ON FERMAT'S LITTLE THEOREM

ROBERT E. BISHOP

ABSTRACT. A new proof of Fermat's Little Theorem is presented. A brief history of this theorem is presented to both provide historical context and to show the new proof adds to the body of knowledge surrounding the theorem in a meaningful way. The new proof is discussed in the context of Euler's classic proof and an intuitive combinatorial proof.

1. Brief History of Fermat's Little Theorem

Pierre de Fermat first wrote what would become his "Little Theorem" in 1679. As was typical of Fermat, he did not include a proof for fear the proof would be too long [1]. The first proof of this theorem was published more than fifty years later by Leonhard Euler, in 1736 [1]. Using the modular arithmetic notation published by Johann Carl Friedrich Gauss in 1801[1], Euler's proof can be presented in a shorter and simpler fashion. Euler's proof using modular arithmetic notation is presented in this paper as the classical proof of Fermat's Little Theorem. Note that even though the notation is slightly different, the basis of Euler's original proof is unchanged in the proof presented in this paper.

In this paper, it is shown that the most modern concept necessary for the proof of Fermat's Little Theorem is either Taylor's theorem, which was published by Brook Taylor in 1717 [2], or the binomial theorem, which was published by Blaise Pascal in 1665 [3] (both theorems lead to the same result in this paper). This is of interest because it shows that mathematicians had the necessary mathematical machinery to prove Fermat's Little Theorem well before Euler published his proof in 1736.

2. New Proof of Fermat's Little Theorem

The proof that follows relies on Taylor's theorem (or the binomial theorem).

Theorem 2.1. *The expression*

$$a^{p-1} - 1 \tag{2.2}$$

is divisible by p, where p is a prime and a is an integer, so long as a is not divisible by p.

Proof. Note that the theorem is trivial for $p = 2$. Thus, consider for some arbitrary odd prime p

$$f(x) = x^{p-1} - 1 \tag{2.3}$$

Using Taylor's theorem, expand $f(x)$ around $x = 1$. This yields

$$f(x) = (p-1)(x-1) + \frac{1}{2!}(p-1)(p-2)(x-1)^2 + \cdots + \frac{1}{(p-1)!}(p-1)!(x-1)^{p-1} \tag{2.4}$$

Date: July 15, 2008.

As a side note, we remark that the series in Equation 2.4 can also be obtained by applying the binomial theorem to the expression

$$(1 + (x - 1))^{p-1} - 1 \tag{2.5}$$

Now consider those values of x divisible by p. For these values of x, $f(x)$ is one less than a multiple of p, and thus not divisible by p.

Now consider $x = kp + c$, $k, c \in \mathbb{Z}$ and $0 < c < p$. Note that when we consider Equation 2.3 mod p, we have

$$f(kp + c) \equiv f(c) \mod p \tag{2.6}$$

Thus, we only have to consider values of x in the interval $0 < x < p$. We will now utilize induction to prove the theorem. The base case is $x = 1$. Note that $f(1) = 0$, and thus is divisible by p. Now by induction, suppose $f(n)$ is divisible by p, $0 < n < p - 1$. Thus, $n^{p-1} - 1$ is divisible by p.

Now we will prove that $f(n + 1)$ is divisible by p. Consider $f(n + 1)$, where

$$f(n+1) = (p-1)(n) + \frac{1}{2!}(p-1)(p-2)(n)^2 + ... + \frac{1}{(p-1)!}(p-1)!(n)^{p-1} \tag{2.7}$$

Note that

$$f(n+1) \equiv -n + n^2 - n^3 + ... + n^{p-1} \mod p \tag{2.8}$$

This is due to the fact that

$$\binom{p-1}{k} = \frac{(p-1)...(p-k)}{k!} \equiv (-1)^k \mod p \tag{2.9}$$

Thus, $f(n + 1)$ is congruent to a finite geometric series with a ratio of $-n$. Using the formula for the sum of a geometric series we obtain

$$f(n+1) \equiv \frac{-n + n^p}{1 + n} \mod p \tag{2.10}$$

This factors easily into

$$f(n+1) \equiv \frac{(n)(-1 + n^{p-1})}{1 + n} \mod p \tag{2.11}$$

As $0 < n < p - 1$, $1 + n$ is not divisible by p. By assumption, $n^{p-1} - 1$ is divisible by p, and therefore $f(n + 1)$ is divisible by p. Thus $f(n + 1)$ is divisible by p. This completes the proof by induction. □

3. Classic Proof

A version of this proof was first provided by Euler.

