1 On Proofs

1.1 Basic Exercises

1. Suppose n is a natural number larger than 2, and n is not a prime number. Then $n \cdot 2 + 13$ is not a prime number.

   Disproof by counterexample:
   Let $n = 8$.
   Then $n \cdot 2 + 13 = 29$.
   But 21 is prime. So the statement is disproved.

2. If $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

   This statement is logically equivalent to the contrapositive: if $x = 3$ then $y = 4$ or $x^2 + y \neq 13$. This is proved below.

$$\begin{aligned} x &= 3 \\ x^2 + y &= 13 \\ 3^2 + y &= 13 \\ 9 + y &= 13 \\ y &= 4 \end{aligned} \tag{1}$$

   So either the $y = 4$ or $x^2 + y \neq 13$ as required.

3. For an integer n, n^2 is even if and only if n is even.

   If:
   Assume n is even. So n can be written in the form $2 \cdot k$ for some k.

$$\begin{aligned} n &= 2 \cdot k \\ n^2 &= 4 \cdot k^2 \\ &= 2(2 \cdot k^2) \end{aligned} \tag{2}$$

   This is an even number of the form $2 \cdot i$ where $i = 2 \cdot k^2$.
   So if n is even; then n^2 is even.

   Only if:
   If n^2 is even then n is even. This is logically equivalent to the contrapositive: if n is odd then n^2 is odd.
   Assume n is odd. So n can be written in the form $2 \cdot k + 1$ for some k.

$$\begin{aligned} n &= 2 \cdot k + 1 \\ n^2 &= (2 \cdot k + 1) \cdot (2 \cdot k + 1) \\ &= 4 \cdot k^2 + 4 \cdot k + 1 \\ &= 2(2 \cdot k^2 + 2 \cdot k) + 1 \end{aligned} \tag{3}$$

   This is an odd number of the form $2 \cdot j + 1$ where $j = 2 \cdot k^2 + 2 \cdot k$.
   So if n is odd; then n^2 is odd. As required.

4. For all real numbers x and y there is a real number z such that $x + z = y - z$.

$$\begin{aligned} x + z &= y - z \\ 2 \cdot z &= y - x \\ \therefore z &= \frac{y - x}{2} \end{aligned} \tag{4}$$

   Since the set of reals is closed under both addition and division and $x, y \in \mathbb{R}$: $\frac{y-x}{2} \in \mathbb{R}$.
   Hence $z \in \mathbb{R}$ and the statement is proved.

5. For all real numbers x and y there is an integer z such that $x + z = y - z$.

   Disproof by counterexample:
   Let $y = x + 1$.

$$\begin{aligned} x + z &= y - z \\ x + z &= x + 1 - z \\ 2 \cdot z &= 1 \\ z &= \frac{1}{2} \end{aligned} \tag{5}$$

   In this case: z is not an integer and so the statement is disproved.

6. The addition of two rational numbers is a rational number. Let $a = \frac{x}{y}$. Let $b = \frac{p}{q}$.

$$\begin{aligned} a + b &= \frac{x}{y} + \frac{p}{q} \\ a + b &= \frac{q \cdot x}{q \cdot y} + \frac{p \cdot y}{q \cdot y} \\ a + b &= \frac{p \cdot y + q \cdot x}{q \cdot y} \end{aligned} \tag{6}$$

   This is a rational number of the form $\frac{a}{b}$ where $a = p \cdot y + q \cdot x$ and $b = q \cdot y$. So the sum of two rational numbers is a rational number – as required.

7. For every real number x, if $x \neq 2$ then there is a unique real number y such that $\frac{2 \cdot y}{y+1} = x$.

$$\begin{aligned} x &= \frac{2 \cdot y}{y + 1} \\ x \cdot y + x &= 2 \cdot y \\ x &= y \cdot (2 - x) \\ \frac{x}{2 - x} &= y \end{aligned} \tag{7}$$

   Since $(\frac{x}{2-x})$ is defined for all $x \neq 2$: there exists a y for all $x \neq 2$.

