Section 2: n=3

The $n = 3$ case of Fermat's Last Theorem states that no cube is the sum of two other cubes. Sums of two cubes have been studied throughout the years and perhaps 1729 is the most famous such number. There is an amusing anecdote regarding famous number theorists and this surprisingly remarkable number.

In the early 20th century, British mathematician G. H. Hardy was a leading number theorist. In 1913, he received a letter from amateur mathematician Srinvasa Ramanajuan of India relating his mathematical achievements and asking for help. Despite having no formal mathematical training, Ramanjuan's results were impressive. Within a year Hardy brought him to London and the two began a prosperous if short-lived collaboration. Ramanajuan was very adept at mental calculations and a brilliant man, but he was often sick and died in India at the age of 32. During one of his hospital stays in London, Hardy visited him and in making small talk he remarked that he had arrived in a taxi number 1729, which he considered a rather dull number. Ramanajuan responded that 1729 was not dull at all, for it is the smallest number that can be expressed as the sum of two cubes in two distinct ways:

$$1729 = 1^3 + 12^3 = 9^3 + 10^3 .$$

But back to Fermat's Last Theorem. The case $n = 3$ is noteworthy because it is one of two cases that Fermat's is believed to have proven himself. We saw in the last section that the one proof attributable to Fermat essentially proves the $n = 4$ case. In letters to his friends, Fermat also claims to have proven the $n = 3$ case and challenges them likewise. (These letters came after his marginal note was left in *Arithmetica*. Which begs the question: if he already claimed to have proven $x^n + y^n = z^n$ had no solutions, why would he prove particular cases of this and "brag" about them? Perhaps he already discovered his general proof had an error?) The first published proof of $x^3 + y^3 = z^3$ came in 1770 and is due to Leonhard Euler. Interestingly enough, Euler's proof contains an error, but the method used to fix it was known to Euler, so mathematicians still give him credit. And the error turned out to be quite important as we will soon see. This proof is a bit involved, but while there are many steps, and many variables, each step follows from previous ones and the logic is not very complicated.

Theorem 2.2.1 The equation $x^3 + y^3 = z^3$ has no nontrivial solutions.

> **Proof**: Suppose we have a nontrivial solution (x, y, z). So $x^3 + y^3 = z^3$ and $xyz \neq 0$ (in other words, all values are nonzero). This proof will utilize infinite descent, so we will find a smaller solution. First, we can assume that (x, y, z) are pairwise relatively prime. (If there was a common factor between two of the variables, it would necessarily be a factor of the third and we could reduce the entire solution by that factor.) Clearly, exactly one of the three variables must be even. (WHY?) We will show that whichever variable

is even, we are able to find some relatively prime positive integers p and q (one even and one odd) such that $2p(p^2+3q^2)$ is a cube.

Case 1: Suppose z is even. Then x and y are both odd and hence $x+y$ and $x-y$ are both even. So there exist integers p and q such that

$$x+y=2p \text{ and } x-y=2q.$$

Solving for x and y, we have $x=p+q$ and $y=p-q$. Therefore, p and q must be relatively prime. (WHY?) We can also assume p and q are positive and exactly one is even. Note that $2p(p^2+3q^2)$ is a cube, in fact $2p(p^2+3q^2)=z^3$. (WHY?)

Exercise 2.2.2 Answer the three previous WHY?'s

Case 2: Suppose x or y is even. Once again, we can deduce that there exist relatively prime positive integers p and q (one even and one odd) such that $2p(p^2+3q^2)$ is a cube.

Exercise 2.2.3 Show Case 2. (Hint: Try and mimic Case 1, it's similar. Make sure you verify the underlined portions are true.)

