1.12 - Problem 3. If $2^n + 1$ is prime, then $n$ is even or $n = 1$. Indeed, assume $n$ is odd and $n > 1$. Then $(-1)^n = -1$. So we have:

\[
2^n + 1 = 2^n - (-1)^n = (2 - (-1)) \sum_{k=0}^{n-1} (-1)^k 2^{n-1-k}
\]

So $2^n + 1$ is divisible by 3. Furthermore, $2^n + 1 > 3$ since $n > 1$. So $2^n + 1$ is not prime.

1.12 - Problem 6. Let us assume first that $f$ is injective. Let $C$ be a set and $g_1, g_2 : C \to A$ be two maps such that $f \circ g_1 = f \circ g_2$. We want to prove that $g_1 = g_2$. Let $x \in C$, we have $f(g_1(x)) = f(g_2(x))$. Since $f$ is injective, we have $g_1(x) = g_2(x)$. This holds for any $x \in C$, so $g_1 = g_2$.

Conversely, assume that for any set $C$ and any two maps $g_1, g_2 : C \to A$ such that $f \circ g_1 = f \circ g_2$ we have $g_1 = g_2$. We want to prove that $f$ is injective. Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$. Consider the set $C = \{0\}$, and the maps $g_1 : C \to A, 0 \mapsto x_1$ and $g_2 : C \to A, 0 \mapsto x_2$. Then we have $f \circ g_1 = f \circ g_2$. So by assumption, $g_1 = g_2$. Hence $x_1 = g_1(0) = g_2(0) = x_2$. So $f$ is injective.

This ends the proof of the equivalence.

1.12 - Problem 8. Since a countable set is in bijection with $\mathbb{N}$, it suffices to prove that a subset of $\mathbb{N}$ is either finite or countable. Let $S$ be a subset of $\mathbb{N}$ that is not finite, we want to prove that $S$ is countable. We do so by explicitly constructing a bijection $f : \mathbb{N} \to S$.

Let us define $f$ inductively.

- Define $f(0) = \min(S)$. This is well defined by the well-ordering principle, since $S$ is a non-empty subset of $\mathbb{N}$.
- Assume we have defined $f(0), \ldots, f(n)$ for some $n \in \mathbb{N}$. Since $S$ is not finite, $S \setminus \{f(0), \ldots, f(n)\}$ is a non-empty subset of $\mathbb{N}$. By the well-ordering principle, we can define:

\[
f(n + 1) = \min(S \setminus \{f(0), \ldots, f(n)\}).
\]
Let us now prove that $f$ is a bijection. First, it follows from the construction that if $m > n$, $f(m) \notin \{f(0), \ldots, f(n), \ldots, f(m - 1)\}$. In particular, $f(m) \neq f(n)$, so $f$ is injective.

To show surjectivity, let us show by induction on $k$ that there exists $P$ such that $\forall k \exists \{f(0), \ldots, f(k)\}$.

- We have $\min(S) = f(0)$, so $S \cap \{0, \ldots, \min(S)\} = \{f(0)\}$, and $P(\min(S))$ is true.
- If $P(n)$ is true for some $n \geq \min(S)$ then we have $S \cap \{0, \ldots, n\} = \{f(0), \ldots, f(k)\}$ for some $k$. There are two cases: either $n + 1 \notin S$, in which case we have $S \cap \{0, \ldots, n + 1\} = \{f(0), \ldots, f(k)\}$, or $n + 1 \in S$. In that last case, we have $n + 1 = f(k + 1)$, and $S \cap \{0, \ldots, n + 1\} = \{f(0), \ldots, f(k + 1)\}$. Thus $P(n + 1)$ holds.

So by the induction principle, $P(n)$ is true for all $n \geq \min(S)$. Now if $n \in S$, the property $P(n)$ tells us in particular that $n \in f(\mathbb{N})$. Hence $f$ is surjective.

So $S$ is countable, and we are done.

2.17 - Problem 1. We prove by induction on $n$ the property $p(n)$: "any set of cardinal $n$ has $2^n$ subsets."

- If $X = \emptyset$ (i.e. the cardinal of $X$ is 0), then $X$ has $1 = 2^0$ subset, namely $\emptyset$. So $p(0)$ is true.
- Assume $p(n)$ holds for some $n \geq 0$, and consider a set $X$ of cardinal $n + 1$. Pick an element $x_0 \in X$. We can divide the subsets of $X$ into two classes: those containing $x_0$, and those not containing $x_0$. Formally, we have a disjoint union:

$$
\mathcal{P}(X) = \{S \subseteq X, x_0 \in S\} \cup \{S \subseteq X, x_0 \notin S\}
$$

Now, there are bijections:

$$
\begin{align*}
\begin{cases}
\{S \subseteq X, x_0 \in S\} & \rightarrow \mathcal{P}(X \setminus \{x_0\}) \\
S & \rightarrow S \setminus \{x_0\} \\
T \cup \{x_0\} & \leftrightarrow T
\end{cases}
\end{align*}
$$

$$
\begin{align*}
\begin{cases}
\{S \subseteq X, x_0 \notin S\} & \rightarrow \mathcal{P}(X \setminus \{x_0\}) \\
S & \rightarrow S \setminus \{x_0\} \\
T & \leftrightarrow T
\end{cases}
\end{align*}
$$

Since $X \setminus \{x_0\}$ has cardinal $n$, $\mathcal{P}(X \setminus \{x_0\})$ has cardinal $2^n$ by $p(n)$. Thus by the bijections above, $\{S \subseteq X, x_0 \in S\}$ and $\{S \subseteq X, x_0 \notin S\}$ have cardinal $2^n$. Using the disjoint union decomposition, we get that $\mathcal{P}(X)$ has cardinal $2^n + 2^n = 2^{n+1}$. Hence $p(n + 1)$ is true.

