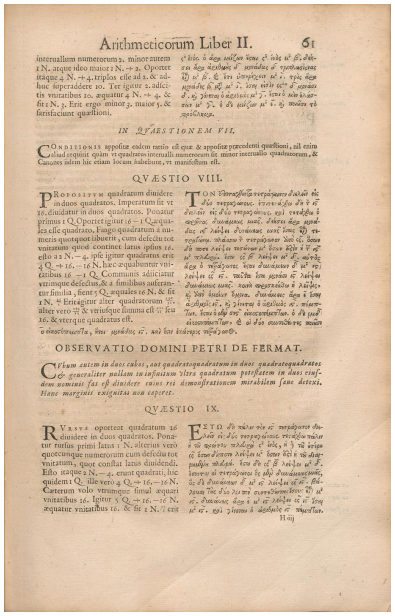
5 Topic: Fermat's last theorem



Arithmeticorum Liber II. 61

IN QVÆSTIONEM VII.

QVÆSTIO VIII.

OBSERVATIO DOMINI PETRI DE FERMAT.

QVÆSTIO IX.

Figure 1: Pierre de Fermat and the page of Diophantus's Arithmetica with his commentary, which is now called "Last theorem."

Theorem 5.1 (Fermat's last theorem)**.** *For any $n, x, y, z \in \mathbf{N}$ and $n > 2$ the equation*

$$x^n + y^n = z^n$$

has no solutions.

The goal of this project is to prove this theorem in the case $n = 4$ by using the *method of infinite descent*. Here is the idea of this method:

> *In order to prove that an equation has no solution in natural numbers, one shows that if this equation had such a solution then it must satisfy some other natural numbers, moreover, significantly smaller.*

In the proof below you will need to rely on the previous project and on its two main results, which I repeat here for convenience (you will need to use twice each of these statements in your proof):

Theorem 5.2 (Theorem 4.1 from Project 4)**.** *Let (a, b, c) be a primitive Pythagorean triple. Then c is odd and exactly one of a and b is even. Assume that b is even. Then there exist relatively prime integers $m < n$, one even and one odd, such that*

$$a = n^2 - m^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

Lemma 5.3 (Lemma 4.2 from Project 4)**.** *If $xy = z^2$, where x and y are relatively prime integers, then both x and y are squares.*

♢ **5.1** (Scratch work and hints)**.**
The goal is to show that $x^4 + y^4 = z^4$ has no solutions in natural numbers.

1. Clearly understand what proof technique is used in the method of infinite descent and what the mathematical justification of the method of infinite descent is.

2. Understand that if you prove that
$$x^4 + y^4 = z^2 \tag{5.1}$$
has no positive integer solutions then the required goal will be achieved (you will need to explain it in your proof).

3. Assume that there is a positive integer solution x, y, z to equation (5.1) and understand that one can assume that x, y, z are pairwise relatively prime.

4. Since (5.1) can be written as $(x^2)^2 + (y^2)^2 = z^2$ and x^2, y^2, z are relatively prime (do you see why?) then by Theorem 5.2 one can write
$$x^2 = 2mn, \tag{5.2}$$
$$y^2 = m^2 - n^2, \tag{5.3}$$
$$z = m^2 + n^2. \tag{5.4}$$
Prove that n must be even in this case (note that this does not follow from Theorem 5.2), i.e., $n = 2n'$ for some natural n'.

5. Analyzing expression in (5.2)-(5.4) and using Lemma 5.3 conclude that m and n' must be squares, i.e., $m = \mu^2, n = 2\eta^2$, hence, from (5.3),
$$y^2 + (2\eta^2)^2 = (\mu^2)^2.$$

6. Argue that you can apply Theorem 5.2 to the triple $y, 2\eta^2, \mu^2$ and therefore...

7. At this point I stop giving precise hints how to proceed. Your task first is to elaborate on the previous hint, write down the corresponding formulas (do not use the same letters for your variables as before!), realize that you can apply Lemma 5.3 one more time (again, do not use the same letters as before, this part also will test you how you choose your notation), and finally, putting together available facts, find a triple of positive integers x', y', z' such that $x'^4 + y'^4 = z'^2$ and $z' < z$, which would conclude the proof by the method of infinite descent.

♢ **5.2.** Put everything together in one coherent and detailed proof (for reference you can include the statements of Theorem 5.2 and Lemma 5.3, but no proof of these facts is needed). Make sure you include arguments for all the steps in your proof (e.g., if you apply Theorem 5.2 to some a, b, c you must first make sure that a, b, c are pairwise relatively prime, etc).