Let's consider the two integers $2p, p^2+3q^2$. What is their greatest common divisor? From either previous case, we have two relatively prime integers p and q such that $2p(p^2+3q^2)$ is a cube. Let d be a prime common divisor of $2p$ and p^2+3q^2. Since one of p and q is even and the other is odd, d cannot be 2 (since p^2+3q^2 is odd). Suppose that $d>3$. Therefore, there exist m and n such that $2p=dm$ and $p^2+3q^2=dn$. Since 2 divides $2p$, it must divide dm. But since $d\neq 2$, 2 must divide m. So $m=2r$ (for some r) and hence $p=dr$. So

$$\begin{aligned} 3q^2 &= dn-p^2 \\ &= dn-(dr)^2 \\ &= d(n-dr^2) \end{aligned}$$

Since $d>3$, d obviously does not divide 3. So d must divide q. But that means that d divides both p and q, which is a contradiction. Therefore, $\gcd(2p, p^2+3q^2)$ is either 1 or 3.

Case A: Suppose $\gcd(2p, p^2+3q^2)=1$

Since $2p$ and p^2+3q^2 are relatively prime and their product is a cube, they must both be cubes individually. So there exist integers u and v such that $2p=u^3$ and $p^2+3q^2=v^3$. Let's focus on this second equation first. Clearly, v is odd. (WHY?) It can be shown that every odd factor of a number of the form p^2+3q^2 (with p and q relatively prime) must also be of the same form. So there exist integers a and b such that $v=a^2+3b^2$. From this, using a bit of algebra, we can deduce that $p=a^3-9ab^2$ and $q=3a^2b-3b^3$. So

$$u^3=2p=2(a^3-9ab^2)=2a(a-3b)(a+3b).$$

Those three factors $2a$, $a-3b$, and $a+3b$ are pairwise relatively prime again (WHY?) and equal to a cube. Therefore they are all cubes themselves:

$$2a=A^3,\ a-3b=B^3, \text{ and } a+3b=C^3.$$

But notice that

(a) $A^3=B^3+C^3$ (WHY?)
(b) (B,C,A) is a smaller solution to FLT than (x,y,z). (WHY?)

Exercise 2.2.4 You guessed it. Answer the four previous WHY?'s.

So in Case A, we found a smaller solution to FLT. By Fermat's method of infinite descent, if we applied the above argument to the new solution we could produce an infinite sequence of smaller solutions, clearly impossible. So there must not be one nontrivial solution. But this was only Case A ($\gcd(2p, p^2+3q^2)=1$). Now for Case B:

Case B: Suppose $\gcd(2p, p^2+3q^2)=3$

Recall that $2p(p^2+3q^2)$ is an even cube. So 4 must divide p. (WHY?) Since $\gcd(2p, p^2+3q^2)=3$, 3 divides $2p$, hence 3 divides p. Therefore there exists an integer w such that $p=3w$. Note that w and q are relatively prime (since p and q were).

Now $2p(p^2+3q^2)$ is a cube and

$$2p(p^2+3q^2)=2(3w)((3w)^2+3q^2)=6w(9w^2+3q^2)=18w(3w^2+q^2).$$

Since w and q are relatively prime, $18w, 3w^2 + q^2$ are relatively prime also and their product equals a cube. So each is a cube. Namely,

$$18w = s^3$$
$$3w^2 + q^2 = t^3$$

Here, we resort to a fact we used moments ago: since t is an odd factor of a number of the form $3w^2 + q^2$, it must be of the same form. So there exist numbers g and h such that $t = 3h^2 + g^2$. Some algebra produces:

$$q = g(g^2 - 9h^2) \text{ and } w = 3h(g^2 - h^2).$$

So we have,

$$s^3 = 54h(g-h)(g+h). \text{ (WHY?)}$$

Since these three factors (as before) are relatively prime and equal to a cube, they are all cubes. So there exist integers such that

$$54h = i^3$$
$$g - h = j^3$$
$$g + h = k^3$$

In fact, we can say more. There exists an integer l such that $2h = l^3$. (WHY?) Finally, $l^3 = k^3 - j^3$, (WHY?) which shows us that (l, j, k) is another (smaller) solution to FLT.

Exercise 2.2.5 Last time. Answer the four previous WHY?'s.

Again we were able to produce a smaller solution to FLT. By Fermat's method of infinite descent, there must not be one nontrivial solution. QED