# SELECTED PROOFS OF FERMAT'S LITTLE THEOREM AND WILSON'S THEOREM

By

CAROLINE LAROCHE TURNAGE

A Thesis Submitted to the Graduate Faculty of

WAKE FOREST UNIVERSITY

in Partial Fulfillment of the Requirements

for the Degree of

MASTER OF ARTS

in the Department of Mathematics

May 2008

Winston-Salem, North Carolina

Approved By:

Fredric T. Howard, Ph.D., Advisor _____

Examining Committee:

Stephen B. Robinson, Ph.D., Chairperson _____

Kenneth S. Berenhaut, Ph.D. _____

Hugh N. Howards, Ph.D. _____

# Table of Contents

# Acknowledgements

The completion of this thesis would not have been possible without the help and support of many people including faculty, friends, and family.

I would first like to extend great thanks to my entire thesis committee. Each has taught me so much about the kind of professor I would like to become. I give my utmost thanks to my advisor, Dr. Fredric Howard, for his support and uplifting motivation throughout my time here at Wake Forest. He has pushed me to realize my capabilities, which he assuredly reminds me of whenever I am in doubt. I am obliged for all of his advice and genuine care, and I hope that one day I can help a student in the tremendous ways he has helped me. I would also like to thank Dr. Stephen Robinson for his inspirational teaching style, Dr. Hugh Howards for his infectious enthusiasm, and Dr. Kenneth Berenhaut for his sincere care. I also thank Dr. Charlotte Knotts-Zides of Wofford College for always believing in me and pushing me to never give up.

Special thanks go to my fellow graduate students for their humor and guidance. We all had the same task of getting past the storm, and we always worked together to help each other through. In particular I would like to thank Jessie Penley for her friendship, laughter, and optimism.

My final thanks go to those who have constantly supported me: my family. My mother Beverley has always believed in me and supported me in my decisions, and I thank her for showing me the kind of woman I am striving to become. I thank my father Wes for all of his support and for constantly reminding me that he is proud of me no matter what. Finally, I want to thank my fiancé Ian for all of his love and selflessness throughout my two years at Wake Forest. He has been a source of motivation and inspiration, and I cherish that he will always be by my side.

I am truly blessed to have so many people to thank because they have all contributed to my well-being and success. I am forever grateful to you all.

# Abstract

Thesis under the direction of Fredric T. Howard, Ph.D., Professor of Mathematics.

Fermat's Little Theorem and Wilson's Theorem are two of the most famous and useful theorems in mathematics. They are found in many realms, however in this thesis we concentrate on them with respect to number theory and combinatorics. We will focus on the early proofs of both theorems and their generalizations, and then provide more recent combinatorial proofs.

# Chapter 1: Introduction

In this thesis we study some of the early proofs of Fermat's Little Theorem and Wilson's Theorem. Our main reference is *History of the Theory of Numbers, Volume 1* by L.E. Dickson. Because many of the original sources to the proofs of these theorems are obscure, we usually refer the reader to Dickson. The sequence of the proofs appears chronologically, in order to display how the proofs evolved throughout the 17th-20th centuries.

One of our main goals is to take sketchy, incomplete proofs outlined in Dickson and fill in the missing details. We do, however, try to retain the original flavor of the proofs with respect to notation and terminology. Another goal is to emphasize the great variety of methods that were used to prove the two theorems and their generalizations.

At the end of the thesis we present very recent combinatorial proofs of both theorems, in order to show that they are still being studied and proved in the twenty-first century.

Note: There are four main theorems in this thesis, and they are presented as Theorems 1,2,3, and 4. Each theorem has several proofs. The notation "Proof X.Y" indicates the Y'th proof of theorem X.

## Chapter 2: Preliminary Theorems

Throughout the thesis, many basic theorems and definitions from number theory and combinatorics will be used in the proofs of Fermat's Little Theorem and Wilson's Theorem. Proofs of the major theorems used can be found in most introductory level number theory and combinatorics texts. Proofs of lesser known but important lemmas are provided.

***Definition 1*** *Let $a, b$, and $m$ be integers, with $m > 0$. If $m \mid (a - b)$, then we say $a$ is* ***congruent*** *to $b \pmod{m}$ and we write*

$$a \equiv b \pmod{m}.$$

The concept of congruence was first formally introduced by Gauss in his first chapter of *Disquisitiones Aritmeticae* [9]. He chose the symbol $\equiv$ because of its close similarity with algebraic equality [5, p.65].

