1. 0 marks Find a formula for $1 + 4 + 7 + \ldots + (3n - 2)$ for positive integers n, and then verify your formula by mathematical induction.

Solution: As in example 6.2, the simplest way to find a formula for $S_n = 1 + 4 + 7 + \ldots + (3n - 2)$ is to notice that

$$2S_n = (3n-1) + (3n-1) + \ldots + (3n-1) = n(3n-1)\,.$$

Dividing both side by 2 gives $S_n = \frac{3n^2-n}{2}$. Lets prove this formula using induction. For $n = 1$ we have $S_n = 2/2 = 1$ so the base case holds. Now, if

$$S_{n-1} = \frac{3(n-1)^2 - n + 1}{2} = \frac{3n^2 - 7n + 4}{2}\,,$$

then

$$\begin{aligned} S_n = S_{n-1} + (3n-2) &= \frac{3n^2 - 7n + 4}{2} + (3n-2) \\ &= \frac{3n^2 - 7n + 4 + (6n-4)}{2} \\ &= \frac{3n^2 - n}{2}\,. \end{aligned}$$

The inductive step holds and so the formula is valid for all $n > 1$.

2. 3 marks Prove that $3^n > n^2$ for every positive integer n.

Solution: First, if $n = 1$ then $3^n = 3 > 1 = n^2$ so the base case holds. To make the calculations easier, we check the case $n = 2$ by hand as well. For $n = 2$, $3^n = 9 > 2 = n^2$. Now, assume that $3^n > n^2$ holds for $n \geq 2$, then

$$3^{n+1} = 3 \times 3^n > 3 \times n^2 = n^2 + 2n^2 \geq n^2 + 4n = n^2 + 2n + 2n \geq n^2 + 2n + 1 = (n+1)^2\,.$$

By the principle of mathematical induction, $3^n > n^2$ for every positive integer n.

3. 4 marks Show that $5 \mid n^5 - n$ for every natural number n.

Solution: We proceed by induction. Since $0 \cdot 5 = 0 = 1^5 - 1$, $5 \mid n^5 - n$ holds for $n = 1$. Now, assume that $5 \mid n^5 - n$. Then $n^5 - n = 5 \cdot k$ for some $k \in \mathbb{Z}$. Now we check that

$$\begin{aligned} (n+1)^5 - (n+1) &= n^5 + 5n^4 + 20n^3 + 20n^2 + 5n + 1 - (n+1) \\ &= n^5 - n + 5n^4 + 20n^3 + 20n^2 + 5n \\ &= 5(k + n^4 + 4n^3 + 4n^2 + n)\,. \end{aligned}$$

By the principle of induction, $5 \mid n^5 - n$ for every $n > 0$.

4. [0 marks] Prove that $(1+2+\ldots+n)^2 = 1^3+2^3+\ldots+n^3$ for every $n \in \mathbb{N}$.

Solution: We proceed by induction. Since $1^2 = 1^3$ the equality holds for $n = 1$. Assume that the equality holds for all integers up to $n-1$. Recall that $1+2+\ldots+k = \frac{k(k+1)}{2}$. Then

$$\begin{aligned} 1^3+2^3+\ldots+(n-1)^3+n^3 &= (1+2+\ldots+n-1)^2+n^3 \\ &= \left(\frac{n(n-1)}{2}\right)^2+n^3 \\ &= \frac{n^4-2n^3+n^2}{4}+n^3 \\ &= \frac{n^4+2n^3+n^2}{4} \\ &= \left(\frac{n(n+1)}{2}\right)^2 \\ &= (1+2+\ldots+n)^2 \end{aligned}$$

By the principle of induction, $(1+2+\ldots+n)^2 = 1^3+2^3+\ldots+n^3$ for every $n \in \mathbb{N}$.

5. a) [0 marks] In Mathematical Proof, Chapter 6.1 we saw that $1^2+2^2+\ldots+n^2$ is the number of squares in an $n \times n$ "chess board" composed of n^2 1×1 squares. What does $1^3+2^3+3^3+\ldots+n^3$ represent geometrically?

   b) [0 marks] Use mathematical induction to prove that $1^3+2^3+3^3+\ +n^3 = \frac{n^2(n+1)^2}{4}$ for every positive integer n.

Solution:

a) Let C be the $n \times n \times n$ cube of n^3 $1 \times 1 \times 1$ cubes. Then $1^3+2^3+3^3+\ldots+n^3$ will be the number of distinct $k \times k \times k$ cubes in C.

b) We verify this formula by mathematical induction. Since $1^3 = \frac{1^2(1+1)^2}{4} = 1$, the formula holds for $n = 1$. Assume the formula holds for $n-1$. Then

$$\begin{aligned} 1^3+2^3+3^3+\ldots+(n-1)^3+n^3 &= \frac{n^2(n-1)^2}{4}+n^3 \\ &= \left(\frac{n(n+1)}{2}\right)^2 \\ &= \frac{n^2(n+1)^2}{4}. \end{aligned}$$

The last two lines follow from the work done in Question 6. By the principle of induction, $1^3+2^3+3^3+\ +n^3 = \frac{n^2(n+1)^2}{4}$

6. [5 marks] Consider the open sentence $P(n) : 9 + 13 + \ldots + (4n + 5) = \frac{4n^2+14n+1}{2}$, where $n \in \mathbb{N}$.

   a) [3 marks] Verify the implication $P(k) \Rightarrow P(k + 1)$ for an arbitrary positive integer k.

   b) [2 marks] Is $\forall n \in \mathbb{N}$, $P(n)$ true?

