2.3.1

$$\begin{array}{l} p \Rightarrow q \\ \underline{\sim q \qquad} \\ \therefore \sim p \end{array}$$

proof by contradiction.

2.3.2

$$\begin{array}{l} p \Rightarrow q \\ \underline{q \qquad} \\ \therefore p \end{array}$$

not valid.

2.3.3

$$\begin{array}{l} p \Rightarrow q \\ \underline{\sim p \qquad} \\ \therefore \sim q \end{array}$$

not valid.

2.3.4

$$\begin{array}{l} p \Rightarrow q \\ \underline{p \qquad} \\ \therefore q \end{array}$$

modus ponens.

2.3.9

$$\begin{array}{l} \sim p \Rightarrow q \\ r \Rightarrow p \\ \underline{r \qquad\quad} \\ \therefore q \end{array}$$

not valid.

2.3.15 Prove that the sum of two odd numbers is even.

For two arbitrary odd integers $a, b \in \mathbb{Z}$ there exist integers $m, n \in \mathbb{Z}$ such that

$$a = 2m+1 \quad \text{and} \quad b = 2n+1.$$

Thus their sum is

$$a+b = 2m+1+2n+1 = 2(m+n+1).$$

Any multiple of 2 is even, so $a+b$ is even. $\square$

2.3.17 Prove that (odd integers, $+, *$) is closed w.r.t. $*$.

Assume again $a, b \in \mathbb{Z}$ are odd with $m, n \in \mathbb{Z}$ such that $a = 2m+1$ and $b = 2n+1$. Then the structure is closed under multiplication, since

$$a * b = (2m+1) * (2n+1) = 4mn + 2m + 2n + 1 = 2(2mn+m+n)+1$$

is odd.

2.3.18 n^2 is even if and only if n is even.

Assuming n is even, then $n = 2m$, $m \in \mathbb{Z}$, and

$$n^2 = (2m)^2 = 4m^2 = 2 \cdot 2m^2$$

which is even. So n even $\Rightarrow n^2$ even.

Assume n is odd, then $n = 2m+1$, and

$$n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$$

is odd. So n odd $\Rightarrow n^2$ odd which is the contrapositive of n^2 even $\Rightarrow n$ even. Thus we have the conclusion. $\square$

2.3.21 (a) $A \subseteq B$ is necessary and sufficient for $A \cup B = B$.

$A \subseteq B \Leftrightarrow A \cup B = B$.

"$\Rightarrow$": Assume $A \subseteq B$. For any $x \in A \cup B$, either $x \in A$ or $x \in B$. If $x \in A$, then $x \in B$ by assumption and and $A \cup B \subseteq B \Rightarrow A \cup B = B$.

"$\Leftarrow$": Assume $A \cup B = B$, then for any $x \in A$ we have $x \in A \cup B = B$. So $A \subseteq B$.

Thus $A \subseteq B \Leftrightarrow A \cup B = B$. $\square$

(b) $A \subseteq B \Leftrightarrow A \cap B = A$.

"$\Rightarrow$": Assume $A \subseteq B$. For any $x \in A \cap B$, $x \in A$, so $A \cap B \subseteq A$. If $x \in A$, then $x \in B$ by assumption and so $x \in A \cap B$ and thus $A \subseteq A \cap B$. Thus $A \subseteq B \Rightarrow A \cap B = A$.

"$\Leftarrow$" Assume $A \cap B = A$, then for any $x \in A$ we have $x \in A \cap B$ by assumption. Then $x \in B$ and therefore $A \subseteq B$, so we have $A \cap B = A \Rightarrow A \subseteq B$. $\square$

2.3.22 If k is odd $\Leftrightarrow k^3$ is odd.

"$\Rightarrow$":

Let $k \in \mathbb{Z}$ be odd, then there is an $n \in \mathbb{Z}$ such that $k = 2n+1$. Then

$$k^3 = (2n+1)^3 = 8n^3 + 12n^2 + 6n + 1 = 2(4n^3 + 6n^2 + 3n) + 1,$$

which is odd.

"$\Leftarrow$" We prove $\sim p \Rightarrow \sim q$, which is logically equivalent to $q \Rightarrow p$.

Assuming $k = 2n$ then

$$k^3 = (2n)^3 = 8n^3,$$

which is even. $\square$

2.3.23 $n^2 + 41n + 41$ is prime for every $n \in \mathbb{Z}$. (Assume $n \geq 1$?)