   Now we only need to prove that y is unique for all x.

   I will prove this by contradiction. Let $f(x) = \frac{x}{2-x}$. Assume that there exists an x_0 and an x_1 such that $f(x_0) = f(x_1)$.

$$\begin{aligned} f(x_0) &= f(x_1) \\ \frac{x_0}{2 - x_0} &= \frac{x_1}{2 - x_1} \\ 2 \cdot x_0 - x_0 \cdot x_1 &= 2 \cdot x_1 - x_0 \cdot x_1 \\ 2 \cdot x_0 &= 2 \cdot x_1 \\ x_0 &= x_1 \\ \therefore (f(x_0) = f(x_1)) &\implies (x_0 = x_1) \text{ so f is an injective function} \end{aligned} \tag{8}$$

   Since $(\frac{x}{2-x})$ is an injective function: y is unique.

   Hence the statement is proved.

8. For all integers m and n, if $m \cdot n$ is even, then either m is even or n is even.

   This statement is logically equivalent to the contrapositive:
   If both m and n are odd then $m \cdot n$ is odd.

Let $m = 2 \cdot i + 1$ and $n = 2 \cdot j + 1$.

$$\begin{aligned} m \cdot n &= (2 \cdot i + 1) \cdot (2 \cdot j + 1) \\ m \cdot n &= 4 \cdot i \cdot j + 2 \cdot i + 2 \cdot j + 1 \\ m \cdot n &= 2 \cdot (2 \cdot i \cdot j + i + j) + 1 \end{aligned} \tag{9}$$

This is an odd number of the form $2 \cdot k + 1$ where $k = 2 \cdot i \cdot j + i + j$. So the contrapositive is proved and hence the statement is proved – as required.

1.2 Core Exercises

1. Characterise those integers d and n such that:

   (a) $0|n$

   $n = 0$

   (b) $d|0$

   $d \in \mathbb{N}$

2. Let k, m, n be integers with k positive. Show that:

$$(k \cdot m)|(k \cdot n) \iff m|n \tag{10}$$

$$(\Longrightarrow)$$

$$\begin{aligned} (k \cdot m)&|(k \cdot n) \\ k \cdot m \cdot i &= k \cdot n \\ m \cdot i &= n \\ \therefore m&|n \text{ as required} \end{aligned} \tag{11}$$

$$(\Longleftarrow)$$

$$\begin{aligned} m&|n \\ m \cdot i &= n \\ k \cdot m \cdot i &= k \cdot n \\ (k \cdot m) \cdot i &= (k \cdot n) \\ \therefore (k \cdot m)&|(k \cdot n) \text{ as required} \end{aligned} \tag{12}$$

And so the statement is proved.

3. Prove or disprove that: For all natural numbers n, $2|2^n$.

   n is a natural number. So $n \geqslant 1$. So $n - 1 \geqslant 0$.
   Hence $2^{n-1} \in \mathbb{Z}^+$.

$$\begin{aligned} 2 \cdot (2^{n-1}) &= 2^n \\ 2^{(n-1)} &\in \mathbb{Z}^+ \\ &\therefore 2|2^n \text{ as required} \end{aligned} \tag{13}$$

   Hence $2|2^n$.

4. Show that for all integers l, m, n,

$$l|m \land m|n \implies l|n \tag{14}$$

$$\begin{aligned} a \cdot l &= m \\ b \cdot m &= n \\ a \cdot (b \cdot l) &= n \\ (a \cdot b) \cdot l &= n \\ \therefore l&|n \end{aligned} \tag{15}$$

5. Find a counterexample to the statement: For all positive integers k, m, n,

$$(m|k \land n|k) \implies (m \cdot n)|k \tag{16}$$

Let $m = 4$, $n = 6$ and $k = 12$.
$4|12 \land 6|12$
So $m|k \land n|k$
But $24 \nmid 12$.
Hence this is a counterexample to the statement so the statement is disproved.

