Worksheet Claims (and Proof sketches)

Claim 1 \( \forall x \in \mathbb{N} \; x/x \)

Let \( x \in \mathbb{N} \)

Let \( k = 1 \).

Then \( x = x \cdot k \)

\( \Rightarrow \exists k \in \mathbb{Z} \quad x = x \cdot k \)

Claim 2 \( \forall x, y \in \mathbb{N} \; y \geq 1 \land x/y \Rightarrow 1 \leq x \land x \leq y \)

Let \( x, y \in \mathbb{N} \) and assume \( y \geq 1, x/y \)

Let \( k \in \mathbb{Z} \) be such that \( y = k \cdot x \) (since \( x/y \))

1. \( y = k \cdot x, y \geq 1 \Rightarrow k \cdot x \geq 1 \)
   
   Therefore \( k, x \geq 0 \)
   
   \( \therefore x \geq 1 \)

2. \( y = k \cdot x \) and \( x, y \in \mathbb{N} \Rightarrow k \cdot x = 1 \)

Since \( y = 1, x \leq y \)
Claim 3: \( \forall n, p \in \mathbb{N} \) \( \text{Prime}(p) \land p \nmid n \Rightarrow \gcd(p, n) = 1 \)

Let \( n, p \in \mathbb{N} \)

We will prove the statement by contradiction.

Assume \( \text{Prime}(p) \), and \( p \nmid n \), and \( \gcd(p, n) \neq 1 \)

Let \( k \in \mathbb{N} \), \( k \geq 2 \) such that \( k \mid p \) and \( k \nmid n \)

(\ since \( \gcd(p, n) \neq 1 \) \)

Since \( p \) is prime, \( k \mid p \) implies that \( k = p \)

But this implies \( p \mid n \) which contradicts our assumption that \( p \nmid n \).
Claim 4 \( \forall n, m \in \mathbb{Z}^+ , \gcd(n, m) = 1 \)

Let \( n \), \( m \in \mathbb{Z}^+ \\
\text{let } K = \gcd(n, m) \\
\text{then } K|n \text{ and } K|m \\
\text{therefore } \exists n_1 \text{ such that } K \cdot n_1 = n \\\n\text{since } n \in \mathbb{Z}^+ \text{ and } K \in \mathbb{N}, \\
K = 1 \left( \begin{array}{l}
\text{K can't be negative since } n_i + n \text{ are both non-negative} \\
\text{and K can't be 0 since } n \text{ is in } \mathbb{Z}^+ \\
\end{array} \right) \)
Claim 5 \( \forall n,m \in \mathbb{N} \ \forall r,s \in \mathbb{Z} \) \( \gcd(n,m) \mid (rn+sm) \)

Let \( n,m \in \mathbb{N} \), let \( r,s \in \mathbb{Z} \)

Let \( K = \gcd(n,m) \). Then \( K \mid n \) and \( K \mid m \)

We want to show \( \exists K' \in \mathbb{Z} \) such that \( K \cdot K' = rn + sm \)

Since \( K \mid n \), by definition of divide \( \exists n_1 \in \mathbb{Z} \) such that \( K \cdot n_1 = n \)

Similarly, since \( K \mid m \) \( \exists m_1 \in \mathbb{Z} \) such that \( K \cdot m_1 = m \)

Then \( K \cdot n_1 = n \Rightarrow r \cdot K \cdot n_1 = r \cdot n \)

and \( K \cdot m_1 = m \Rightarrow s \cdot K \cdot m_1 = s \cdot m \)

So \( r \cdot n_1 + s \cdot k \cdot m_1 = rn + sm \)

\[ \therefore K( r \cdot n_1 + s \cdot m_1 ) = rn + sm \]

Let \( K' = r \cdot n_1 + s \cdot m_1 \). Then \( K \cdot K' = rn + sm \)
Claim 6: $\forall n,m \in \mathbb{N} \ \exists a,b \in \mathbb{Z} \ \text{such that } an + bm = \gcd(n,m)$

*Note this claim is advanced and you won't be expected to prove it on an exam!

Let $d$ be the smallest positive integer such that there exists $s,t \in \mathbb{Z}$ such that $ns + mt = d$.

We will prove that $d|n$ and $d|m$. Since all elements of the form $nx + my$, $x,y \in \mathbb{Z}$ are divisible by $\gcd(n,m)$, it follows that $d$ is the greatest common divisor.

Write $n = dq + r$, where $0 \leq r < d$ (so $r$ is the remainder).

Then $r = n - dq = n - q(ns + mt)$

\[ = n(1 - qs) - mq \]

But $r$ is of the form $nx + my$, so $r = 0$.

$\therefore d|n$. A similar argument shows that $d|m$. 