FERMAT'S LITTLE THEOREM

ELABORATION ON HISTORY OF FREMAT'S THEOREM

AND IMPLICATIONS OF EULER'S GENERALIZATION BY MEANS OF THE TOTIENT THEOREM

by

James Robinson

A Thesis Submitted to the Faculty of the

DEPARTMENT OF MATHEMATICS

In Partial Fulfillment of the Requirements

For the Degree of

MASTER OF ARTS
WITH A MAJOR IN MIDDLE SCHOOL MATHEMATICS

In the Graduate College

THE UNIVERSITY OF ARIZONA

2011

Part I. Background and History of Fermat's Little Theorem

Fermat's Little Theorem is stated as follows:

If *p* is a prime number and *a* is any other natural number not divisible by *p,* then the number $a^{p-1}-1$ is divisible by *p.*

However, some people state Fermat's Little Theorem as,

If *p* is a prime number and *a* is any other natural number, then the number $a^p - a$ is divisible by *p.*

In this paper, I will address the following: if these two representations of Fermat's Little Theorem are these the same thing, how the Little Theorem works, and whether the Little Theorem can/will work with composite moduli. Before beginning my explanation, it seemed necessary to put to paper the different ways that Fermat's Little Theorem can be represented. Aforementioned above are two representations, but another variation of those two forms has been given as I studied this problem.

When I first tackled the problem, I thought it proper to write out Fermat's Little Theorem as an equation. If $a^{p-1}-1$ is divisible by *p*, then the remainder would be zero, and so:

$$a^{p-1}-1 \equiv 0 \pmod{p}$$

And, in the same way, the second form of the Theorem would be:

$$a^p - a \equiv 0 \pmod{p}$$

However, elsewhere I came across the Little Theorem written slightly differently, although equivalent (Weisstein, 1995)

$$a^{p-1} \equiv 1 \pmod{p}$$

and

$$a^p \equiv a \pmod{p}$$

The difference between the second forms is that 1 and *a* have been left on the right side of the congruence. In setting the congruences equal to a remainder of zero, the 1 and *a* have been moved to the left side, still preserving its original value. These last two representations will play a role in justifying my explanation of how Fermat's Little Theorem works, but I wanted to establish these alternate forms before beginning my explanations.

A Brief History of Fermat's Little Theorem

1. Who preceded the Little Theorem:

Before working through the problem of Fermat's Little Theorem, I thought it prudent to look backward first to establish some of the ideas behind the direction that Fermat (and, ultimately, Euler) headed. Knowing that I was looking for relatively prime numbers, that is, numbers that only share 1 as a common factor, I first thought of Euclid's division algorithm. Also, the foundation set by the Fundamental Theorem of Arithmetic was an essential tool in the sense that anticipating and predicting other larger numbers necessitates utilizing prime factorization to logically simplify the process.

Around 300 BC, Euclid had written a mathematical work called the *Elements.* Within this work, Proposition VII.2 provides an algorithm on how to find the Greatest Common Factor (divisor) for any numbers. This algorithm has come to be known as Euclid's Algorithm. In Proposition VII.30 of Euclid's *Elements*, he indirectly claims the fact that all composite numbers can be represented as a product of prime numbers, but it is in fact Gauss, in 1801, who is attributed with the first direct statement of the Fundamental Theorem of Arithmetic in his book, *Disquisitiones Arithmeticae* (Bogomolny, 2000).

Around 200 BC, another mathematician, Eratosthenes, provided a tool for identifying prime numbers. The "Sieve of Eratosthenes" functions by identifying and eliminating multiples, first 2's, then 3's, then 4's, etc. The results of casting out these multiples eventually leaves only primes (Caldwell, 1994)

Discovering more about Euclid and Eratosthenes helped my progress as I worked with Fermat's Little Theorem as well as Euler's Totient Function, which I will discuss in more depth along with Euler. Specifically, getting a better understanding of the preceding ideas around prime and composite numbers, Euclid's algorithm for finding a Greatest Common Factor, and the notion that all numbers are either prime or can be represented as a product of prime factors, all these concepts aided me to understand the process used by Fermat and Euler.

2. Who was involved in proving/establishing Theorem:

From what I have discovered in my research behind the problem, Pierre de Fermat (1601-1655) was well regarded mathematician. He is ascribed with contributing to the areas of analytic geometry, probability, number theory, and optics. One of his greatest problems, aptly named his "Last Theorem", stood unsolved until a proof was successfully accomplished in 1995 by the British mathematician Andrew Wiles. This paper, however, is about Fermat's "Little Theorem". It is said that Fermat's Little Theorem was first proposed in 1640 in a letter he sent to his friend, Frénicle. (Weisstein, 1994 and Stevenson, 2000) Moreover, Fermat claimed in the letter to Frénicle to have a proof for this Little Theorem, but he chose not to include because it was "too long" (Caldwell, 1994). No one successfully proved Fermat's claim until Leonhard Euler in

1736, although Stevenson makes mention of an unpublished manuscript in 1683 by Leibnitz. (2000, p.132)

Euler (1707-1783) was also an esteemed mathematician. Prior to studying his contribution to this particular problem of Fermat's Little Theorem, I had read about his work involving discrete math and, in particular, vertex edge graphs involving paths and circuits. Specifically, he is associated with the famous Seven Bridges of Konigsberg problem (Reed, 1998).