Hence by the induction principle, the property $p(n)$ is true for all $n \geq 0$.

2.17 - Problem 2. Let us prove by induction on $n$ the formula:

$$
\sum_{k=1}^{n} k^3 = \frac{n^2(n + 1)^2}{4}.
$$

- We have $1^3 = 1 = \frac{1^2(1+1)^2}{4}$, so the result holds for $n = 1$. 


• Assume the result holds for some \( n \geq 1 \). Then we have:
\[
\sum_{k=1}^{n+1} k^3 = \sum_{k=1}^{n} k^3 + (n+1)^3 \\
= \frac{n^2(n+1)^2}{4} + (n+1)^3 \quad \text{using the result for } n \\
= (n+1)^2 \frac{n^2 + 4(n+1)}{4} \\
= \frac{(n+1)^2(n+2)^2}{4}.
\]
So the result holds for \( n+1 \).

By the induction principle, the formula is true for all \( n \geq 1 \).

2.17 - Problem 3. The recurrence relation defining the Fibonacci sequence is:
\[ F_{n+1} = F_n + F_{n-1}. \]

From linear algebra, we know how to find an explicit formula for such a sequence. First, we start by solving the characteristic equation of the relation: \( X^2 = X + 1 \). The two roots are \( \frac{1+\sqrt{5}}{2} \) and \( \frac{1-\sqrt{5}}{2} \). Then we know that the solutions have the form:
\[ F_n = a \left( \frac{1+\sqrt{5}}{2} \right)^n + b \left( \frac{1-\sqrt{5}}{2} \right)^n \]
for some real numbers \( a,b \). To find \( a \) and \( b \), it suffices to use \( F_0 = 0 \) and \( F_1 = 1 \). We get \( a = \frac{1}{\sqrt{5}} = -b \). Hence the formula we wanted is:
\[ F_n = \frac{1}{\sqrt{5}} \left( \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right). \]

Remark: it is pretty incredible (and a priori not obvious if one does not know the recurrence relation) that this formula returns an integer!

Now, let us prove by (strong) induction on \( n \) that \( F_n < 2^n \).

• We have \( F_0 = 0 < 2^0 \) and \( F_1 = 1 < 2^1 \).
• Assume that \( F_{n-1} < 2^{n-1} \) and \( F_n < 2^n \) for some \( n \leq 1 \). Then we have:
\[
F_{n+1} = F_n + F_{n-1} \\
< 2^n + 2^{n-1} \\
< 2^n + 2^n \\
= 2^{n+1}.
\]
Hence we get \( F_{n+1} < 2^{n+1} \), and the property is true by induction.
Remark: since we used the property for \( n \) AND \( n - 1 \) to prove it for \( n + 1 \), we have to check it for two consecutive integers (0 and 1 here) to start the induction.

Problem 3. We have the following result: if \( S \) is a finite set, any surjective (resp. injective) function \( S \to S \) is a bijection.
Proof: for any function \( f : S \to S \) we get a partition:
\[
S = \bigsqcup_{y \in S} f^{-1}(y)
\]
where \( f^{-1}(y) = \{ x \in S, f(x) = y \} \). Now if \( f \) is surjective (resp. injective) we have \( |f^{-1}(y)| \geq 1 \) (resp. \( |f^{-1}(y)| \leq 1 \)) for all \( y \). Hence we have:
\[
|S| = \sum_{y \in S} |f^{-1}(y)| \geq \sum_{y \in S} 1 = |S|
\]
(resp. \( |S| = \sum_{y \in S} |f^{-1}(y)| \leq \sum_{y \in S} 1 = |S| \))
This forces \( |f^{-1}(y)| = 1 \) for all \( y \in S \), which means that \( f \) is a bijection.

Now we know that the number of bijections \( S \to S \) is \( n! \) if \( S \) has cardinal \( n \).

Problem 4. If \( f(x) = ax + b \), then we have \( (f \circ f)(x) = a^2x + b(1 + a) \). Assume that we have \( f \circ f = \text{id}_\mathbb{Z} \) Plugging in 0 and 1 yields the two equations:
\[
\begin{cases}
    b(1 + a) = 0 \\
    a^2 + b(1 + a) = 1
\end{cases}
\]
Thus we have \( a^2 = 1 \), so \( a = 1 \) or \( a = -1 \). If \( a = 1 \), the first equation gives \( b = 0 \). If \( a = -1 \), the first equation doesn’t give any additional condition. In conclusion, we have found that a necessary condition on \( (a, b) \) to have \( f \circ f = \text{id}_\mathbb{Z} \) is \( (a = -1) \) or \( (a = 1 \text{ and } b = 0) \).

Conversely, it is very easy to check that the functions \( x \mapsto -x + b \) (where \( b \) is an arbitrary fixed integer) and \( x \mapsto x \) satisfy the desired property.