6. Prove that for all integers d, k, l, m, n,

(a) $d|m \land d|n \implies d|(m+n)$

$$\begin{aligned} &d|m \\ i \cdot d &= m \\ &d|n \\ j \cdot d &= n \\ i \cdot d + j \cdot d &= m + n \\ (i+j) \cdot d &= (m+n) \\ \therefore d&|(m+n) \end{aligned} \tag{17}$$

So the statement is proved as required.

(b) $d|m \implies d|k \cdot m$

$$\begin{aligned} &d|m \\ i \cdot d &= m \\ k \cdot i \cdot d &= k \cdot m \\ (k \cdot i) \cdot d &= k \cdot m \\ \therefore d&|(k \cdot m) \text{ as required} \end{aligned} \tag{18}$$

(c) $d|m \land d|n \implies d|(k \cdot m + l \cdot n)$
From part (b): $d|m \implies d|(k \cdot m)$.
So $d|m \land d|n \implies d|(k \cdot m) \land (l \cdot n)$.

From part (a): $d|m \land d|n \implies d|(m+n)$.
So $d|(k \cdot m) \land d|(l \cdot n) \implies d|(k \cdot m + l \cdot n)$ as required.

7. Prove that for all integers n,

$$30|n \iff (2|n \land 3|n \land 5|n) \tag{19}$$

If:

$$\begin{aligned} 30&|n \\ 30\cdot k &= n \\ 2\cdot(15\cdot k) &= n \\ \therefore 2|n &\text{ as required} \\ 3\cdot(10\cdot k) &= n \\ \therefore 3|n &\text{ as required} \\ 5\cdot(6\cdot k) &= n \\ \therefore 5|n &\text{ as required} \end{aligned} \tag{20}$$

Only if:

If $a|c$ and $b|c$ and b and c are coprime: then $a\cdot b|c$.

Since 2, 3 and 5 are all coprime:

$$\begin{aligned} 2|n \land 3|n \land 5|n &\implies (2\cdot 3\cdot 5)|n \\ &\implies 30|n \text{ as required} \end{aligned} \tag{21}$$

8. Show that for all integers m and n,

$$(m|n \land n|m) \implies (m = n \cup m = -n) \tag{22}$$

$$\begin{aligned} m&|n \\ k\cdot m &= n \end{aligned} \tag{23}$$

$$\begin{aligned} n&|m \\ c\cdot n &= m \end{aligned} \tag{24}$$

Combining (23) and (23) gives:

$$\begin{aligned} k\cdot c\cdot n &= n \\ k\cdot c &= 1 \\ c &= \frac{1}{k} \end{aligned} \tag{25}$$

However, since both c and k are integers, this means that either $(c = 1 \land k = 1) \cup (c = -1 \land k = -1)$.
So $(n = m) \cup (n = -m)$ as required.

9. Prove or disprove that: For all positive integers k, m, n,

$$k|(m\cdot n) \implies k|m \cup k|n \tag{26}$$

Disproof by counterexample:

Let $k = 6$, $m = 3$ and $n = 4$.
$6|12$ so $k|(m\cdot n)$.
However, $6 \nmid 3$ and $6 \nmid 4$.
So the statement is disproved by a counterexample.

10. Let $P(m)$ be a statement for m ranging over the natural numbers, and consider the following derived statemets (with n also ranging over the natural numbers):

$$P^{\#}(n) \triangleq \forall k \in \mathbb{N}.0 \leqslant k \leqslant n \implies P(k) \tag{27}$$

(a) Show that, for all natural numbers ℓ, $P^{\#}(\ell) \implies P(\ell)$

$$\begin{aligned} P^{\#}(n) &\triangleq \forall k \in \mathbb{N}.0 \leqslant k \leqslant n \implies P(k) \\ P^{\#}(n) &= (\forall k \in \mathbb{N}.0 \leqslant k \leqslant (n-1) \implies P(k)) \wedge P(n) \\ P^{\#}(n) &= P^{\#}(n-1) \wedge P(n) \\ \therefore P^{\#}(n) &\implies P(n) \text{ as required} \end{aligned} \tag{28}$$

(b) Exhibit a concrete statement $P(m)$ and a specific natural number n for which the following statement does *not* hold:

$$P(n) \implies P^{\#}(n) \tag{29}$$

Let $P(n) \triangleq (\exists k \in \mathbb{N}.n = 2 \cdot k)$.

