INTRODUCTION TO PROOFS: HW5 SOLUTIONS

Your solutions should be organised to proceed logically, and should be written in complete sentences.

Note: In the solutions, remarks made in square brackets [such as these] are not necessary for a complete proof.

7.1. Let $a_1, a_2, a_3, \ldots$ be the Fibonacci sequence; so $a_1 = a_2 = 1$, and for $i \in \mathbb{Z}$ with $i \geq 3$, $a_i = a_{i-1} + a_{i-2}$.

(a) Use strong induction to prove that for $n \in \mathbb{Z}_+$,

$$a_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

(Suggestion: Show directly that $P(1), P(2)$ hold. Then suppose that $k \in \mathbb{Z}$ with $k \geq 2$, and that $P(i)$ holds for all $i \in \mathbb{Z}_+$ with $i \leq k$, and use this to evaluate $a_k + a_{k-1}$.)

Solution:

(a) For $n \in \mathbb{Z}_+$, let $P(n)$ be the proposition that

$$a_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

[Base case:] We have

$$\begin{aligned}\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1\right] &= \frac{1}{\sqrt{5}}\sqrt{5} \\ &= 1 \\ &= a_1,\end{aligned}$$

and

$$\begin{aligned}\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2\right] &= \frac{1}{\sqrt{5}}\left[\frac{6+2\sqrt{5}}{2} - \frac{6-2\sqrt{5}}{2}\right] \\ &= \frac{1}{\sqrt{5}}\sqrt{5} \\ &= 1 \\ &= a_2.\end{aligned}$$

Thus $P(1), P(2)$ hold.

[Induction step:] Now suppose that $k \in \mathbb{Z}$ with $k \geq 2$ and that $P(i)$ holds for all $i \in \mathbb{Z}_+$ with $i \leq k$. Using the assumption that

$P(k)$ and $P(k-1)$ hold, we have

$$\begin{aligned}
a_{k+1} &= a_k + a_{k-1} \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right] \\
&\quad + \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right] \\
&= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k\left(\frac{3+\sqrt{5}}{2}\right)\frac{2}{2} \\
&\quad - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^k\left(\frac{3-\sqrt{5}}{2}\right)\frac{2}{2} \\
&= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k\left(\frac{1+\sqrt{5}}{2}\right)^2 \\
&\quad - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^k\left(\frac{1-\sqrt{5}}{2}\right)^2 \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right].
\end{aligned}$$

Thus $P(i)\ \forall i \in \mathbb{Z}_+$ with $i \le k \implies P(k+1)$; hence by the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{Z}_+$.

7.3. (a) Find all primes p so that $7p+4$ is the square of a positive integer. (Suggestion: First suppose that p is a prime so that $7p+4 = n^2$ for some $n \in \mathbb{Z}_+$, and deduce constaints on p. Then consider all primes p subject to these constraints and determine for which of these p we have that $7p + 4 = n^2$ for some $n \in \mathbb{Z}_+$.)

Solution: (a) Suppose first that p is a prime so that $7p + 4 = n^2$; so $7p = n^2 - 4 = (n+2)(n-2)$. Thus $n+2$ divides $7p$, and since $n \in \mathbb{Z}_+$, we have that $n + 2 > 0$. By the Fundamental Theorem of Arithmetic, the only positive divisors of $7p$ are $1, 7, p, 7p$. Hence $n+2$ is one of these values.

Suppose $n+2 = 1$; then $n - 2 < 0$ and hence $7p < 0$, a contradiction since $7, p > 0$.

Suppose $n + 2 = 7$. Then $n - 2 = 3$, and $21 = 7p$. Hence $p = 3$, which is prime.

Suppose $n + 2 = p$. Then $n - 2 = p - 4$, and $7p = p(p-4)$. So $7 = p - 4$, which implies that $p = 11$, and 11 is prime.

Suppose $n+2 = 7p$. Hence $n-2$ must equal 1 [since $(n+2)(n-2) = 7p$], so n must equal 3. Then $7p = 3$, which is impossible [since $7p > 7 > 3$, or since 3 is prime and $7p$ is not, or since 7 does not divide 3].

Thus if p is a prime so that $7p + 4 = n^2$ for some $n \in \mathbb{Z}_+$, then $p = 3$ or 11.

