An Equivalent Form in Fermat's Last Theorem

Youn-Sha Chan[1] & Linda Becerra[1]

[1] Department of Mathematics and Statistics, University of Houston-Downtown, Houston, Texas, USA

Correspondence: Youn-Sha Chan, Department of Mathematics and Statistics, University of Houston-Downtown, Houston, Texas, USA. E-mail: chany@uhd.edu

Received: August 28, 2022 Accepted: September 20, 2022 Online Published: September 30, 2022

doi:10.5539/jmr.v14n5p46 URL: https://doi.org/10.5539/jmr.v14n5p46

Abstract

An equivalent form to $a^n + b^n = c^n$ in Fermat's Last Theorem (FLT) is proposed and proved for any odd prime exponent n. Some specific cases, $n = 3, 5, 7, 11$, are provided to demonstrate the outcomes of the equivalent form. It is our hope that the equivalent form will lead to more insightful viewpoints of FLT.

Keywords: Fermat's Last Theorem, recursive relationship, modular congruence

1. Introduction

Fermat's Last Theorem (FLT) states that there are no positive integer solutions a, b, c to $a^n + b^n = c^n$ if $n \geq 3$. "This problem had been unsolved by mathematicians for 300 years. It looked so simple, and yet all the great mathematicians in history couldn't solve it. Here was a problem, that I, a 10 year old, could understand, and I knew from that moment that I would never let it go. I had to solve it." said by Andrew Wiles in 1965 [1]. Amazingly, Wiles remained steadfast in his goal, and thirty years later, at age 40, he stated that he had a proof. The proof, published in 1995, is over 100 pages long, and uses methods of modern mathematics that did not exist at the time of Fermat [1607-1665].

During those hundreds of years in which the quest for a proof was ongoing, numerous mathematicians came up with clever ideas and new mathematics in support of this endeavor. A nice summary of the major accomplishments made towards a proof of the FLT during this time is given in [2]. Any student who studies these past achievements will not only gain in their mathematical knowledge of many areas of mathematics, but will also learn of many related questions that remain unanswered.

Our goal in this paper is to follow up on one of the so called naive approaches [4] for a proof of FLT. We will present an identity equivalent to FLT that illuminates relationships between solutions a, b, and c, and the power n in FLT. Our hope is that students will learn some mathematics and enjoy this historical approach.

2. Some Factoring Results Related to FLT

As noted in [4], since

$$a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots - ab^{n-2} + b^{n-1})$$

for odd positive integers n, attention was given to results related to this factorization beginning with the earliest attempts at proofs of FLT. We now present two results of this type that will be utilized in later sections.

Proposition 1. *Assume n is an odd prime and there are positive integer solutions to $a^n + b^n = c^n$ with gcd(a, b, c)=1. Then $a + b$, $c - b$, and $c - a$ are relatively prime integers.*

Proof. Since

$$c^n = a^n + b^n = (a + b)\sum_{k=1}^{n} a^{n-k}(-b)^{k-1}$$

$$b^n = c^n - a^n = (c - a)\sum_{k=1}^{n} c^{n-k}a^{k-1}$$

$$a^n = c^n - b^n = (c - b)\sum_{k=1}^{n} c^{n-k}b^{k-1},$$

it follows that if there is a factor p of two of $a + b$, $c - b$ and $c - a$, then p would be a factor of two of a, b and c. This would contradict that a, b and c are relatively prime. □

Theorem 2. *Suppose n is an odd prime and $a+b$, $c-b$ and $c-a$ are relatively prime, then $n(a+b)(c-a)(c-b)$ is a factor of $(a+b-c)^n+c^n-a^n-b^n$ and we define*

$$R_n(a,b,c) = \frac{(a+b-c)^n - a^n - b^n + c^n}{n(a+b)(c-b)(c-a)}. \tag{1}$$

Proof. Let's first rewrite the numerator of $R_n(a,b,c)$.