In 1736, Euler published a proof for Fermat's theorem. Not only that, but Euler also generalized it. Bogomolny (2000) asserts that the generalization was accomplished by Euler in 1860. Euler's proof ingeniously modifies Fermat by what has been called the Totient Theorem. Euler's Theorem relies on his Totient Function, designated as $\phi(m)$, where *m* represents a determined number of integers. The Totient Function, $\phi(m)$, determines the number of relatively prime numbers to a given number. For instance, all primes (p) have p-1 values that are relatively prime to itself. Case in point, the prime 7 has $\phi(7) = 6$ because (1,2,3,4,5, and 6) are relatively prime to 7. In this respect, Euler's Totient Theorem matches Fermat, but Euler took it further as he does not have the condition that the modulo must be prime. His Totient Function allows for both composite and prime moduli (Weisstein, 1995) This fact has direct bearing on what is to be discussed in this paper, and I will explain this difference and its connection to the Little Theorem in more detail near the end of this paper.

Fermat's Little Theorem is considered a special case of Euler's general Totient Theorem as Fermat's deals solely with prime moduli, while Euler's applies to any number so long as they are relatively prime to one another (Bogomolny, 2000). I want to be careful, though, not to get too far ahead here in what is meant to provide a background to the history of Fermat's Little Theorem.

The last person I investigated was Carl Friedrich Gauss (1777-1855). One of his contributions was the idea of congruence arithmetic. According to Pommersheim et al., "Mathematicians consider the publication of *Disquisitiones* as the birth of modern number theory. In particular, the concept of congruence modulo *n...*revolutionized the way that mathematicians thought about number theory" (2010, p. 239). Clearly, Euler preceded Gauss, yet still his ideas helped to build on both Fermat and Euler. I read a bit about Gauss, but beyond establishing congruences, Gauss' role is incidental in my research on Fermat's Little Theorem (O'Connor & Robertson , 1997).

Gauss is absolutely involved in the math underlying the use of the Little Theorem as well as Euler's Totient Theorem, but I want to stay focused just on Euler and Fermat. The role of congruence, as I understand it, has more importance to how Euler/Fermat is used now than it does with what I hope to discuss here. This paper is intended solely to focus on Fermat, and as a consequence, Euler's generalization and not on its current use.

3. Where the Theorem has gone:

As I investigated the Little Theorem and the Totient Theorem, I found it fascinating that the work of Fermat and Euler is still in use today with computer data encryption. Still, I do not intend to do more than document this application. This application is relevant, but beyond the scope of this paper.

RSA is a computer algorithm named for its designers, Rivest, Shamir, and Adleman in 1977. RSA uses Euler's Totient Function and, in turn, Fermat's Little

Theorem, as a cipher to encode and decode data. The idea behind this cipher is that a computer can very efficiently multiply two very large numbers together, but starting with a very large number and working backward to find its prime factors still requires a guess and check method. Of course, a computer clearly can do the checks much faster than human computation, but it still remains that computers require many hours, if not days or more, of processing time to successfully factor numbers that may be dozens of digits or more (Pommersheim et al, 2010).

In conclusion, what began as a unproven claim by Fermat in a letter has ultimately provided mathematics with a very powerful algorithm to protect data from being deciphered. Through the advances and innovations of Leonhard Euler in the 18th century and Wilhelm Gauss in the 19th century, Fermat's initial claim in 1640 has been augmented and digitized by the RSA in the 20th century, nearly 240 years from its beginnings with Fermat. When one also recognizes that Eratosthenes and Euclid provided a foundation regarding prime numbers, factorization, and an algorithm for finding a Greatest Common Factor (divisor), this problem has been toiled over in various forms by some of the greatest mathematicians for more than two thousand years.

Part II. Explanation of the Two Representations of Fermat's Little Theorem.

As I said at the beginning of this paper, the first thing I will address is whether the two representations of Fermat's Little Theorem, $a^{p-1}-1\equiv 0$ (mod *p*) and $a^{p}-a\equiv 0$

(mod *p*) , are the same thing. That is, are the two forms equivalent? At the outset, my answer is yes.

I began my research by testing both of the forms and comparing the results. On the right side of Table 1 above, I have included and highlighted the multiples of 3, which do not work for the $a^{p-1}-1\equiv 0$ representation of the Little Theorem. In modulo 3, clearly all multiples of 3 will share a common factor and therefore will be divisible by 3 before subtracting 1, resulting in a remainder of 2. As can be seen from the results above, the Little Theorem works consistently and the pattern repeats through all multiples of 3.