For $n = 41$, we have that $n \mid n^2 + 41n + 41$, so $n^2 + 41n + 41$ is not prime, and the statement is false.

2.3.30 Valid proof by contradiction. Given $p \Rightarrow q$, the assumption $\sim p \Rightarrow \sim q$, i.e. contradiction.

2.3.33 If $x \in \mathbb{Q}$ and $y \in \mathbb{R} \setminus \mathbb{Q}$, then $x+y \in \mathbb{R} \setminus \mathbb{Q}$.

Assume for contradiction that $x+y \in \mathbb{Q}$. There exist $p, q \in \mathbb{Z}$, $q \neq 0$, such that $x+y = \frac{p}{q}$. Since x is rational there exist $a, b \in \mathbb{Z}$, $b \neq 0$, such that $x = \frac{a}{b}$. It follows that

$$y = x+y-x = \frac{p}{q} - \frac{a}{b} = \frac{pb-aq}{bq} \in \mathbb{Q}.$$

This contradict y being irrational. Thus if x is rational and y irrational, then $x+y$ is irrational. $\square$

2.3.34 If $2y$ is irrational, then y is irrational.

Contrapositive: if y is rational, then $2y$ is rational.

Let $y \in \mathbb{Q}$, so that $y = \frac{p}{q}$, $q \neq 0$. Then $2y = \frac{2p}{q} \in \mathbb{Q}$. $\square$

2.4.1 Let $P(n)$ be the predicate $2+4+6+\cdots+2n = n(n+1)$.

Basis step: for $n=1$ $P(1)$ is the statement $2 \cdot 1 = 1 \cdot (1+1)$, which holds true.

Induction step: assume for $k \geq 1$ that if $P(k)$ is true, then $P(k+1)$ is true. For fixed $k \geq 1$

$$2+4+6+\cdots+2k = k(k+1)$$

is true.

For $k+1$ we have $P(k+1)$

$$\begin{aligned} \underbrace{2+4+6+\cdots+2k}_{k(k+1)}+2(k+1) &= k(k+1)+2(k+1) \\ &= (k+1)(k+2) \\ &= (k+1)((k+1)+1). \end{aligned}$$

So $P(k+1)$ holds. Since $P(1)$ is true and $P(k) \Rightarrow P(k+1)$, then it follows by the principle of mathematical induction that $P(n)$ is true for all $n \in \mathbb{Z}_+$. $\square$

2.4.6 Let $P(n)$ be the predicate $1+a+a^2+\cdots+a^{n-1} = \frac{a^n-1}{a-1}$, $a \neq 1$.

Basis step: for $n=1$ the statement $P(1)$ is $1 = \frac{a-1}{a-1}$, which is true.

Induction step: assume for $k \geq 1$ that $P(k)$ is true.

$$1 + a + a^2 + \cdots + a^{k-1} + a^k = \frac{a^k - 1}{a-1} + a^k$$
$$= \frac{a^k - 1 + a^k(a-1)}{a-1}$$
$$= \frac{a^{k+1} - 1}{a-1}.$$

So $P(k+1)$ holds.

Since $P(1)$ is true and $P(k) \Rightarrow P(k+1)$ it follows by the principle of mathematical induction that $P(n)$ is true for all $n \in \mathbb{Z}_+$. ⌑

2.4.10 Let $P(n)$ be $1 + 2^n < 3^n$, $n \geq 2$.

$P(2)$ is $1 + 2^2 = 5 < 9 = 3^2$, i.e. true. Assume for $k \geq 2$ that $P(k)$ is true.
Then

$$1 + 2^{k+1} < 2 + 2^{k+1} = 2(1 + 2^k) \underset{\text{by assumption}}{<} 2 \cdot 3^k < 3^{k+1},$$

so $P(k) \Rightarrow P(k+1)$.