$$\begin{aligned}(a+b-c)^n - (a^n+b^n) + c^n &= [(a+b)-c]^n - (a^n+b^n) + c^n \\ &= \sum_{k=0}^{n}\binom{n}{k}(a+b)^{n-k}(-c)^k - (a+b)\sum_{l=1}^{n} a^{n-l}(-b)^{l-1} + c^n \\ = (a+b)^n + \sum_{k=1}^{n-1}\binom{n}{k}(a+b)^{n-k}(-c)^k &+ (-c)^n - (a+b)\sum_{l=1}^{n} a^{n-l}(-b)^{l-1} + c^n \\ &= (a+b)^n + \sum_{k=1}^{n-1}\binom{n}{k}(a+b)^{n-k}(-c)^k - (a+b)\sum_{l=1}^{n} a^{n-l}(-b)^{l-1}\end{aligned}$$

Hence,

$$\begin{aligned}R_n(a,b,c) &= \frac{(a+b)^n + \sum_{k=1}^{n-1}\binom{n}{k}(a+b)^{n-k}(-c)^k - (a+b)\sum_{l=1}^{n} a^{n-l}(-b)^{l-1}}{n(a+b)(c-b)(c-a)} \\ &= \frac{\frac{1}{n}(a+b)^{n-1} + \sum_{k=1}^{n-1}\frac{\binom{n}{k}}{n}(a+b)^{n-k-1}(-c)^k - \frac{1}{n}\sum_{l=1}^{n} a^{n-l}(-b)^{l-1}}{(c-b)(c-a)} \\ &= \frac{\sum_{k=1}^{n-1}\frac{\binom{n}{k}}{n}(a+b)^{n-k-1}(-c)^k + \frac{1}{n}[(a+b)^{n-1} - \sum_{l=1}^{n} a^{n-l}(-b)^{l-1}]}{(c-b)(c-a)}\end{aligned}$$

Let

$$P(-c) = \sum_{k=1}^{n-1}\frac{\binom{n}{k}}{n}\sigma^{n-k-1}(-c)^k + \frac{1}{n}[\sigma^{n-1} - \sum_{l=1}^{n} a^{n-l}(-b)^{l-1}]$$

where $\sigma = (a+b)$. Then using long division to divide $P(-c)$ by

$$(c-a)(c-b) = [(-c)^2 + \sigma(-c) + ab]$$

we obtain that $R_n(a,b,c)$ is a polynomial in a, b and c of degree $(n-3)$ which we will write in the form

$$R_n(a,b,c) = \sum_{k=1}^{n-2} s_k(-c)^{n-2-k}, k = 1,2,3,\ldots,n-2 \tag{2}$$

where each coefficient s_k is a function of $a+b$ and ab. We have also used the fact [3] that if n is prime, then $\binom{n}{1}$, $\binom{n}{2}$, $\cdots$, $\binom{n}{n-1}$ are divisible by n. It is easier to define s_k as follows according to whether k is even or odd. Recall again that n is an odd prime.

- For k being odd with $k = 2m-1$,

$$s_k = s_{2m-1} = \sum_{\ell=1}^{m} t_{2m-1,\ell}(a+b)^{2m-2\ell}(ab)^{\ell-1}, \quad m = 1,2,3,\cdots,\frac{n-1}{2}. \tag{3}$$

- For k being even with $k = 2m$,

$$s_k = s_{2m} = \sum_{\ell=1}^{m} t_{2m,\ell}(a+b)^{2m-2\ell+1}(ab)^{\ell-1}, \quad m = 1,2,3,\cdots,\frac{n-3}{2}. \tag{4}$$

The last step is to describe each coefficient $t_{k,j}$ for $j = 1, 2, 3, \ldots, n-2,$ and $k = 1, 2, 3, \ldots, \lceil \frac{k}{2} \rceil$, where $\lceil \; \rceil$ denotes the ceiling function. The coefficients $t_{k,j}$ obey the following recursive relations.
(i) For $j = 1$,

$$t_{1,1} = 1\,,, \quad t_{k,1} = \frac{1}{n}\binom{n}{k} - t_{k-1,1}\,, \quad \text{where} \quad k = 2, 3, \cdots, n-2\,.$$