Table 1. Mod 3

	a^(p-1)-1	mod p		a^p-a	mod p
2^(3-1)-1	3	0	2^3-2	6	0
3^(3-1)-1	8	2	3^3-3	24	0
4^(3-1)-1	15	0	4^3-4	60	0
5^(3-1)-1	24	0	5^3-5	120	0
6^(3-1)-1	35	2	6^3-6	210	0
7^(3-1)-1	48	0	7^3-7	336	0
8^(3-1)-1	63	0	8^3-8	504	0
9^(3-1)-1	80	2	9^3-9	720	0
10^(3-1)-1	99	0	10^3-10	990	0
11^(3-1)-1	120	0	11^3-11	1,320	0
12^(3-1)-1	143	2	12^3-12	1,716	0
13^(3-1)-1	168	0	13^3-13	2,184	0
14^(3-1)-1	195	0	14^3-14	2,730	0
15^(3-1)-1	224	2	15^3-15	3,360	0
16^(3-1)-1	255	0	16^3-16	4,080	0
17^(3-1)-1	288	0	17^3-17	4,896	0

On the left side of Table 1 above, it can be seen that the Little Theorem works for every number, even multiples of 3. One would wonder why this representation of the theorem, $a^{p}-a\equiv 0$, works and not the other. Starting with the second form, $a^{p}-a\equiv 0$, if you factor out the natural number *a,* the result is $a(a^{p-1}-1)\equiv 0$ (mod *p*). The consequence of this is that one is left with the first form of the Little Theorem multiplied by a factor of the natural number *a.* As I have stated previously, the constraints placed on the first form, that **"*p* is a prime number and *a* is any other natural number not divisible by *p*"** , has been removed allowing for the Little Theorem to work in all cases.

Specifically, this can be seen in the case when *a* is 3 and the prime is 3:

		mod 3			**mod 3**
3^(3-1)-1	**8**	**2**	**3^3-3**	**24**	**0**

Before subtracting 1, the product would have been 9, which would be 0 (mod 3). However, in subtracting 1, the result is a remainder of 2. However, in the second case, $3^3 = 27$, which is 0 (mod 3), but subtracting *a,* which is 3, results in 24 which is still 0 (mod 3). If I were to factor out 3 from this example, it is clearer to see that the second form can work "**for any other natural number"** because *a* has been included as a factor.

$$a^p - a \equiv 0 (\bmod p)$$

becomes $a(a^{p-1} - 1) \equiv 0 (\bmod p)$

$$(3^3 - 3) \equiv 24 \equiv 0 \ (\bmod 3)$$

therefore, $3(3^{3-1} - 1) \equiv 24 \equiv 3(8) \equiv 0 \quad (\bmod 3)$

So, in the case of $a^{p-1} - 1 \equiv 0$, where the Little Theorem does not work, the modified second form $a(a^{p-1} - 1) \equiv 0$ does work because now 3 is included in the factors which results in 0 (mod 3).

Again, addressing the question as to whether or not the two representations of Fermat's Little Theorem are the same, I must answer that they are equivalent. The first form, $a^{p-1} - 1 \equiv 0 \pmod{p}$, however must have the constraint that the natural number *a* cannot be divisible by *p,* which effectively mandates that any natural number chosen must be relatively prime. In the second form, $a^p - a \equiv 0 \pmod{p}$, any natural number will work. Firstly, if a product was already divisible by 3, then doubling, tripling, quadrupling, etc., does not change that the number remains divisible by 3. That is, whether we are talking about 12, 24, 36, etc., all of these can still be divided by 3, or better put result in 0 (mod 3).

On a side note, when I first tackled this problem, I did not first use a spreadsheet program, which I did use to produce the data tables provided below. I struggled with how to display the immensity of the numbers generated when raising a larger number to large power. My calculator quickly became useless, and even my spreadsheet program ran out of available digits.

However, I made a breakthrough when I made use of the Fundamental Theorem of Arithmetic. I had this idea after I read about Euler's Totient Function. The Totient Function is multiplicative, and from there I realized that I could, in fact, predict with certainty what numbers would still work with Fermat's Little Theorem by what I knew about common factors and the fact that numbers can be represented as a product of prime factors (Bogomolny, 2000).

To illustrate that prime factorization still applies, I have shown below Fermat's Little Theorem applied to the natural numbers 2, 7, and 14 in modulo 3. I have chosen these natural numbers because to satisfy the Little Theorem, the numbers chosen for *a* cannot be divisible by *p*, which is 3.

$2^{3-1} - 1 \equiv 0 \pmod 3$

$2^2 - 1 \equiv 0 \pmod 3$

$3 \equiv 0 \pmod 3$

$7^{3-1} - 1 \equiv 0 \pmod 3$

$7^2 - 1 \equiv 0 \pmod 3$

$48 \equiv 0 \pmod 3$

$14^{3-1} - 1 \equiv 0 \pmod 3$

$14^2 - 1 \equiv 0 \pmod 3$

$(2 * 7)^2 - 1 \equiv 0 \pmod 3$

$(2^2 * 7^2) - 1 \equiv 0 \pmod 3$

$(4 * 49) - 1 \equiv 0 \pmod 3$

$196 - 1 \equiv 0 \pmod 3$

$195 \equiv 0 \pmod 3$

Tables 2-4 show Fermat’s Little Theorem applied in moduli 5, 7, and 11.