Solution:

a) Assume that $P(k)$ holds. To see $P(k + 1)$ holds we simply check that

$$\begin{aligned} 9 + 13 + \ldots + (4k + 5) + (4k + 9) &= \frac{4k^2 + 14k + 1}{2} + (4k + 9) \\ &= \frac{4k^2 + 14k + 1 + 8k + 18}{2} \\ &= \frac{4k^2 + 8k + 4 + 14k + 14}{2} \\ &= \frac{4(k + 1)^2 + 14(k + 1)}{2}. \end{aligned}$$

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

b) No. Checking the base case, $P(1) = 19/2 \neq 9$. Since the base case does not hold, there is no reason to think that $P(k)$ is true for any $k \in \mathbb{N}$.

7. [9 marks] Consider the sequence F_1, F_2, F_3, ... , where $F_1 = 1$, $F_2 = 1$, and $F_k = F_{k-2} + F_{k-1}$. The terms of this sequence are called Fibonacci numbers.

   a) [0 marks] What are the first 5 Fibonacci numbers?

   b) [0 marks] For all $n \in \mathbb{N}$, prove that $2|F_n$ if and only if $3|n$.

   c) [3 marks] For all $n \in \mathbb{N}$, prove that $F_1 + F_2 + \ldots + F_n = F_{n+2} - 1$.

   d) [6 marks] For every $n \in \mathbb{N}$, let T_n be the number of ways to break n into a sum of a sequence of 1's and 2's. For example, here are the possibilities listed for $n = 3$.

   $$3 = 2 + 1 \qquad 3 = 1 + 2 \qquad 3 = 1 + 1 + 1$$

   Prove that $\forall n \in \mathbb{N}$, $T_n = F_{n+1}$.

Solution:

a) The first 5 Fibonacci numbers are $\{1, 1, 2, 3, 5\}$.

b) We need to use the principle of strong induction. First, lets check that the statement holds for F_1 and F_2. This is clear, since $3 \nmid 1$ and $3 \nmid 2$, and indeed $F_1 = F_2 = 1$ are not even.

Assume that the statement holds for all F_k up to n. We need to show that $2|F_n$ if and only if $3|n$, ans so we must show both that $2|F_n$ implies $3|n$ and that $3|n$ implies $2|F_n$. To prove that $3|n$ implies $2|F_n$ we observe that if $3 \mid n$, then $3 \nmid n-1$ and $3 \nmid n-2$, and so since the statement holds for all $k > n$, F_{n-1} and F_{n-2} are both odd. This means there exists integers j and ℓ such that $F_{n-1} = 2j+1$ and $F_{n-2} = 2\ell + 1$. But then

$$F_n = F_{n-1} + F_{n-2} = 2(j + \ell + 1)\,,$$

and so $2 \mid F_n$. Therefore $3|n$ implies $2|F_n$.

To prove that $2|F_n$ implies $3|n$, we will check the contrapositive, that is that if $3 \nmid n$ then $2 \nmid F_n$. If $3 \nmid n$, than 3 must divide exactly one of $n-1$ or $n-2$. Without loss of generality assume that $3 \mid n-1$. There exist integers j and ℓ such that $F_{n-1} = 2j$ and $F_{n-2} = 2\ell + 1$, so

$$F_n = F_{n-1} + F_{n-2} = 2(j + \ell) + 1\,.$$

It is clear that the proof goes through the same way if $3 \mid n-2$.

We have shown that if $2|F_k$ if and only if $3|k$ for all $k < n$, than it also holds for n. By the principle of strong induction the statement holds for all F_n, for $n \geq 1$.

c) We will proceed by induction. First, $F_1 = 1 = 2 - 1 = F_3 - 1$, so the base case of $n = 1$ holds. Now, assume that $F_1 + F_2 + \ldots + F_k = F_{k+2} - 1$ holds for all $k < n$. Then in particular if holds for $k = n - 1$ so

$$F_1 + F_2 + \ldots + F_{n-1} + F_n = F_{n+1} - 1 + F_n = F_{n+2} - 1\,.$$

By the principle of induction, $F_1 + F_2 + \ldots + F_n = F_{n+2} - 1$ holds for all naturals n.

d) Proof by strong induction. Base Case: For $n = 1$ we have $T_1 = 1 = F_2$

Inductive Step: Assume for some natural n, we have $T_k = F_{k+1}$ for all naturals $k \leq n$, we show that $T_{n+1} = F_{n+2}$. A natural $n+1 = 1+(n)$ and $n+1 = 2+(n-1)$, so the number of ways to break $n+1$ into a sum of a sequence of 1's and 2's (this sum either starts with 1 or with 2) is equal to the number of ways one can break n into a sum of a sequence of 1's and 2's plus the number of ways one can break $n-1$ into a sum of a sequence of 1's and 2's. So $T_{n+1} = T_n + T_{n-1} = F_{n+1} + F_n = F_{n+1}$.

