left( \frac{n}{2} \right) \), so that \( n = dq + r \) and
\( 0 \leq r < 2 \)
Thus \( n = 2q + r \) and note \( r = 1 \), that is \( n = 2q + 1 \)
for some \( q \in \mathbb{Z} \)
Proposition: If a prime number $P$ is greater than 2, then it is odd.

Proof: Assume $P > 2$ is a prime number. Since $P$ is prime, its only divisors are 1 and $P$. Since $2 \neq 1$ and $2 \neq P$, then 2 is not a divisor of $P$, which implies (see claim above) that $P$ is odd.

Claim: To show $m \leq n$ we show $m \leq n$ and $n \leq m$. 

Proposition: If $a, b, c \in \mathbb{N}$, then $\text{lcm}(ca, cb) = c \cdot \text{lcm}(a, b)$. 

Proof: Assume $a, b, c \in \mathbb{N}$.

Let $m = \text{lcm}(a, b)$, $n = c \cdot \text{lcm}(a, b)$.

$\text{lcm}(a, b) = ax = by$ for some $x, y \in \mathbb{Z}$.

Note $n = c \cdot \text{lcm}(a, b) = (ca)x = (cb)y$, so that $n$ is a multiple of $ca$ and of $cb$, so

$m \leq n$.