Table 2. Mod 5

	a^(p-1)-1	mod p		a^p-a	mod p
2^(5-1)-1	**15**	0	**2^5-2**	30	0
3^(5-1)-1	**80**	0	**3^5-3**	240	0
4^(5-1)-1	**255**	0	**4^5-4**	1,020	0
5^(5-1)-1	**624**	**4**	**5^5-5**	3,120	0
6^(5-1)-1	**1,295**	0	**6^5-6**	7,770	0
7^(5-1)-1	**2,400**	0	**7^5-7**	16,800	0

	a^(p-1)-1	mod p		a^p-a	mod p
8^(5-1)-1	**4,095**	0	**8^5-8**	32,760	0
9^(5-1)-1	**6,560**	0	**9^5-9**	59,040	0
10^(5-1)-1	**9,999**	**4**	**10^5-10**	99,990	0
11^(5-1)-1	**14,640**	0	**11^5-11**	161,040	0
12^(5-1)-1	**20,735**	0	**12^5-12**	248,820	0
13^(5-1)-1	**28,560**	0	**13^5-13**	371,280	0
14^(5-1)-1	**38,415**	0	**14^5-14**	537,810	0
15^(5-1)-1	**50,624**	**4**	**15^5-15**	759,360	0

In Table 2 showing modulo 5, the same pattern occurs where the Little Theorem does not work on the right side for all multiples of 5, yet on the left, the Theorem works. In Tables 3-4 showing prime moduli 7 and 11, the same pattern occurs where the Little Theorem does not work on the right side with multiples of the stated moduli.

Table 3. Mod 7

	a^(p-1)-1	mod p		a^p-a	mod p
2^(7-1)-1	**63**	0	**2^7-2**	126	0
3^(7-1)-1	**728**	0	**3^7-3**	2,184	0
4^(7-1)-1	**4,095**	0	**4^7-4**	16,380	0
5^(7-1)-1	**15,624**	0	**5^7-5**	78,120	0
6^(7-1)-1	**46,655**	0	**6^7-6**	279,930	0
7^(7-1)-1	**117,648**	**6**	**7^7-7**	823,536	0
8^(7-1)-1	**262,143**	0	**8^7-8**	2,097,144	0
9^(7-1)-1	**531,440**	0	**9^7-9**	4,782,960	0
10^(7-1)-1	**999,999**	0	**10^7-10**	9,999,990	0
11^(7-1)-1	**1,771,560**	0	**11^7-11**	19,487,160	0
12^(7-1)-1	**2,985,983**	0	**12^7-12**	35,831,796	0
13^(7-1)-1	**4,826,808**	0	**13^7-13**	62,748,504	0
14^(7-1)-1	**7,529,535**	**6**	**14^7-14**	105,413,490	0

Table 4. Mod 11

	a^(p-1)-1	mod p		a^p-a	mod p
2^(11-1)-1	**1,023**	0	**2^11-2**	2,046	0
3^(11-1)-1	**59,048**	0	**3^11-3**	177,144	0
4^(11-1)-1	**1,048,575**	0	**4^11-4**	4,194,300	0
5^(11-1)-1	**9,765,624**	0	**5^11-5**	48,828,120	0

	a^(p-1)-1	mod p		a^p-a	mod p
6^(11-1)-1	**60,466,175**	0	**6^11-6**	362,797,050	0
7^(11-1)-1	**282,475,248**	0	**7^11-7**	1,977,326,736	0
8^(11-1)-1	**1,073,741,823**	0	**8^11-8**	8,589,934,584	0
9^(11-1)-1	**3,486,784,400**	0	**9^11-9**	31,381,059,600	0
10^(11-1)-1	**9,999,999,999**	0	**10^11-10**	99,999,999,990	0
11^(11-1)-1	**25,937,424,600**	**10**	**11^11-11**	2.85312E+11	0
12^(11-1)-1	**61,917,364,223**	0	**12^11-12**	7.43008E+11	0

Again, in Table 4 showing modulo 11, where I have used 11 for the natural number *a*, predictably it does not work on the right side when using the $a^{p-1}-1$ representation of the Little Theorem. I can deduce that it will also not work for 22 as it factors into 2*11. I can also deduce that it will work for 16 as it factors into 2*8 or 2*2*4 or 2*2*2*2, and for the natural numbers 2,4,and 8, these result in 0 (mod 11).

Part III. Explanation on Why Fermat’s Little Theorem Works.

The next topic that I will address is why the Little Theorem is works. To illustrate how the Little Theorem is true, I have provided multiplication tables for 3, 5, 7, and 11. In the prime moduli, a pattern recurs that demonstrates the inherent process at work. Specifically, in each of the multiplication tables for the prime moduli, there is no instance in which a zero occurs as a remainder. The lack of an zeroes is crucial. Tables 5 and 6 are adapted from an explanation made by Pommersheim (2010, p. 360-361) As is shown below, a multiplication table is made for a prime modulo *p*, then extending those results, a table for exponents in the prime modulo *p* illustrates that for the row *p-1,* only 1 occurs as a remainder.