Since $P(1)$ is true and $P(k) \Rightarrow P(k+1)$ it follows by the principle of mathematical induction that $P(n)$ is true for all $n \in \mathbb{Z}_+$. ⌑

2.4.16 Let $P(n)$ be $3 \mid (n^3 - n)$ $\forall n \in \mathbb{Z}_+$.

We have $P(1)$: $3 \mid (1^3 - 1)$ is true. Assume for $k \geq 1$ that $P(k)$ is true.
Now for $P(k+1)$:

$$(k+1)^3 - (k+1) = (k^2 + 2k + 1)(k+1) - k - 1 = k^3 + 3k^2 + 3k - k$$
$$= k^3 - k + 3(k^2 + k)$$

By assumption $3 \mid (k^3 - k)$ and $3 \mid 3(k^2 + k)$, so $3 \mid k^3 - k + 3(k^2 + k)$ and $P(k+1)$ is true.

Since $P(1)$ is true and $P(k) \Rightarrow P(k+1)$ it follows by the principle of mathematical induction that $P(n)$ is true for all $n \in \mathbb{Z}_+$. ⌑

2.4.20 Let $P(n)$ be $2 \mid (2n - 1)$.

(a) Prove that $P(k) \Rightarrow P(k+1)$ is a tautology.

Assume $P(k)$ is true.

$$2(k+1) - 1 = (2k - 1) + 2,$$

where $2 \mid (2k-1)$ by assumption and $2 \mid 2$, so $P(k+1)$ is true. Thus $P(k) \Rightarrow P(k+1)$ is a tautology.

(b) Show that $P(n)$ is false $\forall n \in \mathbb{Z}_+$. Since $2n - 1$ is an odd number $2 \nmid (2n-1)$ for any $n \in \mathbb{Z}_+$.

(c) Do (a) and (b) contradict induction?

No, since $P(1)$ is not true (or any $P(k)$ for that matter).

2.4.28 Prove that for integers greater than 27 we can write it as $5a+8b$, where $a,b \in \mathbb{Z}_+$.

Let $P(n)$ be $\exists a,b \in \mathbb{Z}_+ : 5a+8b=n$. Observe that

$$P(28): \quad 5\cdot 4 + 8\cdot 1 = 28$$
$$P(29): \quad 5\cdot 1 + 8\cdot 3 = 29$$
$$P(30): \quad 5\cdot 6 + 8\cdot 0 = 30$$
$$P(31): \quad 5\cdot 3 + 8\cdot 2 = 31$$
$$P(32): \quad 5\cdot 0 + 8\cdot 4 = 32$$

Assume that $k \geq 32$ and $P(28), P(29), \dots, P(k)$ are true. There exist $a,b \in \mathbb{Z}_+$ such that $5a+8b=k-4$, but then

$$5(a+1)+8b=k+1,$$

and so $P(k+1)$ is true.

It follows by strong induction that $P(n)$ is true for all $n \geq 28$.

2.4.35 Set $z_0 = x$ and $w_0 = y$, and recursively define $z_{n+1} = z_n - 1$ and $w_{n+1} = w_n - 1$ for $n \geq 0$.

Let $P(n)$ be the predicate $x - z_n + w_n = y$.

We see that $P(0)$ is true by definition of z_0 and w_0. For $k \geq 1$ assume $P(k)$ is true. It follows that

$$x - z_{k+1} + w_{k+1} = x - (z_k - 1) + (w_k - 1)$$
$$= x - z_k + w_k = y,$$

and so $P(k+1)$ is true. Since $P(0)$ is true and $P(k) \Rightarrow P(k+1)$ by the principle of mathematical induction $P(n)$ is true. Thus loop invariant.

The loop terminat when $n=y$, so the output is $z_y = x - y + w_y = x - y$.

2.4.36 Set $R_0 = 1$ and $K_0 = 2M$, and recursively define $R_n = R_{n-1}\cdot N$ and $K_n = K_{n-1} - 1$ for $n \geq 1$.

Let $P(n)$ be $R_n \cdot N^{K_n} = N^{2M}$. $P(0)$ is $R_0 \cdot N^{K_0} = N^{2M}$ which is true. For $k \geq 1$ assume $P(k)$ is true. Then

$$R_{k+1}\cdot N^{K_{k+1}} = R_k \cdot N \cdot N^{K_k - 1} = R_k \cdot N^{K_k} = N^{2M}.$$

Thus $P(k) \Rightarrow P(k+1)$. By the principle of mathematical induction $P(n)$ is true for all $n \in \mathbb{Z}_+$. For $n = 2M$ the loop terminates, and

$$R_{2M} = R_{2M}\cdot N^0 = R_{2M}\cdot N^{K_{2M}} = N^{2M}.$$