Fermat's Last Theorem

Fermat's Last Theorem (17th century). For any integer $n > 2$ there are no positive integers a, b, c satisfying $a^n + b^n = c^n$. I've found a remarkable proof of this fact, but there is not enough space in the margin to write it.

1. **Discussion.** Is Fermat's Last Theorem rather Fermat's Lost Theorem or Fermat's Last Conjecture? Consider the following assertions:

   (a) Fermat used to state results to other mathematicians without revealing their proof.

   (b) A theorem needs a complete proof to be called theorem.

   (c) Maybe Fermat had a proof, but it was flawed.

   (d) Fermat tested small numbers and found no solutions.

   (e) No proof of Fermat's Last Theorem has yet been found that only uses mathematical methods known in the 17th century.

   (f) A mathematical guess is not a conjecture, a conjecture needs supporting evidence.

2. **Easy proof.** Prove that there are infinitely many Pythagorean triples. Hint: Do you know one Pythagorean triple?

3. **Proof.** Explain the relation $30^2 + 30 + 31 = 31^2$ and generalize it to the squares of any two consecutive integers. Then prove that there are many Pythagorean triples (a, b, c) where a is odd and $c = b + 1$. Also show that such Pythagorean triples are *primitive* (i.e. a, b, c have no common factor).

4. **Corollary.** Can a Pythagorean triple consist of numbers that are all squares? How does this assertion relate to Fermat's Last Theorem?

5. **Example.** Find a unit fraction that is the sum of two unit fractions. (A unit fraction is a fraction of the form $1/m$ for some positive integer m).

6. **Proof needs statement.** What does the following reasoning prove for $n > 2$ and a, b, c positive integers?

$$\frac{1}{a^n} + \frac{1}{b^n} = \frac{1}{c^n}$$

$$\frac{a^n + b^n}{(ab)^n} = \frac{1}{c^n} \qquad \frac{(ab)^n}{a^n + b^n} = \frac{c^n}{1}$$

$$(ab)^n = (ac)^n + (bc)^n$$

7. **Example needs statement.** Consider the relation

$$1/225 + 1/400 = 1/144\,.$$

What does this example show?

8. **Proof.** Prove that in every primitive Pythagorean triple (a, b, c) there is precisely one even number, and this is not c. General method: Fix some integer $m \geqslant 2$. If you have a polynomial equality with integer values for the variables, then the remainder after division by m of the left-hand-side equals the one of the right-hand-side. To compute these remainders, you may replace the given integers by their remainder after division by m. This method for $m = 2$ amounts to considering whether the numbers are even or odd.

9. **Guided proof.** A triple of positive integers (a, b, c) is a primitive Pythagorean triple if and only if there exist two coprime positive integers x, y such that $x > y$, $x + y$ is odd, and (supposing w.l.o.g. that a is even)

$$a = 2xy \qquad b = x^2 - y^2 \qquad c = x^2 + y^2\,.$$

Hint for the 'only if' direction: Set $\frac{x}{y} := \frac{(c+b)}{a} = \frac{a}{(c-b)}$ in lowest terms and solve

$$\frac{c}{a} + \frac{b}{a} = \frac{x}{y}, \qquad \frac{c}{a} - \frac{b}{a} = \frac{y}{x}$$

$$\frac{c}{a} = \frac{x^2 + y^2}{2xy}, \qquad \frac{b}{a} = \frac{x^2 - y^2}{2xy}\,.$$

Can you complete this sketch of proof with the missing details (pay attention to the last step)? Can you prove the 'if' direction?

10. **Infinite descent.** Consider an equation with finitely many variables, and its solutions consisting of tuples of positive integers (possibly, with some additional properties). Given any solution, there are not infinitely many solutions that are smaller than it. So, to prove that there is no solution at all, it suffices to show that, given any solution (with the additional properties), it is possible to construct a strictly smaller one (with the additional properties).

    With this method, we prove Fermat's Last Theorem for $n = 4$. More generally, we prove that in a Pythagorean triple (a, b, c) it is not possible that the following property holds: at least two among a, b, c are "$\square$ or $2\square$" (here $\square$ stands for a square).

    (a) If (a, b, c) has the property and is not primitive, then rescale it to be primitive and prove that this strictly smaller triple still has the property.

    (b) Now suppose that (a, b, c) has the property and it is primitive. W.l.o.g. suppose that a is even, hence b,c are odd. So write

    $$a = 2xy \qquad b = x^2 - y^2 \qquad c = x^2 + y^2$$

    (x, y are coprime positive integers).

    (c) If a is "$\square$ or $2\square$", then prove that the same holds for x and y, and morover $b = \square$ or $c = \square$. Then show that one of the following triples (a', b', c') is as requested:

    $$a' = x \qquad b' = y \qquad c' = \sqrt{c}$$
    $$a' = y \qquad b' = \sqrt{b} \qquad c' = x\,.$$

    (d) Else, prove that we must have $b = \square$ and $c = \square$ and the following triple (a', b', c') is as requested:

    $$a' = \sqrt{bc} \qquad b' = y^2 \qquad c' = x^2\,.$$

11. **Corollary.** Prove that Fermat's equation for $n > 2$ does not have solutions (a, b, c) where a, b, c are non-zero integers. Hint: Write

    $$a^n + b^n - c^n = 0$$

and study the sign of the three summands on the left-hand-side. Is there a shortcut if n is even?

12. **Corollary.** Prove that Fermat's equation for $n > 2$ does not have solutions (a, b, c) where a, b, c are positive rational numbers. (Remark: Similarly to the previous exercise you may deduce that they cannot be non-zero rational numbers.)

13. **Piece of proof.** Show that it is enough to prove Fermat's Last Theorem for $n = 4$ and for any odd prime n. How can you deduce the general case from these special cases?

14. **Example.** Consider the example

$$2.682.440^4 + 15.365.639^4 + 18.796.760^4 = 20.615.673^4 .$$

What does this tell us about possible generalizations of Fermat's Last Theorem?

15. **Strategy.** Put the following assertions in logical order to make a proof of Fermat's Last Theorem.

    (a) Ribet proved that Frey's curve is not modular.

    (b) The Taniyama-Shimura Conjecture says that every elliptic curve (defined over $\mathbb{Q}$) is modular, i.e. it corresponds to a modular form.

    (c) Frey proved that from a solution to Fermat's equation it is possible to construct some strange elliptic curve (defined over $\mathbb{Q}$) which is semistable.

    (d) Breuil, Conrad, Diamond, and Taylor proved the Taniyama-Shimura Conjecture.

    (e) Wiles proved the Taniyama-Shimura Conjecture for semistable elliptic curves.

16. **Computer.** Write a small program to list all Pythagorean triples (respecively, all Pythagorean triples) made with numbers up to 100.

17. **Computer.** Write a small program to find solutions for $\frac{1}{a^2} + \frac{1}{b^2} = \frac{1}{c^2}$.

18. **Latin.** Translate Fermat's original text: Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

19. **Follow up.** Read about the tree of primitive Pythagorean triples. Try to understand the main properties and write them up in your own words.

20. **Mathematical families.** The PhD is a period of guided research after the university Master degree. The supervisor of a PhD student in mathematics is called the mathematical parent of the student. Find out in the website *Mathematics Geneaology Project* how many mathematical descendants Wiles has today.