Table 5. Mod 3

x	1	2
1	1	2
2	2	1

By multiplying the values in Table 5, you can set up a numeric equation, which is shown on the next page. I will used 1 for the natural number *a* to demonstrate Fermat’s Little Theorem. However, because all the values occur for both 1 and 2, we can say that the results apply to both numbers 1 and 2 in modulo 3. Regrettably, in modulo 3, the results are true, but a bit anti-climactic.

$(1*1)*(2*1)=1*2$ *(mod 3)*

$(1*1)*(1*2)=1*2$ *(mod 3)* commutative property

$1^2=1$ *(mod 3)* regrouped with exponents

$1^{3-1}-1=0$ *(mod 3)* **[Fermat's observed Little Theorem]**

$0=0$ *(mod 3)*

<u>Table 6. Exponents in Mod 3</u>

	1	**2**
a^1	1	2
a^2	**1**	**1**
a^3	1	2

The implications for this result are shown in Table 6. As I have stated, because all the values appear, in this case 1 and 2, for each of the numbers, the steps shown above will work for 2 as well. Fermat's Little Theorem states that $a^{p-1}\equiv 1$ (mod *p*) and can also be represented as $a^{p-1}-1\equiv 0$ (mod *p*). In Table 6, only 1's occur in row 2 (3-1=2, where , a^{3-1}mod 3).

Let us next look at modulo 5.

Table 7. Mod 5

x	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Again, for modulo 5, from Table 7, one can observe that all the values 1-4 occur as products for each number after multiplication. Because every value occurs without zeroes, Fermat's Little Theorem can be applied to any number. Here, I chose 2 for the value of the natural number *a.* The result of the Little Theorem is the row for a^4 (mod 5).

$$(1*2)*(2*2)*(3*2)*(4*2)=1*2*3*4 \text{ (mod 5)}$$

$$(2*2*2*2)*(1*2*3*4)=1*2*3*4 \text{ (mod 5)}$$

$$2^4=1 \text{ (mod 5)}$$

$$2^{5-1}-1=0 \text{ (mod 5)}$$

$$16-1=0 \text{ (mod 5)}$$

$$15=5(3)=0 \text{ (mod 5)}$$

Table 8 represents exponents in prime modulo 5. Again, only 1's occur in the fourth row, where a^{5-1} modulo 5.

Table 8. Exponents in Mod 5

	1	**2**	**3**	**4**
a^1	1	2	3	4
a^2	1	4	4	1
a^3	1	3	2	4
a^4	**1**	**1**	**1**	**1**
a^5	1	2	3	4

Below, I have used 3 for my calculations. Again, please observe in Table 9 that the values 1-6 occur in varied order but without zeroes for all the products in modulo 7.

Table 9. Mod 7

x	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$$(1*3)*(2*3)*(3*3)*(4*3)*(5*3)*(6*3)=1*2*3*4*5*6 \quad \text{(mod 7)}$$

$$(3*3*3*3*3*3)*(1*2*3*4*5*6)=1*2*3*4*5*6 \quad \text{(mod 7)}$$

$$3^6=1 \quad \text{(mod 7)}$$

$$3^{7-1}-1=0 \quad \text{(mod 7)}$$

$$729-1=0 \quad \text{(mod 7)}$$

$$728=7(104)=0 \quad \text{(mod 7)}$$

Table 10. Exponents in Mod 7

	1	**2**	**3**	**4**	**5**	**6**
a^1	1	2	3	4	5	6
a^2	1	4	2	2	4	1
a^3	1	1	6	1	6	6
a^4	1	2	4	4	2	1
a^5	1	4	5	2	3	6
a^6	**1**	**1**	**1**	**1**	**1**	**1**
a^7	1	2	3	4	5	6

From Table 10, the predictable results have been highlighted. Below, I have applied the same process one last time for prime modulo 11. Again, because values 1-10 occur for all numbers in varied order but without zeroes, it can be confirmed that Fermat’s Little Theorem can be applied consistently.

Table 11. Mod 11

x	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	1	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

One can see that from table 11, that all the values occur. The result of this is that the row a^{10} has only 1’s for values as are displayed in Table 12, which shows how exponents work in modulo 11. Below are steps to establish that the Little Theorem works and the table of resulting exponents is shown on the following page.

$$(1*4)*(2*4)*(3*4)*(4*4)*(5*4)*(6*4)*(7*4)*(8*4)*(9*4)*(10*4)=1*2*3*4*5*6*7*8*9*10$$
$$(4*4*4*4*4*4*4*4*4*4)*(1*2*3*4*5*6*7*8*9*10)=1*2*3*4*5*6*7*8*9*10$$

$4^{10}=1$ (mod 11)

$4^{11-1}=1$ (mod 11)

$1048576-1=0$ (mod 11)

$1048575=11(95325)=0$ (mod 11)

Table 13. Exponents in Mod 11

x	1	2	3	4	5	6	7	8	9	10
a^1	1	2	3	4	5	6	7	8	9	10
a^2	1	4	9	5	3	3	5	9	4	1
a^3	1	8	5	9	4	7	2	6	3	10
a^4	1	5	4	3	9	9	3	4	5	1
a^5	1	10	1	1	1	10	10	10	1	10
a^6	1	9	3	4	5	5	4	3	9	1
a^7	1	7	9	5	3	8	6	2	4	10
a^8	1	3	5	9	4	4	9	5	3	1
a^9	1	6	4	3	9	2	8	7	5	10
a^{10}	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
a^{11}	1	2	3	4	5	6	7	8	9	10

Part IV. Fermat Little Theorem, Euler's Totient Functions, and Composite Moduli.