(ii) For $j \geq 2$,

$$t_{2\ell-1,j} = (-1)^{\ell-1}\,, \quad \text{where} \quad \ell = 1,\, 2,\, \cdots,\, \frac{n-1}{2}\,,$$
$$t_{k,j} = -t_{k-2,\,j-1} - t_{k-1,\,j}\,, \quad \text{otherwise.} \tag{5}$$

□

Let's consider the case $n = 7$. Following the notation of Theorem 2, it can be verified that

$$\begin{aligned} R_7(a,b,c) \;\; = \;\; & a^4 + 2a^3b - 2a^3c + 3a^2b^2 - 5a^2bc + 3a^2c^2 + 2ab^3 - 2ac^3 \\ & -5ab^2c + 5abc^2 + b^4 - 2b^3c + 3b^2c^2 - 2bc^3 + c^4\,. \end{aligned} \tag{6}$$

Moreover, the recursive relationship (5) of the coefficients $t_{k,j}$ in the polynomial $R_7(a,b,c)$ can be illustrated, as shown in Figure 1.

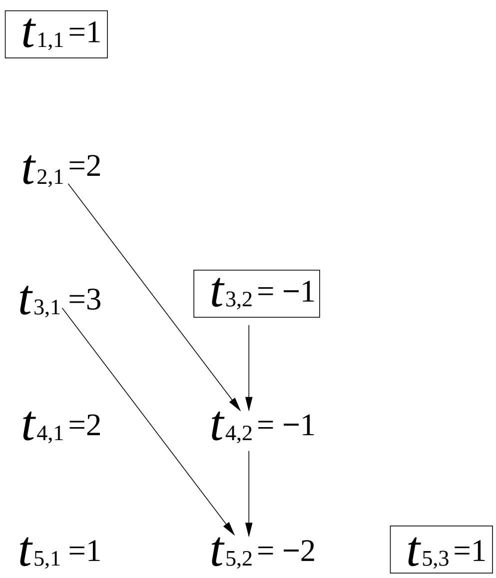

Figure 1. Coefficients $t_{k,j}$ for $n = 7$. The numbers inside the boxes are 1 or −1, alternately

Additionally, the recursive relationship (5) of the coefficients $t_{k,j}$ in the polynomial $R_{11}(a,b,c)$ is shown in Figure 2.

3. FLT equivalent identity

We now combine our results to determine an identity that is equivalent to FLT.

Theorem 3. *Let n be an odd prime, and a, b and c be positive relatively prime integers, then* $a^n + b^n = c^n$ *if and only if*

$$n(a+b)(c-b)(c-a)R_n(a,b,c) = (a+b-c)^n\,, \tag{7}$$

where $R_n(a,b,c)$ *is the homogeneous polynomial in a, b and c of degree* $n-3$ *that satisfies*

$$R_n(a,b,c) = \frac{(a+b-c)^n - a^n - b^n + c^n}{n(a+b)(c-b)(c-a)}.$$

Proof. The proof of the equivalent form follows from Proposition (1) and Theorem (2), which basically use the following manipulation