Proof. From the Binomial Theorem, we note that

$$(a + 1)^p \equiv a^p + 1 \mod p \tag{3.1}$$

This is due to the fact that

$$\binom{p}{k} \equiv 0 \mod p \tag{3.2}$$

for $0 < k < p$. Subtract $a + 1$ from both sides of the congruence in Equation 3.1.

$$(a + 1)^p - (a + 1) \equiv a^p - a \mod p \tag{3.3}$$

Thus, we note that if $a^p - a$ is divisible by p, then so also must $(a + 1)^p - (a + 1)$ be divisible by p.

Clearly, $1^p - 1$ is divisible by p. Now by induction, suppose that $n^p - n$ is divisible by p. Note that Equation 3.3 then implies that $(n+1)^p - (n+1)$ is divisible by p, which completes the induction. This gives the general statement

$$a^p \equiv a \mod p \tag{3.4}$$

We can multiply both sides of Equation 3.4 by the multiplicative inverse of a mod p to obtain the classical statement:

$$a^{p-1} \equiv 1 \mod p \tag{3.5}$$

□

4. Combinatorial Proof

This proof is intuitive and requires less mathematics than the two previous proofs. It is based upon the concept of bracelets.

Proof. First, we consider an alphabet with a distinct symbols, and we then consider all possible strings of symbols of length p. Clearly, there are a^p distinct strings. For concreteness, we will use $p = 5$ and $a = 2$ for an example. Thus, we can let the alphabet be {A,B}, and there are clearly $2^5 = 32$ possible strings.

AAAAB	AAABA	AABAA	ABAAA	BAAAA
AABAB	ABABA	BABAA	ABAAB	BAABA
AAABB	AABBA	ABBAA	BBAAA	BAAAB
AABBB	ABBBA	BBBAA	BBAAB	BAABB
ABABB	BABBA	ABBAB	BBABA	BABAB
ABBBB	BBBBA	BBBAB	BBABB	BABBB
AAAAA				
BBBBB				

Now we bring the ends of each string together to create bracelets. Note that for a fixed string $x_0, \ldots, x_{p-1}$, the set of strings that determine the same bracelet as that string (excluding the string itself) is $\{x_k, \ldots, x_{p-1}, x_0, \ldots, x_{k-1} \mid 1 \leq k \leq p-1\}$. For example, each row above consists of strings which determine the same bracelet.

Now, we claim that for each non-constant string $x_0, \ldots, x_{p-1}$, there are precisely p strings that determine the same bracelet (including itself). Suppose for contradiction that a rotation by k, $0 < k < p$, yields the original bracelet. Then it follows that $x_0 = x_k = x_{2k} = \ldots = x_{(p-1)k}$. Here $x_{tk} := x_r$ for the unique r such that $0 \leq r \leq p-1$ and $tk \equiv r \bmod p$. Since p is prime, we note that as t takes on all values from $0 \leq t \leq p-1$, r takes on all values in the interval $0 \leq r \leq p-1$. Thus, the string is constant, which is a contradiction.

We also note that there are precisely a strings which are constant, such as AAAAA and BBBBB. Thus, there are $a^p - a$ non-constant strings. We know that we can partition these strings into groups of size p, and thus $a^p - a$ is divisible by p. This implies that

$$a^p \equiv a \mod p \tag{4.1}$$

For a not divisible by p, this is clearly

$$a^{p-1} \equiv 1 \mod p \tag{4.2}$$

□

5. Concluding Remarks

In this paper, we have presented an original proof of Fermat's Little Theorem. The significance of this proof lies in the fact that it relies only on mathematical techniques older than either the statement of the theorem by Fermat or the first proof by Euler, but was not discovered until now. In other words, the proof is not the result of more modern mathematical tools, but rather was perfectly accessible to mathematicians at the time of Fermat, and certainly to those in the more than fifty years that elapsed between the statement by Fermat and the proof by Euler. We then compared this new proof to the proof by Euler, and to an intuitive proof based on the concepts of strings and bracelets. This provided context in which to view the new proof.

6. Acknowledgements

The author would like to thank Burton Newman for his close reading of the paper and his useful comments.

References

[1] Oystein Ore. Number Theory and its History. Dover Publications. 1976.
[2] Brook Taylor. Methodus Incrementorum Directa et Inversa. Impensis Gulielmi Innys, 1717.
[3] Blaise Pascal. Traite du Triangle Arithmetique, Avec Quelques Autres Petits Traitez Sur la Mesme Matiere. Guillaume Desprez, 1665.