The next topic I will address are whether Fermat's Little Theorem will work if the constraint of ***p*** being prime is removed, allowing for a natural number raised to a composite power. Specifically, I will address two things. First, if the Theorem will work with a composite *p* and **all natural numbers** that do not share a common factor with *p* other than 1. Second, if the Theorem will work with a composite power and **any natural number *a*.**

Same as I had done before, I plugged in various values for *a* in order to see the trends that might appear in the results. I have highlighted in green values for *a* which do not share a common factor (relatively prime) with 4. These highlighted values (3,7, and 11) are ones that do not work, despite not sharing factors. The natural numbers 5 and 9 do work with Fermat's modified Little Theorem using a composite numbers rather than a prime value. Also, I should add that although Table 13 is limited to the natural numbers 2-11, factorizations allow us to predict results beyond these numbers. One can observe the repeated pattern of {3, 2, 3, 0} in the third column and {2, 2, 0, 0} in the sixth column. Still, it can be stated that the Little Theorem does not work consistently with a composite value rather than a prime for *p*.

Table 13. Mod 4

	a^(p-1)-1	mod 4		a^p-a	mod 4
2^(4-1)-1	**7**	3	**2^4-2**	14	2
3^(4-1)-1	**26**	2	**3^4-3**	78	2
4^(4-1)-1	**63**	3	**4^4-4**	252	0
5^(4-1)-1	**124**	0	**5^4-5**	620	0
6^(4-1)-1	**215**	3	**6^4-6**	1,290	2
7^(4-1)-1	**342**	2	**7^4-7**	2,394	2
8^(4-1)-1	**511**	3	**8^4-8**	4,088	0

	a^(p-1)-1	mod 4		a^p-a	mod 4
9^(4-1)-1	**728**	0	**9^4-9**	6,552	0
10^(4-1)-1	**999**	3	**10^4-10**	9,990	2
11^(4-1)-1	**1,330**	2	**11^4-11**	14,630	2

In Table 14 below are the results for modulo 6. Again, the relatively prime value 5 does not work, but the value 7 does. Because of it only work for one of two candidates, it confirms that a modified Little Theorem does not generate the expected results as it did with the prime moduli.

Table 14. Mod 6

	a^(p-1)-1	mod 6		a^p-a	mod 6
2^(6-1)-1	**31**	1	**2^6-2**	62	2
3^(6-1)-1	**242**	2	**3^6-3**	726	0
4^(6-1)-1	**1,023**	3	**4^6-4**	4,092	0
5^(6-1)-1	**3,124**	4	**5^6-5**	15,620	2
6^(6-1)-1	**7,775**	5	**6^6-6**	46,650	0
7^(6-1)-1	**16,806**	0	**7^6-7**	117,642	0
8^(6-1)-1	**32,767**	1	**8^6-8**	262,136	2
9^(6-1)-1	**59,048**	2	**9^6-9**	531,432	0
10^(6-1)-1	**99,999**	3	**10^6-10**	999,990	0

In Table 15 below are the results for modulo 8. The numbers that are relatively prime to 8 are: 3, 5, 7, 9, and 11. Of those 5 natural numbers, only 9 works.

Table 15. Mod 8

	a^(p-1)-1	mod 8		a^p-a	mod 8
2^(8-1)-1	**127**	7	**2^8-2**	254	6
3^(8-1)-1	**2,186**	2	**3^8-3**	6,558	6
4^(8-1)-1	**16,383**	7	**4^8-4**	65,532	4
5^(8-1)-1	**78,124**	4	**5^8-5**	390,620	4
6^(8-1)-1	**279,935**	7	**6^8-6**	1,679,610	2
7^(8-1)-1	**823,542**	6	**7^8-7**	5,764,794	2
8^(8-1)-1	**2,097,151**	7	**8^8-8**	16,777,208	0
9^(8-1)-1	**4,782,968**	0	**9^8-9**	43,046,712	0

	a^(p-1)-1	mod 8		a^p-a	mod 8
10^(8-1)-1	9,999,999	7	10^8-10	99,999,990	6
11^(8-1)-1	19,487,170	2	11^8-11	214,358,870	6
12^(8-1)-1	35,831,807	7	12^8-12	429,981,684	4

In Table 16 showing the results for modulo 10, based on the condition that *a* must not have any common factors other than 1, the natural numbers 3, 7, 9, and 11 are expected to work, yet only 11 results in 0 (mod 10).