$$(a+b-c)^n - a^n - b^n + c^n = n(a+b)(c-b)(c-a)R_n(a,b,c)$$

combined with the assumption that $a^n + b^n = c^n$. □

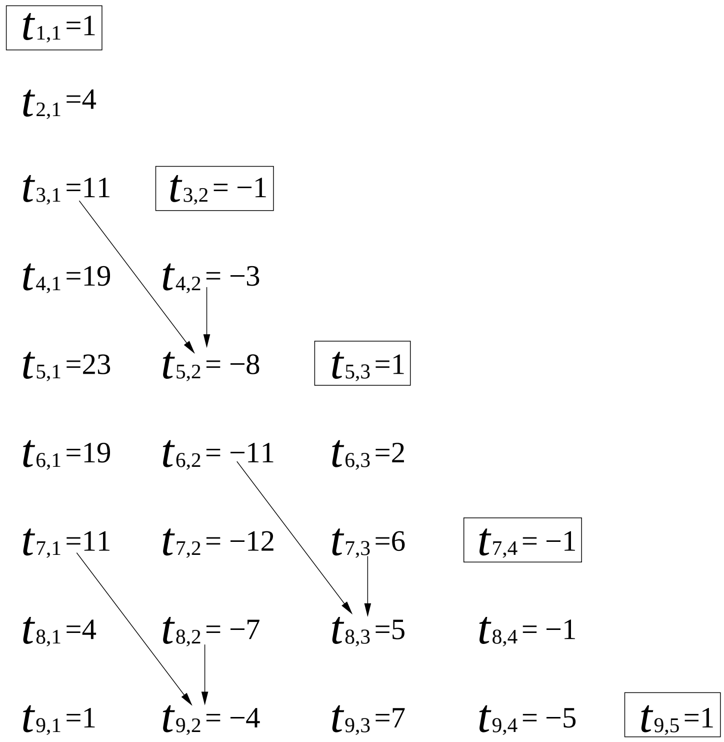

Figure 2. Coefficients $t_{k,j}$ for $n = 11$. The numbers inside the boxes are 1 or −1, alternately

4. Insight Gained From the Equivalent Identity

In the equivalent form (7), we observe that n is a multiplier on the left side of the equation and is an exponent on the right side of the equation. How is this useful?

Let's consider FLT for $n = 3$. If $a^3 + b^3 = c^3$ where a, b, c are relatively prime integers, we obtain the equivalent identity

$$3(a + b)(c - b)(c - a) = (a + b - c)^3. \tag{8}$$

This identity tells us that $n = 3$ must be a factor of one of a, b, or c. We note that this is an alternative proof to previous proofs of this case that use a congruence modulus relation [4]. Similar results are true for $n = 5$, and these are presented in the next two propositions.

Proposition 4. *Let a, b and c be positive relatively prime integers with $a^5 + b^5 = c^5$, then 5 does not divide $R_5(a, b, c) = a^2 + b^2 + c^2 + ab - bc - ad$. Therefore 5 must divide one of a, b or c.*

Proof. The equivalent form is

$$5(a + b)(c - b)(c - a)R_5(a, b, c) = (a + b - c)^5\,. \tag{9}$$

Assume that none of the three terms $(a + b)$, $(c - a)$, or $(c - b)$ has a factor 5. Equivalently, we have

$$5 \nmid c\,, \qquad 5 \nmid b\,, \qquad 5 \nmid a\,, \qquad 5|(a + b - c)\,. \tag{10}$$

This implies that

$$a \equiv 1 \pmod 5\,,\; b \equiv 1 \pmod 5\,,\; c \equiv 2 \pmod 5 \tag{11}$$

is one possibility. On the other hand, $R_5(a, b, c)$ can be expressed as

$$R_5(a, b, c) = (a + b - c)^2 + c(a + b - c) + c^2 - ab\,,$$

which is congruent to 3 (mod 5) under the congruences of a, b, c from equation (11). In Table 1 we list all possible congruences for a, b, c, and $c^2 - ab$ after modulo 5.

For example, the numbers 1, 1, 2, 3, in the second row of Table 1 are to be read as: If $a \equiv 1 \pmod 5$, $b \equiv 1 \pmod 5$, and $c \equiv 2 \pmod 5$, then $R_5(a, b, c) \equiv c^2 - ab \equiv 3 \pmod 5$. Consequently, 5 does not divide $R_5(a, b, c)$ and so 5 must divide one and only one of a, b or c. □

Table 1. Congruence table for variables a, b, c, and $c^2 - ab$ after modulo 5

$a \equiv$	$b \equiv$	$c \equiv$	$R_5(a, b, c) \equiv c^2 - ab \equiv$
1	1	2	3
1	2	3	2
2	1	3	2
1	3	4	3
3	1	4	3
2	2	4	2
2	4	1	3
4	2	1	3
3	3	1	2
3	4	2	2
4	3	2	2
4	4	3	3

5. Cases for Higher Exponents

To reiterate the insight gained by the equivalent form, we move on to a higher exponent case $n = 11$, and the similar insight provided by the equivalent form can be observed still. The details are addressed as follows.

