Section 17. Infinite Descent and Fermat's Conjecture

Note. In this section, we briefly tell the story of "Fermat's Last Theorem." This result claims that there are no positive integer solutions to the equation $x^n+y^n = z^n$ for $n \geq 3$. We prove that the equation $x^4 + y^4 = z^2$ has no integer solutions; see Theorem 17.1. This, in turn, implies that the equation $x^4+y^4 = z^4$ has no solutions and so we give a proof of Fermat's Last Theorem for the case $n = 4$. In the process, we illustrate Fermat's method of infinite descent. We take a short excursion away from the text book and consider equations of the form $w^3 + x^3 + y^3 = z^3$.

Note. In Section 16. Pythagorean Triangles we found all solutions (in integers) of the equation $x^2 + y^2 = z^2$ (see Theorem 16.1). Since, by the Pythagorean Theorem, we see that integer solutions of this equation allow us to construct right triangles (and to use these right triangles in connection with certain trigonometric functions), then we see a practical reason to search for such solutions. This has a historical foundation; see my notes for History of Mathematics (MATH 3040), especially the material Egyptian geometry (which is, at this date [spring 2022], still in preparation). Dudley comments (page 135) that: "...it would be natural to try the same ideas on an equation of one higher degree, $x^3 + y^3 = z^3$." Your humble instructor interprets this as one of those weird instances of the use of the term "natural" in a rather unnatural setting! None-the-less, this is the beginning of a mathematically famous problem. We tell the back story in more detail in the supplement Fermat's "Last" Theorem to this section.

Definition. An integer solution to $x^n + y^n = z^n$ where one of the variables is 0 is a *trivial solution*.

Note. Around 1630, Fermat famously wrote in the margin of his copy of Diophantus' *Arithmetica* (for historical details on Diophantus and *Arithmetica*, see the online notes for Section 3. Linear Diophantine Equations) that there are no non-trivial solutions for $x^n + y^n = z^n$ when $n \geq 2$, but he failed to provide a proof (as was often the case with his claims). He wrote:

> It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.

See the MacTutor History of Mathematics Archive's page on Fermat's Last Theorem and the Wikipedia page on Fermat's Last Theorem. The statement was discovered after Fermat's death in 1665 by his son, Clément-Samuel Fermat, who included his father's marginal comment in a new edition 1670 of *Arithmetica*. Fermat had made a number of unproved claims such as this. All eventually fell in due time, except for this claim, which became known as "Fermat's Last Theorem" (though it was not prove for three centuries, and should have been known at the time as "Fermat's Conjecture"). The Last Theorem was proved, after about a decade of dedicated work, in 1994 by Andrew Wiles (April 11, 1953–present) of the University of Oxford and Princeton University, using techniques involving elliptic curves and the Modularity Theorem. His proof appears in two articles in *Annals of Mathematics*, **141**(3) (1995) as:

Wiles, Andrew. "Modular Elliptic Curves and Fermat's Last Theorem." *Annals of Mathematics*, **141**(3), 443–551 (1995).

Taylor, Richard, and Andrew Wiles. "Ring-Theoretic Properties of Certain Hecke Algebras." *Annals of Mathematics*, **141**(3), 553–572 (1995).

You an see previews of these articles through JSTOR, but you may have to enter your university username and password to read the entire article.

Note. The rest of this section of the book is devoted to proving the following.

Theorem 17.1. There are no nontrivial solutions of $x^4 + y^4 = z^2$.

Note. The technique of proof used in Theorem 17.1 allows us to produce a strictly smaller nontrivial value of z^2 from a given solution, and to repeat this process producing progressively smaller values of z^2. This is the reason the technique is called Fermat's method of infinite descent.

Note. When your less-than-humble instructor was taking Number Theory (MH 330) at Auburn University at Montgomery in fall quarter 1982, he noticed that $3^3 + 4^3 + 5^3 = 6^3$. Having access to reliable computing equipment while working at the Alabama Department of Environmental Management—Air Division, he found hundreds primitive of quadruples (A, B, C, D) that satisfy the equation $A^3 + B^3 + C^3 = D^3$. Using terminology similar to that of "Pythagorean triples" (and pushing

aside any humility), these became "internally" known as *Gardner quadruples*! By Fermat's Last Theorem (or "Wiles Theorem"), we know that $x^3 + y^3 = z^3$ has no nontrivial solution. So a "natural" equation to consider is $w^3 + x^3 + y^3 = z^3$.

Note. It turns out that Leonhard Euler (April 15, 1707–September 18, 1783) found all *rational* solutions (A, B, C, D) in his "Solutio generalis quorundam problematum Diophanteorum, quae vulgo nonnisi solutiones speciales admittere videntur" (1761), Euler Archive—All Works 255. You can download a PDF of this (in Latin) from the Scholarly Commons' Euler Archives (accessed 3/19/2022); see his Section 16 on page 165. Euler's solution is also presented in G. H. Hardy and E. M. Wright's *An Introduction to the Theory of Numbers*, Oxford University Press, London. There are several editions of this in print (starting in 1938) and you may find a version online in PDF. Euler's solution is given in the section "The Equation $x^3 + y^3 + z^3 = t^3$" of the chapter "Some Diophantine Equations." It uses five parameters to produce the solution (A, B, C, D), sometimes using a non-integer rational as a parameter to give an integer solution. A cleaner solution was given by Ajai Choudhry in "On Equal Sums of Cubes," *Rocky Mountain Journal of Mathematics*, **28**(4), 1251–1257 (1998). A copy of his work is online at the Project Euclid page (accessed 3/19/2022). Choudhry considers three types of Diophantine equations: (1) $w^3 + x^3 + y^3 + z^3 = 0$, (2) $w^3 + x^3 = y^3 + z^3$, and (3) $w^3 + x^3 + y^3 = z^3$. If we consider negative values of the variables as well, then these three equations are equivalent. His result concerning $w^3 + x^3 + y^3 = z^3$ is:

Choudhry's Theorem. The complete solution in positive integers of the equation $w^3 + x^3 + y^3 = z^3$, where the greatest common divisor $(w, x, y, z) = 1$, is given by

$$\begin{aligned} dw &= c(-a^3 - b^3 + c^3) \\ dx &= -a^4 + 2a^3b - 3a^2b^2 + 2ab^3 - b^4 + (a+b)c^3 \\ dy &= a^4 - 2a^3b + 3a^2b^2 - 2ab^3 + b^4 + (2a-b)c^3 \\ dz &= c(a^3 - (a-b)^3 + c^3) \end{aligned}$$

where a, b, c are positive integers such that $a > b$ and $c > (a^3 + b^3)^{1/3}$, and $d > 0$ is taken so that $(w, x, y, z) = 1$.

Maybe a better name for a quadruple (A, B, C, D) such that $A^3 + B^3 + C^3 = D^3$ is a *Euler quadruple* or a *Choudhry quadruple*! A related result appears in James Harper's "Ramanujan, Quadratic Forms, and the Sum of Three Cubes," *Mathematics Magazine*, **86**(4), 275–279 (2013). In a simple approach "using only basic precalculus tools," he finds solutions where each of A, B, C, and D are given by quadratic forms; that is, given in the form $au^2 + buv + cv^2$. His paper is available on the JSTOR website (accessed 3/19/2022).

Note. As a final comment, we mention that the equation $w^4 + x^4 + y^4 = z^4$ was solved in general in N. Elkies' "On $A^4 + B^4 + C^4 = D^4$," *Mathematics of Computation*, **51**, 825-835 (1988).

Revised: 3/19/2022