If $n = 2$ the the statement above does not hold (since $P(n)$ is true but $P^{\#}(n)$ is not true.

(c) Prove the following:

- $P^{\#}(0) \iff P(0)$

$$\begin{aligned} P^{\#}(n) &\triangleq \forall k \in \mathbb{N}.0 \leqslant k \leqslant n \implies P(k) \\ \therefore P^{\#}(0) &\triangleq \forall k \in \mathbb{N}.0 \leqslant k \leqslant 0 \implies P(k) \\ P^{\#}(0) &\triangleq P(0) \end{aligned} \tag{30}$$

So $P^{\#}(0)$ is equivalent to $P(0)$.
Hence $P^{\#}(0) \iff P(0)$ as required.

- $\forall n \in \mathbb{N}.(P^{\#}(n) \implies P\#(n+1)) \iff (P^{\#}(n) \implies P(n+1))$

$(\implies)$

$$\begin{aligned} & P^{\#}(n) \implies P^{\#}(n+1) \\ = {} & P^{\#}(n) \implies P^{\#}(n+1) \implies P(n+1) \text{ using (28)} \\ = {} & P^{\#}(n) \implies P(n+1) \text{ as required} \end{aligned} \tag{31}$$

$(\impliedby)$

$$\begin{aligned} P^{\#}(n+1) &\triangleq \forall k \in \mathbb{N}.0 \leqslant k \leqslant n+1 \implies P(k) \\ P^{\#}(n+1) &= \forall k \in \mathbb{N}.0 \leqslant k < n \implies P(k) \wedge P(n+1) \\ \therefore P^{\#}(n+1) &= P^{\#}(n) \wedge P(n+1) \end{aligned} \tag{32}$$

$$\begin{aligned} & P^{\#}(n) \implies P(n+1) \\ = {} & P^{\#}(n) \implies (P^{\#}(n) \wedge P(n+1)) \\ = {} & P^{\#}(n) \implies P^{\#}(n+1) \text{ as required using (32)} \end{aligned} \tag{33}$$

- $(\forall m \in \mathbb{N}.P^{\#}(m)) \iff (\forall m \in \mathbb{N}.P(m))$

$(\implies)$

$$\begin{aligned} P^{\#}(n) &\implies P(n) \text{ using 28} \\ \therefore (\forall m \in \mathbb{N}.P^{\#}(m)) &\implies (\forall m \in \mathbb{N}.P(m)) \text{ as required} \end{aligned} \tag{34}$$

$(\impliedby)$

$$\begin{aligned} &\forall m \in \mathbb{N}.P(m) \\ \therefore\ &\forall m, k \in \mathbb{N}.\ 0 \leqslant k \leqslant m \implies P(m) \\ \therefore\ &\forall m \in \mathbb{N}P^{\#}(m) \\ \text{Since } m \text{ is arbitrary: } &\forall m \in \mathbb{N}.P^{\#}(m) \text{ as required} \end{aligned} \tag{35}$$

$$\tag{36}$$

1.3 Optional Exercises

1. A series of questions about the properties and relationships of triangular and square numbers (adapted from David Burton).

   - A natural number is said to be *triangular* if it is of the form $\Sigma_{i=0}^{k} i = 0+1+...+k$, for some natural k. For example, the first three triangular numbers are $t_0 = 0$, $t_1 = 1$ and $t_2 = 3$.

     Find the next three triangular numbers t_3, t_4 and t_5.