5.1 Case $n = 11$

By using equation (2) and the recursive relation described in equations (3) and (4), we find the equivalent form for $n = 11$ to be:

$$11\ (c-b)(a+b)(c-a)\,R_{11}(a,b,c) = (a+b-c)^{11}\,, \tag{12}$$

where (see also Figure 2)

$$\begin{aligned} R_{11}(a,b,c) &= -54\,ab^2c^5 - 19\,a^3c^5 + 84\,a^3bc^4 + 123\,a^2b^2c^4 - 84\,a^3b^4c - 54\,a^5b^2c \\ &- 159\,a^2b^3c^3 - 84\,a^4b^3c + 21\,abc^6 + 123\,a^4b^2c^2 + 84\,ab^3c^4 - 19\,a^3c^5 \\ &- 159\,a^3b^2c^3 - 21\,a^6bc + 54\,ab^5c^2 - 54\,a^2b^5c - 84\,a^4bc^3 - 4\,b^7c \\ &- 54\,a^2bc^5 + 54\,a^5bc^2 - 84\,ab^4c^3 - 21\,ab^6c + 11\,a^6b^2 + 123\,a^2b^4c^2 \\ &+ 19\,a^5b^3 + 23\,a^4b^4 + 4\,a^7b + 19\,a^3b^5 + 11\,a^6c^2 - 19\,a^5c^3 - 4\,a^7c \\ &+ 11\,a^2b^6 + 11\,a^2c^6 + 4\,ab^7 - 4\,ac^7 + 11\,b^6c^2 - 19\,b^5c^3 + 23\,b^4c^4 \\ &- 19\,b^3c^5 + 11\,b^2c^6 - 4\,bc^7 + a^8 + b^8 + c^8 + 159\,a^3b^3c^2 + 23\,a^4c^4\,. \end{aligned}$$

Proposition 5. *In the factored form in equation (12), the four terms $(a + b)$, $(c - b)$, $(c - a)$, and $R_{11}(a, b, c)$ are relatively prime. That is, there is no common factor between any two of them.*

Proof. It is sufficient to show that $R_{11}(a, b, c)$ does not have any common factor with either one of $(a + b)$, $(c - b)$, and $(c - a)$.

Let us assume there is a common factor between $(a + b)$ and $R_{11}(a, b, c)$, say, $p|(a + b)$ and $p|R_{11}(a, b, c)$. This implies that $p|c$ and $p|R_{11}(a, b, c)$. Let $c = p\,k$, for some positve integer k. Replacing c in $R_{11}(a, b, c)$ by pk, we get

$$\begin{aligned} R_{11}(a,b,c) &= (a^2+ab+b^2)\left(b^6+3ab^5+7a^2b^4+9a^3b^3+7a^4b^2+3a^5b+a^6\right) \\ &+ p\,G_{11}(a,b,k)\,, \end{aligned} \tag{13}$$

where $G_{11}(a, b, k)$ is some polynomial in terms of (a, b, k). We know that $p \nmid (a^2 + ab + b^2)$; otherwise, by

$$(a+b)^2 - (a^2+ab+b^2) = ab\,,$$

the number p must divide either a or b.

It is sufficient to show that, in equation (13),

$$p \nmid \left(b^6 + 3\,ab^5 + 7\,a^2b^4 + 9\,a^3b^3 + 7\,a^4b^2 + 3\,a^5b + a^6\right)\,. \tag{14}$$

But claim (14) is clear from the fact that

$$\begin{aligned}(a+b)^6 &- \left(b^6 + 3\,ab^5 + 7\,a^2b^4 + 9\,a^3b^3 + 7\,a^4b^2 + 3\,a^5b + a^6\right)\\ &= ab\left(b^2+ab+a^2\right)\left(3\,b^2+5\,ab+3\,a^2\right),\end{aligned}$$

and $3(a+b)^2 - \left(3\,b^2+5\,ab+3\,a^2\right) = ab$. Therefore, there is no common factor between $(a+b)$ and $R_{11}(a,b,c)$.