8. 8 marks Prove that for every positive integer n, there exists an integer x_n such that $x_n^2 \equiv 14 \pmod{5^n}$.

Solution: Proof by basic induction:

Base case: For $n = 1$ let $X = 2$ then $X^2 \equiv 14 \pmod{5}$.

Inductive step: Assume for some natural n there exists an integer Y such that $Y^2 \equiv 14 \pmod{5^n}$ we show that there exists an integer X such that $X^2 \equiv 14 \pmod{5^{n+1}}$. If $X^2 \equiv 14 \pmod{5^{n+1}}$ then $X^2 \equiv 14 \pmod{5^n}$ so $X^2 \equiv Y^2 \pmod{5^n}$. Therefore $5^n | (X^2 - Y^2)$ or $5^n | (X - Y)(X + Y)$. Since $X^2 \equiv 14 \pmod{5}$ and $Y^2 \equiv 14 \pmod{5}$. We have $5 \nmid X$ and $5 \nmid Y$ so $5 \nmid X - Y$ or $5 \nmid X + Y$ otherwise 5 divides their sum and difference. So $5^n | (X - Y)$ or $5^n | (X + Y)$. So $X = 5^n k + Y$ notice that Y and $-Y$ have the same square and k is an integer, we can only continue with this case and drop the case $X = 5^n k - Y$.

Since $X^2 \equiv 14 \pmod{5^{n+1}}$ we get $5^{n+1} | (5^{2n}k^2 + Y^2 + 2kY5^n - 14)$ or $5^{n+1} | (Y^2 - 14 + 2kY5^n)$ or $5 | (r + 2kY)$ where $r = (Y^2 - 14)/5^n$ is an integer. $5 | (r + 2kY)$ has an integer solution for k, as equation $(2Y)k - 5l = r$ has integer solutions for k and l since $2Y$ and 5 are relatively prime.

Solution: We proceed by induction on n.

- Base Case: $n = 1$. You can take any integer x_1 such that either $x_1 \equiv 2 \pmod{5}$ or $x_1 \equiv 3 \pmod{5}$.
- Inductive Step: Suppose that x_n is an integer such that $x_n^2 \equiv 14 \pmod{5^n}$. Now consider the square of the integer $x_n + k \cdot 5^n$, where k can be any integer.

$$(x_n + k \cdot 5^n)^2 = x_n^2 + 2kx_n \cdot 5^n + 5^{2n} \equiv (x_n^2 + 2kx_n \cdot 5^n) \pmod{5^{n+1}}$$

  So for the five values $k = 0, 1, 2, 3, 4$, this square takes on different values modulo 5^{n+1}, because x_n is not divisible by 5. However, for each of these values of k, it is congruent to $14 \pmod{5^n}$. Therefore, for the values $k = 0, 1, 2, 3, 4$, this square must take on the five values $14, 14 + 5^n, 14 + 2 \cdot 5^n, 14 + 3 \cdot 5^n, 14 + 4 \cdot 5^n$ in some order. Hence, there exists a $k \in \{0, 1, 2, 3, 4\}$ such that $(x_n + k \cdot 5^n)^2 \equiv 14 \pmod{5^{n+1}}$.

Comment: Many students had trouble with arriving at this idea - here's the best explanation I can give of my thought process in constructing this solution. In order to make the induction work, you have to figure out how to construct x_{n+1} assuming that you already have x_n. My first thought looking at the condition that $x_n^2 \equiv 14 \pmod{5^n}$ is,

Suppose that I already had the numbers x_n, for all n. How must they be related to each other?

Trying to get a feel for how the numbers would *have* to be related will give me a clue as to how I can use x_n to product the number x_{n+1}. My observation is that $x_n^2 \equiv x_{n+1}^2$

(mod 5^n), and so it probably makes sense to try to pick an x_{n+1} such that $x_{n+1} \equiv x_n \pmod{5^n}$. From there, the solution falls out easily.

Lastly, it is a good strategy to try your hand at computing these for some small values of n ($n = 1, 2, 3$) before trying to write out the general proof! Start concrete, and start small, then look for patterns.

Note: an interesting thing about this fact is the following. There exist, for every n, an integer x_n such that $x_n^2 \equiv 14 \pmod{5^n}$. Moreover, each successive x_n can be chosen as a 'lift' of the previous one, in the sense that $x_{n+1} \equiv x_n \pmod{5^n}$. However, it is *not* true that there is an integer x such that $x^2 = 14$. This means that there is a difference between modular arithmetic mod 5^n as $n \to \infty$, versus arithmetic in the ordinary integers! (Modular arithmetic mod p^n as $n \to \infty$ is known as *p-adic arithmetic*, where p can be any prime.)