     $t_3 = 6$, $t_4 = 10$, $t_5 = 15$

   - Find a formula for the k^{th} triangular number t_k.

     $t_k = \frac{k}{2} \cdot (k+1)$

   - A natural number is said to be *square* if it is of the form k^2 for some natural number k.

     Show that n is triangular iff $8 \cdot n + 1$ is a square. (Plutarch, circ. 100BC)

     If:

     Let n be a number such that $8 \cdot n + 1$ is a square number.
     Let $k^2 = 8 \cdot n + 1$
     Since $8 \cdot n + 1$ is a number of the form $2 \cdot i + 1$ where $i = (4 \cdot n)$; $8 \cdot n + 1$ is odd.
     As $8 \cdot n + 1$ is odd: k must be odd.
     So $k = 2 \cdot j + 1$ for some j.

$$\begin{aligned} 8 \cdot n + 1 &= (2 \cdot j + 1)^2 \\ 8 \cdot n + 1 &= 4 \cdot j^2 + 4 \cdot j + 1 \\ 8 \cdot n &= 4 \cdot j^2 + 4 \cdot j \\ n &= \frac{1}{2}(j^2 + j) \\ n &= \frac{j}{2}(j+1) \text{ as required} \end{aligned} \tag{37}$$

     Only if:

Let n be a triangle number. So $n = \frac{k}{2} \cdot (k+1)$ for some k.

$$\begin{aligned}
8 \cdot n + 1 &= 8 \cdot \frac{k}{2} \cdot (k+1) + 1 \\
&= 4 \cdot k \cdot (k+1) + 1 \\
&= 4 \cdot k^2 + 4 \cdot k + 1 \\
&= (2 \cdot k + 1)^2
\end{aligned} \tag{38}$$

So if n is a trangle number then $8 \cdot n + 1$ is a square number.

Hence n is triangular iff $8 \cdot n + 1$ is a square number.

- Show that the sum of every two consecutive triangular numbers is a square. (Nicomachus, circ. 100BC)

$$\begin{aligned}
t_k + t_{k+1} &= \frac{k}{2} \cdot (k+1) + \frac{k+1}{2} \cdot (k+2) \\
&= \frac{k+1}{2} \cdot k + \frac{k+1}{2} \cdot (k+2) \\
&= \frac{k+1}{2} \cdot (2 \cdot k + 2) \\
&= (k+1) \cdot (k+1) \\
&= (k+1)^2
\end{aligned} \tag{39}$$

So the sum of two consecutive triangular numbers is square. As required.

- Show that, for all natural numbers n, if n is triangular, then so are $9 \cdot n + 1$, $25 \cdot n + 3$, $49 \cdot n + 6$ and $81 \cdot n + 10$. (Euler, 1775)

  n is triangular. So $n = \frac{k}{2} \cdot (k+1)$ for some k.

$$\begin{aligned}
9 \cdot n + 1 &= 9 \cdot \frac{k}{2} \cdot (k+1) + 1 \\
&= \frac{9 \cdot k^2}{2} + \frac{9 \cdot k}{2} + 1 \\
&= \frac{1}{2} \cdot (9 \cdot k^2 + 9 \cdot k + 2) \\
&= \frac{1}{2} \cdot (3 \cdot k + 1) \cdot (3 \cdot k + 2) \\
&= \frac{3 \cdot k + 1}{2} \cdot ((3 \cdot k + 1) + 1)
\end{aligned} \tag{40}$$

So if n is a triangular number then so is $9 \cdot n + 1$.

$$\begin{aligned}
25 \cdot n + 3 &= 25 \cdot \frac{k}{2} \cdot (k+1) + 3 \\
&= \frac{25 \cdot k^2}{2} + \frac{25 \cdot k}{2} + 3 \\
&= \frac{1}{2} \cdot (25 \cdot k^2 + 25 \cdot k + 6) \\
&= \frac{1}{2} \cdot (5 \cdot k + 2) \cdot (5 \cdot k + 3) \\
&= \frac{5 \cdot k + 2}{2} \cdot ((5 \cdot k + 2) + 1)
\end{aligned} \tag{41}$$