By the same token, suppose there is a common factor between $(c-a)$ and $R_{11}(a,b,c)$, say, $p|(c-a)$ and $p|R_{11}(a,b,c)$. This means $p|b$ and $p|R_{11}(a,b,c)$. Then $b = p\,k$, for some positive integer k. Replacing b in $R_{11}(a,b,c)$ by $p\,k$, one gets

$$\begin{aligned}R_{11}(a,b,c) &= \left(c^2-ac+a^2\right)\left(c^6 - 3\,c^5a + 7\,c^4a^2 - 9\,c^3a^3 + 7\,c^2a^4 - 3\,ca^5 + a^6\right)\\ &+ p\,H_{11}(a,c,k),\end{aligned} \tag{15}$$

where $H_{11}(a,b,k)$ is some polynomial in terms of (a,c,k). But $p \not| (c^2-ac+a^2)$; otherwise, by

$$(c^2-ac+a^2)-(c-a)^2 = c\,a,$$

the number p must divide either c or a, and this contradicts with the assumption that the triple (a,b,c) is relatively prime.

Furthermore, in equation (15) above,

$$\begin{aligned}&\left(c^6 - 3\,c^5a + 7\,c^4a^2 - 9\,c^3a^3 + 7\,c^2a^4 - 3\,ca^5 + a^6\right) - (c-a)^6\\ =\;& ac\left(c^2-ac+a^2\right)\left(3\,c^2-5\,ac+3\,a^2\right),\end{aligned}$$

and $\left(3\,c^2-5\,ac+3\,a^2\right) - 3(c-a)^2 = ca$. We conclude that there is no common factor between $(c-a)$ and $R_{11}(a,b,c)$.

Similarly, if there is a common factor between $(c-b)$ and $R_{11}(a,b,c)$, then the triple (a,b,c) is not relatively prime. □

Similar to the case $n=5$ we have following observation for $n=11$ by using the equivalent form.

Proposition 6. *Let a, b and c be positive relatively prime integers with $a^{11}+b^{11}=c^{11}$, then* 11 *does not divide $R_{11}(a,b,c)$. Therefore 11 must divide one of a, b or c.*

Proof. The proof is essentially the same as the proof for the case $n=5$. Here we break down $R_{11}(a,b,c)$ as

$$R_{11}(a,b,c) = P(a,b) - c(a+b-c)Q(a,b,c), \tag{16}$$

where

$$P(a,b) = (b^2+ab+a^2)(b^6+3ab^5+7a^2b^4+9a^3b^3+7a^4b^2+3a^5b+a^6)$$

and $Q(a,b,c)$ is a 6-degree homogeneous polynomial in the variables a, b and c. Then a similar table to Table 1 can be constructed with all possible congruences for a, b, c, and $P(a,b)$ after modulo 11. See Table 2.

Table 2. Congruence table for variables a, b, c, and $P(a,b)$ after modulo 11

$a \equiv$	$b \equiv$	$c \equiv$	$P(a,b) \equiv$
1	1	2	5
1	2	3	2
1	3	4	7
1	4	5	8
⋮	⋮	⋮	⋮
10	10	9	5

For example, the numbers 1, 1, 2, 5, in the second row are to be read: If $a \equiv 1 \pmod{11}$, $b \equiv 1 \pmod{11}$, $c \equiv 2 \pmod{11}$, then $P(a,b) \equiv 5 \pmod{11}$. From Table 2 it follows that 11 cannot be a factor of $R_{11}(a,b,c)$, hence by the equivalent form 11 must divide one of a, b, or c. □

5.2 Case $n = 7$

Though the FLT equivalent identity yields some good insight for the cases $n = 3$, 5, and 11—namely that if $a^n + b^n = c^n$ then n divides one of a, b or c—it does not provide the exact same outcome for the case $n = 7$. As shown for $n = 3$, 5 and 11, it still follows for $n = 7$ that $(a + b)$, $(c - b)$, $(c - a)$ and $R_n(a, b, c)$ are relatively prime, as shown in Proposition (7), but the stronger result that 7 divides one of a, b or c can only be stated as a conjecture at this time.

