MATH 3050 Handout about Fermat's Theorem and Epp's Exercise 4.7#31

Epp's exercise 4.7#31 is a mess, but I would like you to work on it because (a) Fermat's Theorem is one of the most famous theorems in math, and anybody who has had an introduction to number theory ought to at least understand the statement of the theorem and (b) some of the concepts that you have studied already this quarter can be used to clarify the statement of the theorem and to understand a strategy for proving it.

Understanding the statement of Fermat's Theorem

First, understand an underlying question: For which positive integers n can one find positive integers x, y, and z that will make the equation $x^n + y^n = z^n$ true? We can organize our answers to the question in a table.

n	equation	example of a solution	x, y, z that work
1	$x^1 + y^1 = z^1$	$5^1 + 2^1 = 7^1$	$x = 5, y = 2, z = 7$
2	$x^2 + y^2 = z^2$	$5^2 + 12^2 = 13^2$	$x = 5, y = 12, z = 13$
3	$x^3 + y^3 = z^3$	?	?
4	$x^4 + y^4 = z^4$	?	?
5	$x^5 + y^5 = z^5$	?	?
$\vdots$	$\vdots$	$\vdots$	$\vdots$

I am unable to find any solutions for $n = 3,4,5 \cdots$. The question is, are there really no solutions, or are there solutions that I just have not been able to find? Fermat's theorem is a statement that answers the question:

Fermat's Theorem: For all integers $n > 2$, for all positive integers x, y, z, $x^n + y^n \neq z^n$.

Let's express this in symbols. For that, it helps to define the set $A = \{k \in \mathbb{Z} \text{ such that } k > 2\}$. With this definition of the set A, we can write Fermat's Theorem in symbols:

Fermat's Theorem: $\forall n \in A, \forall x,y,z \in \mathbb{Z}^+, x^n + y^n \neq z^n$.

We could could call this statement S. Notice that this is a statement about the set A. It will be useful to make similar statements about other sets, though, so let's use the symbol $S(A)$, to indicate that it is a statement about set A.

To reiterate, $S(A)$ is the statement $\forall n \in A, \forall x,y,z \in \mathbb{Z}^+, x^n + y^n \neq z^n$, which is the statement of Fermat's Theorem.

Strategy for Proving Fermat's Theorem

Define the following sets
- Let $B = \{k \in \mathbb{Z} \text{ such that } k > 2 \text{ and } k \text{ is prime}\}$
- Let $C = \{k \in \mathbb{Z} \text{ such that } k > 2 \text{ and } k \text{ is not a power of 2}\}$
- Let $D = \{4\}$
- Let $E = \{k \in \mathbb{Z} \text{ such that } k > 4 \text{ and } k \text{ is a power of 2}\}$

With these sets, we can build the following statements:
- $S(B)$ is the statement $\forall\ n \in B, \forall\ x,y,z \in \mathbb{Z}^+, x^n + y^n \neq z^n$. (In words, "there are no integer solutions to the equation $x^n + y^n = z^n$ when n is a prime number greater than 2.")
- $S(C)$ is the statement $\forall\ n \in C, \forall\ x,y,z \in \mathbb{Z}^+, x^n + y^n \neq z^n$. (In words, "there are no integer solutions to the equation $x^n + y^n = z^n$ when n is an integer greater than 2 that is not a power of 2.")
- $S(D)$ is the statement $\forall\ n \in D, \forall\ x,y,z \in \mathbb{Z}^+, x^n + y^n \neq z^n$. (In words, "there are no integer solutions to the equation $x^4 + y^4 = z^4$.")
- $S(E)$ is the statement $\forall\ n \in E, \forall\ x,y,z \in \mathbb{Z}^+, x^n + y^n \neq z^n$. (In words, "there are no integer solutions to the equation $x^n + y^n = z^n$ when n is an integer greater than 4 that is a power of 2.")

Observe that set A is the union of sets C, D, and E. So, if $S(C)$ is true and $S(D)$ is true and $S(E)$ is true, then $S(A)$ will be true as well. That is, $S(C) \land S(D) \land S(E) \rightarrow S(A)$. Here is an outline for a proof of Fermat's theorem that uses the statements introduced above.

statement	justification
1: $S(B)$	??
2: $S(B) \rightarrow S(C)$	you are supposed to prove this in problem 4.7#31a
3: $S(C)$	by 1, 2, and modus ponens
4: $S(D)$	Fermat proved this statement
5: $S(D) \rightarrow S(E)$	you are supposed to prove this in problem 4.7#31b
6: $S(E)$	by 4,5, and modus ponens
7: $S(C) \land S(D) \land S(E)$	3,4,5, and conjunction
8: $S(C) \land S(D) \land S(E) \rightarrow S(A)$	because set A is the union of sets C, D, and E.
9: $S(A)$	by 7, 8, and modus ponens

Statement 1 is not justified. Why not? Well, at the time of the writing of this book, $S(B)$ had not been proven. In a sense, this whole proof of Fermat's theorem is just waiting for somebody to prove statement $S(B)$. Once somebody does that, the proof outlined above can be used to prove Fermat's theorem. In a sense, the proof of Fermat's theorem has been *reduced to* a proof of statement $S(B)$.

In the years since the writing of this book, Fermat's theorem *has* been proven. I don't know if the outline of the proof follows the outline above. But the outline above gives a little of the flavor of how research in mathematics progresses: It can be difficult to identify and clearly articulate an important question, to put it into a statement to be proven. Once the statement has been identified, it might not be possible to prove it right away. It is common for one researcher to identify an important statement to be proven, and for another researcher to later find an outline for a proof structure, fill in some of the steps, but be unable to fill in some others. The completion of the proof can sit for years (in the case of Fermat's theorem, centuries!) before somebody can fill in the missing steps.