Table 16. Mod 10

	a^(p-1)-1	mod 10		a^p-a	mod 10
2^(10-1)-1	511	1	2^10-2	1,022	2
3^(10-1)-1	19,682	2	3^10-3	59,046	6
4^(10-1)-1	262,143	3	4^10-4	1,048,572	2
5^(10-1)-1	1,953,124	4	5^10-5	9,765,620	0
6^(10-1)-1	10,077,695	5	6^10-6	60,466,170	0
7^(10-1)-1	40,353,606	6	7^10-7	282,475,242	2
8^(10-1)-1	134,217,727	7	8^10-8	1,073,741,816	6
9^(10-1)-1	387,420,488	8	9^10-9	3,486,784,392	2
10^(10-1)-1	999,999,999	9	10^10-10	9,999,999,990	0
11^(10-1)-1	2,357,947,690	0	11^10-11	25,937,424,590	0
12^(10-1)-1	5,159,780,351	1	12^10-12	61,917,364,212	2

Another way to show how composite moduli differ from prime moduli can be observed in the multiplication tables for those moduli. Below are the multiplication tables for moduli 4, 6, 8, and 10. With the prime moduli, all the values 1 through (p-1) show up in varied order without any products yielding a 0 (mod *p).* However, in the composite moduli zeroes occur with regular frequency. Also, there are columns and rows that have only repeating values and not all values as occur with primes.

Table 17. Mod 4

x	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Table 18. Mod 6

x	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Table 19. Mod 8

x	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Table 20. Mod 10

x	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	0	2	4	6	8
3	3	6	9	2	5	8	1	4	7
4	4	8	2	6	0	4	8	2	6
5	5	0	5	0	5	0	5	0	5
6	6	2	8	4	0	6	2	8	4
7	7	4	1	8	5	2	9	6	3
8	8	6	4	2	0	8	6	4	2
9	9	8	7	6	5	4	3	2	1

Next I will discuss if the Theorem will work with a composite number *p* and **any *a*** that does not share a common factor with *p* other than 1.

As I have said, the Little Theorem does not work consistently with a composite *p* as it does with a prime *p.* However, Euler contributed to Fermat's observation and Theorem. This contribution has come to be known as the Totient Theorem. Euler's Totient Theorem is grounded in the idea of identifying relatively prime numbers. Specifically, the Totient Function is a tool to generate the quantity of relatively prime numbers for any given natural number.

Euler's totient function is represented by the symbol $\phi(m)$, where *m* is the given natural number and the result is the number of relative prime numbers. If *m* is a prime, then $\phi(m)$= *p* - 1. It is so because for any given prime number, the resulting residue is {1, ..., p-1}, and a prime is only divisible by 1 and itself.

For composite numbers, Euler's totient function yield a residue ring of the numbers relatively prime to a given number. In the instance of modulo 8, given below in Tables 21 and 22, Euler creatively gets around the limitations of Fermat's Little Theorem by reducing the residue to {1, 3, 5, 7}. Euler's totient theorem, generalizing Fermat's idea, is stated as $a^{\phi(m)} \equiv 1$ (mod *m*), where z(*m*) is the reduced residue.

Table 21. Mod 8

x	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Table 22. Reduced Residue, Mod 8

x	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Using a similar method as was used with Fermat's Little Theorem accounted by both Pommersheim (2010) and Ore (1948), this reduced residue of {1, 3, 5, 7} constrains one only to choose an *a* that is relatively prime to 8. Furthermore, the pattern of results has all the values 1-7 without zeroes as was true for the prime moduli. To illustrate this, I have picked the integer 5:

$$(5*1)*(5*3)*(5*5)*(5*7)=1*3*5*7(\bmod 8)$$

$$(5*5*5*5)*(1*3*5*7)=1*3*5*7(\bmod 8)$$

[the 5's can be rewritten using exponents]

$$5^4*(1*3*5*7)=1*3*5*7(\bmod 8)$$

[(dividing the left side by (1*3*5*7) becomes]

$$5^4=1(\bmod 8)$$

Using Table 23 below (highlighted in red), you will see that this result, $5^4=1(\bmod 8)$, is indeed shown to be true.

Table 23. Exponents in Mod 8

	1	2	3	4	5	6	7
a^1	1	2	3	4	5	6	7
a^2	1	4	1	0	1	4	1
a^3	1	0	3	0	5	0	7
a^4	1	0	1	0	1	0	1
a^5	1	0	3	0	5	0	7
a^6	1	0	1	0	1	0	1
a^7	1	0	3	0	5	0	7
a^8	1	0	1	0	1	0	1

Additionally, in constraining the table to only include a residue of relatively prime numbers, Euler's Totient Theorem will work for **any *a*** that does not share a common factor with 8 other than 1.