Proposition 7. *Let a, b and c be positive relatively prime integers with $a^7 + b^7 = c^7$. Then in the equivalent form, equation (7), the four terms $(a + b)$, $(c - b)$, $(c - a)$, and $R_7(a, b, c)$ are relatively prime. That is, there is no common factor between any two of them.*

Proof. We have already seen that the three terms $(a+b)$, $(c-b)$, and $(c-a)$ are relatively prime in Proposition (1). Hence, it suffices to show that $R_7(a, b, c)$ does not have a common factor with $(a + b)$, $(c - b)$ or $(c - a)$.

Let's assume there is a common factor between $(a + b)$ and $R_7(a, b, c)$, say, $p|(a + b)$ and $p|R_7(a, b, c)$. Then also $p|c$, and so $c = pk$ for some positive integer k. Replacing c by pk in $R_7(a, b, c)$, which is given in equation (6), we get

$$R_7(a, b, c) = (a^2 + ab + b^2)^2 + pG(a, b, k), \tag{17}$$

where $G(a, b, k)$ is a polynomial in terms of (a, b, k). But $p \nmid (a^2 + ab + b^2)$, since otherwise from

$$(a + b)^2 - (a^2 + ab + b^2) = ab, \tag{18}$$

the prime p must divide either a or b. This contradicts the assumption that the triple (a, b, c) is relatively prime.

Next, let's assume there is a common factor between $(c - a)$ and $R_7(a, b, c)$, say, $p|(c - a)$ and $p|R_7(a, b, c)$. Then also $p|b$, and so $b = pk$ for some positive integer k. Replacing b in $R_7(a, b, c)$ by pk, one obtains

$$R_7(a, b, c) = (c^2 - ac + a^2)^2 + pH(a, b, k), \tag{19}$$

where $H(a, b, k)$ is a polynomial in terms of (a, b, k). But $p \nmid (c^2 - ac + a^2)$, since otherwise from

$$(c^2 - ac + a^2) - (c - a)^2 = ca, \tag{20}$$

the prime p must divide either c or a, and this contradicts the assumption that the triple (a, b, c) is relatively prime.

Similarly, if there is a common factor between $(c - b)$ and $R_7(a, b, c)$, then the triple (a, b, c) is not relatively prime. □

Conjecture 8. *If there are positive integer solutions to $a^7 + b^7 = c^7$ with $gcd(a, b, c) = 1$, then one and only one of a, b or c is divisible by 7.*

6. A Big Conjecture

In summary, we have established that for a prime number $n \geq 3$, $a^n + b^n = c^n$ is equivalent to

$$n(a + b)(c - a)(c - b)R_n(a, b, c) = (a + b - c)^n\,, \tag{21}$$

where $R_n(a, b, c)$ can be obtained according to the recursive relationship that we have derived in this paper. Here we list the following three observations regarding the the equivalent form (21).

6.1 Consistency of the Equivalent Form

The first major observation we have is that the equivalent form (21) stays the same for all n. Particularly, the term $(a + b - c)^n$ on the right hand side of the equivalent form (21) is the same for all n. Based on the fact (and assumption) that $(a + b)$, $(c - a)$, $(c - b)$, and $R_n(a, b, c)$ are all relatively prime, it seems that the term $(a + b - c)$ "takes up too many factors".

6.2 Too Many nth-power Terms

The second observation is that the equivalent form (21) tells us there are "too many nth-power terms". For instance, for $n = 3$, according to the equivalent form (8) and the assumption that 3 divides c, we have the following outcomes:

$$a = \alpha_1\alpha_2,\ b = \beta_1\beta_2,\ c = 3^2\gamma_1\gamma_2, \quad a + b = 3^5\gamma_1^3,\ c - b = \alpha_1^3, \text{ and } c - a = \beta_1^3\,, \tag{22}$$

where the integers α_1, α_2, β_1,β_2, γ_1, and γ_2 are relatively prime. So, the terms $c-a$ and $c-b$ are both cubes, and $a+b$ contains a cube as a factor.