So if n is a triangular number then so is $25 \cdot n + 3$.

$$
\begin{aligned}
49 \cdot n + 6 &= 49 \cdot \frac{k}{2} \cdot (k+1) + 6 \\
&= \frac{49 \cdot k^2}{2} + \frac{49 \cdot k}{2} + 6 \\
&= \frac{1}{2} \cdot (49 \cdot k^2 + 49 \cdot k + 12) \\
&= \frac{1}{2} \cdot (7 \cdot k + 3) \cdot (7 \cdot k + 4) \\
&= \frac{7 \cdot k + 3}{2} \cdot ((7 \cdot k + 3) + 1)
\end{aligned} \tag{42}
$$

So if n is a triangular number then so is $49 \cdot n + 6$.

$$
\begin{aligned}
81 \cdot n + 10 &= 81 \cdot \frac{k}{2} \cdot (k+1) + 10 \\
&= \frac{81 \cdot k^2}{2} + \frac{81 \cdot k}{2} + 10 \\
&= \frac{1}{2} \cdot (81 \cdot k^2 + 81 \cdot k + 20) \\
&= \frac{1}{2} \cdot (9 \cdot k + 4) \cdot (9 \cdot k + 5) \\
&= \frac{9 \cdot k + 4}{2} \cdot ((9 \cdot k + 4) + 1)
\end{aligned} \tag{43}
$$

So if n is a triangular number then so is $81 \cdot n + 10$.

Hence the statement is proved.

- Prove the generalisation: For all n and k natural numbers, there exists a natural number q such that $(2 \cdot n + 1)^2 \cdot t_k + t_n = t_q$. (Jordan 1991, attributed to Euler)

$$
\begin{aligned}
&(2 \cdot n + 1)^2 \cdot t_k + t_n \\
=&(2 \cdot n + 1)^2 \cdot \frac{k}{2} \cdot (k+1) + \frac{n}{2} \cdot (n+1) \\
=&(4 \cdot n^2 + 4 \cdot n + 1) \cdot \frac{k}{2} \cdot (k+1) + \frac{n}{2} \cdot (n+1) \\
=&\frac{1}{2}((4 \cdot n^2 \cdot k + 4 \cdot n \cdot k + k) \cdot (k+1) + n^2 + n)) \\
=&\frac{1}{2}(4 \cdot n^2 \cdot k^2 + 4 \cdot n \cdot k^2 + k^2 + 4 \cdot n^2 \cdot k + 4 \cdot n \cdot k + k + n^2 + n) \\
=&\frac{1}{2}(2 \cdot n \cdot k + n + k) \cdot ((2 \cdot n \cdot k + n + k) + 1) \\
=&\frac{(2 \cdot n \cdot k + n + k)}{2} \cdot ((2 \cdot n \cdot k + n + k) + 1) \\
=&\frac{q}{2} \cdot (q+1) \text{ where } q = 2 \cdot n \cdot k + n + k
\end{aligned} \tag{44}
$$

So for each n and k, there exists an integer q such that $(2 \cdot n + 1)^2 \cdot t_k + t_n = t_q$ as required.

2. Let $P(x)$ be a predicate on a variable x and let Q be a statement not mentioning x. Show that the following equivalence holds:

$$((\exists x.P(x)) \implies Q) \iff (\forall x.(P(x) \implies Q)) \tag{45}$$

($\implies$)

Q is independent of x. Since $P(x)$ is dependent only on x and Q is independent of x; Q is independent of $P(x)$.

So if there exists a single case such that $(P(x) \implies Q)$, then Q is always true (since Q is independent of P(x)).
So $(\forall P(x) \implies Q)$. As required.

($\impliedby$)

Since $(\forall x.(P(x) \implies Q))$, $P(x) \implies Q$ for at least one x. So $((\exists x.P(x)) \implies Q)$ as required.