On the other hand, suppose $p = 3$. Then $7p + 4 = 25 = 5^2$. Similary, with $p = 11$, we have $7p + 4 = 81 = 9^2$.

Hence with p prime, we have $7p + 4 = n^2$ for some $n \in \mathbb{Z}_+$ if and only if $p = 3$ or 11.

7.4. Suppose $k \in \mathbb{Z}$ with $k \geq 2$, and $m_1, \ldots, m_{k+1} \in \mathbb{Z}_+$ are pairwise relatively prime, meaning that $\text{hcf}(m_i, m_j) = 1$for $i, j \in \mathbb{Z}$ with $1 \leq i \leq k+1$, $1 \leq j \leq k+1$ and $i \neq j$. Set $M = m_1 m_2 \cdots m_k$.

(a) Suppose p is a prime so that $p|M$. Show that $p \nmid m_{k+1}$.

Solution:

(a) Suppose p is a prime so that $p|M$. Then since $M = m_1 m_2 \cdots m_k$, we must have $p|m_i$ for some $i \in \mathbb{Z}$ $(1 \leq i \leq k)$. Since $\text{hcf}(m_i, m_{k+1}) = 1$, we know $p \nmid m_{k+1}$.

8.4. Suppose X, Y are countable sets.

(a) Show that $X \times Y$ is countable. (Suggestion: either construct a bijective map from $\mathbb{Z}_+ \times \mathbb{Z}_+$ to $X \times Y$, and use that $\mathbb{Z}_+ \times \mathbb{Z}_+$ is countable, or alternatively, using that $\mathbb{Z}_+ \times \mathbb{Z}_+$ is countable and $X \times Y$ is infinite [as shown in the notes], construct an injective map from $X \times Y$ into $\mathbb{Z}_+$. In the first instance, you must **prove** the map is bijective, and then explain why this means $X \times Y$ is countable; in the second instance, you must **prove** the map is injective, and then explain why this means $X \times Y$ is countable.)

Solution: (a) Since $X, Y, \mathbb{Z}_+ \times \mathbb{Z}_+$ are countable, there exist bijective maps $f : \mathbb{Z}_+ \to X$, $g : \mathbb{Z}_+ \to Y$, and $h : \mathbb{Z}_+ \to \mathbb{Z}_+ \times \mathbb{Z}_+$.

[Solution 1:] Define $j : \mathbb{Z}_+ \times \mathbb{Z}_+ \to X \times Y$ by $j(m, n) = (f(m), g(n))$. We claim j is bijective. To see this, first suppose $(m, n), (m', n') \in \mathbb{Z}_+ \times \mathbb{Z}_+$ so that $j(m, n) = j(m', n')$. So $(f(m), g(n)) = (f(m'), g(n'))$, which means $f(m) = f(m')$ and $g(n) = g(n')$. Since f, g are injective, we have $m = m'$, $n = n'$, and hence $(m, n) = (m', n')$. Thus j is injective. To see j is surjective, take $(x, y) \in X \times Y$. Since f is surjective, there is some $m \in \mathbb{Z}_+$ so that $f(m) = x$; similarly, since g is surjective, there is some $n \in \mathbb{Z}_+$ so that $g(n) = y$. Thus $j(m, n) = (f(m), g(n)) = (x, y)$, showing that j is surjective. Hence j is bijective. So $|\mathbb{Z}_+ \times \mathbb{Z}_+| = |X \times Y|$, and since $\mathbb{Z}_+ \times \mathbb{Z}_+$ is countable, $X \times Y$ must be countable. [One also has that $j \circ h : \mathbb{Z}_+ \to X \times Y$ is bijective since j, h are bijective, which means $X \times Y$ is countable.]