Similarly, for $n = 5$, according to the equivalent form (9) and the assumption that 5 divides c, then

$$a = \alpha_1\alpha_2,\ b = \beta_1\beta_2,\ c = 5^2\gamma_1\gamma_2, \quad a+b = 5^9\gamma_1^5,\ c-b = \alpha_1^5,\ c-a = \beta_1^5, \text{and } R_5(a,b,c,) = \delta^5\,, \tag{23}$$

where α_1, α_2, β_1,β_2, γ_1, γ_2, and δ are relatively prime integers. Among them $c-a$, $c-b$, and $R_5(a,b,c,)$ are all of 5-th power.

For a general prime $n \geq 3$, we may see that at least two of the four terms $(a+b)$, $(c-a)$, $(c-b)$, and $R_n(a,b,c)$ are of nth-power.

6.3 The Third Observation

The third observation does not have an easy name, and we describe it by different cases of n.

For $n = 3$, the combination of equations (8) and (22) leads to

$$3(a+b)(c-b)(c-a) = 3\times 3^5\gamma_1^3\,\alpha_1^3\beta_1^3 = (a+b-c)^3 = (9\alpha_1\beta_1\gamma_1)^3.$$

One interesting observation is that

$$(a+b)-(c-b)-(c-a) = 2(a+b-c)\,, \quad \text{or} \quad 3^5\gamma_1^3 - \alpha_1^3 - \beta_1^3 = 2\times 9\alpha_1\beta_1\gamma_1. \tag{24}$$

Recall the fact that $(a+b)$, $(c-b)$, and $(c-a)$ are all relatively prime. Therefore, equation (24) says that a linear combination of three relatively prime cubes makes up a number being a product of the three numbers $(\alpha_1\beta_1\gamma_1)$. Although we cannot directly show it is not true, we cannot find any examples showing equation (24) is true.

For the cases $n = 5$ and higher exponents n, the argument is very similar. We reiterate the process for $n = 5$ here. The combination of equations (8) and (23) leads to

$$5(a+b)(c-b)(c-a)R_5(a,b,c) = 5\times 5^9\gamma_1^5\,\alpha_1^5\beta_1^5\,R_5(a,b,c) = (a+b-c)^5 = (25\alpha_1\beta_1\gamma_1\delta)^5.$$

By the fact $(a+b)-(c-b)-(c-a) = 2(a+b-c)$, that is,

$$5^9\gamma_1^5 - \alpha_1^5 - \beta_1^5 = 2\times 25\alpha_1\beta_1\gamma_1\delta\,. \tag{25}$$

Equation (25) says that a linear combination of three relatively prime fifth powers makes up a number being a product of the three numbers $(\alpha_1\beta_1\gamma_1)$ themselves. Again, we cannot find any number examples that support equation (25).

6.4 The Big Conjecture

Based on our three given observations, we propose a big conjecture:

The equivalent form (25) cannot be true.

Therefore, $a^n + b^n = c^n$ cannot be true, either.

7. Conclusion

We have demonstrated an equivalent form (Theorem 3) to $a^n + b^n = c^n$ in FLT. The equivalent form provides more information about the relationships between a, b, c and n than FLT due to the fact that n appears both as a factor and a power in the equivalent form. It is our hope that this equivalent form will be useful to others interested in answering questions about the positive integers motivated by FLT.

References

Andrew Wiles on Solving Fermat, *http://www.pbs.org/wgbh/nova/physics/andrew-wiles-fermat.html*, November 2000. Accessed March 8, 2022.

Fermat's Last Theorem, MacTutor History of Mathematics, *www-history.mcs.st-andrews.ac.uk*. Accessed August 8, 2022.

Hardy, G. H., & Wright, E. M. (1979). *An Introduction to the Theory Of Numbers*. (5th ed.). Clarendon Press, Oxford.

Ribenboim, P. (1979). *13 Lectures on Fermat's Last Theorem*. Springer-Verlag, New York. https://doi.org/10.1007/978-1-4684-9342-9