Table 25. Exponents in Mod 8, reduced residue only

	1	**3**	**5**	**7**
a^1	1	3	5	7
a^2	**1**	**1**	**1**	**1**
a^3	1	3	5	7
a^4	**1**	**1**	**1**	**1**
a^5	1	3	5	7
a^6	**1**	**1**	**1**	**1**
a^7	1	3	5	7
a^8	**1**	**1**	**1**	**1**

Here is an example of Euler's totient theorem, and it satisfies the conditions that a composite number *p* is used and the natural number *a* does not share a common factor with *p* other than 1.

$a^{\phi(m)} \equiv 1(\bmod m)$

$a = 3, \phi(m) = 8$

$3^{\phi(8)} \equiv 1$ (mod 8)

$\phi(8) = \{1,3,5,7\} = 4$

$3^4 \equiv 1$ (mod 8)

$81 \equiv 1$ (mod 8)

To continue my illustration of the Totient Theorem, I chose 15 for the integer *a.* It being the case that I am now working in modulo 8, 15 becomes 7 (mod 8). Just as before, the Theorem stands true. 15 is relatively prime to 8, as is 7 (mod 8).

$a^{\phi(m)} \equiv 1(\bmod m)$

$a = 15, \phi(m) = 8$

$$a = 15 = 7(\bmod 8)$$
$$7^{\phi(8)} \equiv 1(\bmod 8)$$
$$\phi(8) = \{1,3,5,7\} = 4$$
$$7^4 \equiv 1(\bmod 8)$$
$$7^4 = 2401 = 1(\bmod 8)$$

In fact, working in mod 8, any relatively prime number beyond 8 converts to 1, 3, 5, or 7:

$$9 \equiv 1(\bmod 8)$$
$$11 \equiv 3(\bmod 8)$$
$$13 \equiv 5(\bmod 8)$$
$$15 \equiv 7(\bmod 8)$$
$$17 \equiv 1(\bmod 8)$$
$$19 \equiv 3(\bmod 8)$$
$$21 \equiv 5(\bmod 8)$$
$$23 \equiv 7(\bmod 8)$$
$$25 \equiv 1(\bmod 8)$$
$$27 \equiv 3(\bmod 8)$$
$$29 \equiv 5(\bmod 8)$$
$$31 \equiv 7(\bmod 8)$$

...et cetera. Thus, so long as the natural number is relatively prime to 8, regardless of being prime or composite, the number becomes {1, 3, 5, 7} in modulo 8. Furthermore, as has been shown in Table 25, this will produce a remainder of 1 in modulo 8.

References:

Bogomolny, A. (2000). Euclid's Algorithm. In *Interactive Mathematics Miscellany and Puzzles*. Retrieved on May 31, 2010, from http://www.cut-the-knot.org/blue/Euclid.shtml

Bogomolny, A. (2000). Fermat's Little Theroem. In *Interactive Mathematics Miscellany and Puzzles*. Retrieved on June 11, 2010 from http://www.cut-the-knot.org/blue/Fermat.shtml

Bogomolny, A. (2000). Euler Function and Theorem. In *Interactive Mathematics Miscellany and Puzzles*. Retrieved on June 11, 2010 from http://www.cut-the-knot.org/blue/Euler.shtml

Caldwell, C. (1994). Proof of Fermat's Little Theorem. In *Prime Pages.* Retrieved on June 13, 2010, from http://primes.utm.edu/notes/proofs/FermatsLittleTheorem.html

Caldwell, C. (1994). Sieve of Eratosthenes. In *Prime Pages.* Retrieved on June 13, 2010, from http://primes.utm.edu/glossary/page.php?sort=SieveOfEratosthenes

O'Connor, J. & Robertson, E. (1998). Eratosthenes of Cyrene. In *The MacTutor History of Mathematics archive*. Retrieved on August 13, 2011, from http://www.gap-system.org/~history/Biographies/Eratosthenes.html

O'Connor, J. & Robertson, E. (1998). Carl Friedrich Gauss. In *The MacTutor History of Mathematics archive*. Retrieved on August 13, 2011, from http://www.gap-system.org/~history/Biographies/Gauss.html

O'Connor, J. & Robertson, E. (1998). Leonhard Euler. In *The MacTutor History of Mathematics archive*. Retrieved on August 13, 2011, from http://www.gap-system.org/~history/Biographies/Euler.html

Ore, O. (1948). Number Theory and Its History. New York, NY: McGraw-Hill Book Company, Inc.

Stevenson, F. (2000). Exploring the Real Numbers. Upper Saddle River, NJ: Prentice-Hall, Inc.

Pommersheim, J., Marks, T., & Flapan, E. (2010). Number Theory. Hoboken, NJ: John Wiley & Sons, Inc.

Reed, I. (1998). The Beginnings of Topology. In *The Math Forum @ Drexel [University].* Retrieved on August 13, 2011, from http://mathforum.org/isaac/problems/bridges1.html

Weisstein, E. (1995). Fermat's Little Theorem. In Wolfram Mathworld. Retreived on June 25, 2010, from http://mathworld.wolfram.com/FermatsLittleTheorem.html

Weisstein, E. (1995). Totient Function. In Wolfram Mathworld. Retreived on June 25, 2010, from http://mathworld.wolfram.com/TotientFunction.html