[Solution 2:] [This uses the result that if we have an injective function from a set A into $\mathbb{Z}_+$ then A is either finite or countable.] Since f, g are bijective, we know $f^{-1} : X \to \mathbb{Z}_+$ and $g^{-1} : Y \to \mathbb{Z}_+$ exist and are bijective. Define $k : X \times Y \to \mathbb{Z}_+ \times \mathbb{Z}_+$ by $k(x, y) = (f^{-1}(x), g^{-1}(y))$. We claim k is injective. To see this, suppose $(x, y), (x', y') \in X \times Y$ with $k(x, y) = k(x', y')$. Thus $(f^{-1}(x), g^{-1}(y)) = (f^{-1}(x'), g^{-1}(y'))$, so $f^{-1}(x) = f^{-1}(x')$ and $g^{-1}(y) = g^{-1}(y')$. Since f^{-1}, g^{-1} are injective, this means $x = x'$, $y = y'$, and so $(x, y) = (x', y')$. Thus k is injective. We also know that $h^{-1} : \mathbb{Z}_+ \times \mathbb{Z}_+ \to \mathbb{Z}_+$ exists and is bijective, so $h^{-1} \circ k : X \times Y \to \mathbb{Z}_+$

is injective. Since $X \times Y$ is infinite, this means $X \times Y$ must be countable.

8.5. Note that $\mathbb{Z}_+ \subseteq \mathbb{Q}_+ \subseteq \mathbb{Q}$; since $\mathbb{Z}_+$ is infinite, so are $\mathbb{Q}_+, \mathbb{Q}$.

(a) Show that $\mathbb{Q}_+$ is countable. (Suggestion: Recall that

$$\mathbb{Q}_+ = \left\{ \frac{a}{b} : \ a, b \in \mathbb{Z}_+, \ \text{hcf}(a,b) = 1 \right\}.$$

Begin by defining an injective map from $\mathbb{Q}_+$ into $\mathbb{Z}_+ \times \mathbb{Z}_+$. Note that you must **prove** this map is injective, then you must explain why that means $\mathbb{Q}_+$ is countable.)

Solution:

(a) [This uses the result that if $f : A \to \mathbb{Z}_+$ is injective then A is finite or countable.] Define $f : \mathbb{Q}_+ \to \mathbb{Z}_+ \times \mathbb{Z}_+$ by $f(a/b) = (a, b)$ where $a, b \in \mathbb{Z}_+$ with $\text{hcf}(a, b) = 1$. [Note: Stating the condition that $\text{hcf}(a, b) = 1$ is important, else this does not give a definition of a function f: We have $(na)/(nb) = a/b$ for all $n, a, b \in \mathbb{Z}_+$, but we do not have $(na, nb) = (a, b)$ for $n, a, b \in \mathbb{Z}_+$ with $n > 1$.] To show f is injective, suppose $a/b, c/d \in \mathbb{Q}_+$ with $a, b, c, d \in \mathbb{Z}_+$, $\text{hcf}(a, b) = 1 = \text{hcf}(c, d)$, and $f(a/b) = f(c/d)$. Thus $(a, b) = (c, d)$, so $a = c$, $b = d$, and hence $a/b = c/d$. So f is indeed injective. Since $\mathbb{Z}_+ \times \mathbb{Z}_+$ is countable, we know there is a bijective function $g : \mathbb{Z}_+ \times \mathbb{Z}_+ \to \mathbb{Z}_+$. Thus $g \circ f : \mathbb{Q}_+ \to \mathbb{Z}_+$ is injective; since $\mathbb{Q}_+$ is infinite, we must have that $\mathbb{Q}_+$ is countable.

9.3. Let A, B be sets. Show:

(a) $(A \subseteq B) \iff (\mathcal{P}(A) \subseteq \mathcal{P}(B))$.

(b) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

Solutions:

(a) Suppose $A \subseteq B$. Then every subset of A is a subset of B, so every element of $\mathcal{P}(A)$ is an element of $\mathcal{P}(B)$ [as $\mathcal{P}(A)$ is the collection of all subsets of A and $\mathcal{P}(B)$ is the collection of all subsets of B]. Thus $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Now suppose $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. We know $A \in \mathcal{P}(A)$, so $A \in \mathcal{P}(B)$, meaning that $A \subseteq B$.

Hence $A \subseteq B \iff \mathcal{P}(A) \subseteq \mathcal{P}(B)$.

(b) Let $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$. So $X \in \mathcal{P}(A)$, meaning $X \subseteq A$, or $X \in \mathcal{P}(B)$, meaning $X \subseteq B$. Since $A \subseteq A \cup B$ and $B \subseteq A \cup B$, we have $X \subseteq A \cup B$; hence $X \in \mathcal{P}(A \cup B)$. Hence $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.