***Lemma 1*** *Cancellation Property of Congruences: If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.*

***Lemma 2*** *The Binomial Theorem: If $n$ is a positive integer, then*

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k,$$

*where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.*

***Lemma 3*** *The Multinomial Theorem: If $k_1, k_2, \ldots, k_m$ and $n$ are nonnegative integers such that $n \geq 1$ and $k_1 + k_2 + \cdots + k_m = n$, then*

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{k_1 + k_2 + \cdots + k_m = n} \binom{n}{k_1, k_2, \ldots, k_m} {x_1}^{k_1} {x_2}^{k_2} \cdots {x_m}^{k_m},$$

*where* $\binom{n}{k_1,k_2,\ldots,k_m} = \frac{n!}{k_1!k_2!\cdots k_m!}$.

***Lemma 4*** *The Chinese Remainder Theorem: Let* $m_1, m_2, \ldots, m_r$, *where* $r \geq 2$, *be natural numbers that are pairwise relatively prime and whose product is* $M$. *Then the system of* $r$ *simultaneous linear congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

*has a unique solution* $\pmod{M}$.

***Lemma 5*** *The Division Algorithm: If* $a$ *and* $b$ *are integers such that* $a \geq b > 0$, *then there exist unique integers* $q, r$ *such that* $a = qb + r$ *and* $0 \leq r < b$.

***Lemma 6*** *Let* $v$ *be the order of* $x \pmod{N}$. *That is,* $v$ *is the smallest positive integer such that* $x^v \equiv 1 \pmod{N}$. *Then* $\{ 1, x, x^2, \ldots, x^{v-1} \}$ *are distinct* $\pmod{N}$ *and relatively prime to* $N$.

***Lemma 7*** *Let* $d = \gcd(a, m)$. *If* $d \mid b$, *then* $ax \equiv b \pmod{m}$ *has exactly* $d$ *solutions* $\pmod{m}$.

***Lemma 8*** *If* $a^2 \equiv 1 \pmod{p}$ *and* $\gcd(a, p) = 1$ *then* $a \equiv 1 \pmod{p}$ *or* $a \equiv p - 1 \pmod{p}$.

***Lemma 9*** *If* $p$ *is prime and* $0 < j < p$, *then* $p \mid \binom{p}{j}$.

**Proof** Note that $\binom{p}{j} = \frac{p!}{j!(p-j)!}$. Since $0 < j < p$, there is no $p$ in the denominator of $\binom{p}{j}$, but there is a factor of $p$ in the numerator. Thus $\binom{p}{j} \equiv 0 \pmod{p}$ which implies $p \mid \binom{p}{j}$. □

***Lemma 10*** *If $p$ is a prime and $1 \leq k \leq p-1$, then $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$.*

**Proof by Induction** Let $S = \{\, k \mid \binom{p-1}{k} \equiv (-1)^k \pmod{p} \,\}$. Note that $1 \in S$ since $\binom{p-1}{1} = p - 1 \equiv -1 \pmod{p}$. Now assume that $k - 1 \in S$. Then $\binom{p-1}{k-1} \equiv (-1)^{k-1} \pmod{p}$. By Pascal's Identity,

$$\binom{p-1}{k} = \binom{p}{k} - \binom{p-1}{k-1}.$$

Thus we have

$$\binom{p-1}{k} \equiv -\binom{p-1}{k-1} \equiv (-1)(-1)^{k-1} \pmod{p} \equiv (-1)^k \pmod{p}.$$

Thus $k \in S$. □

***Lemma 11*** *Let $\gcd(r, n) = 1$ and let $r_1, r_2, \ldots, r_{\Phi(n)}$ be the positive integers less than $n$ and relatively prime to $n$. If $r$ is a primitive root of $n$, then $r, r^2, \ldots, r^{\Phi(n)}$ are congruent modulo $n$ to $r_1, r_2, \ldots, r_{\Phi(n)}$ in some order [4, p.154].*

***Lemma 12*** *An integer $n > 1$ has a primitive root if and only if $n = 2, 4, p^e$, or $2p^e$, where $p$ is an odd prime.*

***Lemma 13*** *Euler's Formula: Let $a$ and $n$ be nonnegative integers with $a \geq n$. Then*

$$n! = a^n - \binom{n}{1}(a-1)^n + \binom{n}{2}(a-2)^n - \binom{n}{3}(a-3)^n + \cdots + (-1)^n \binom{n}{n}(a-n)^n.$$

Euler originally proved this formula by induction. The following proof uses the Principle of Inclusion-Exclusion and is original:

***Proof (Howard and Turnage, 2007)*** First, count the number of different ways to put $n$ distinguishable objects into $a$ distinguishable cells, with none of the first $n$ cells being empty and $n \leq a$. Then there are $n$ choices for cell 1, $n - 1$ choices for cell 2, etc. Thus there are $n!$ ways to put these objects into cells. Now let us find the answer in another way.

First, let the universal set $U$ be all the distributions of $n$ distinguishable objects into $a$ distinguishable cells with no restrictions. Then $|U| = a^n$, since for each of the $n$ objects, there are $a$ choices for a cell.

Let $P_i$ be the property that the $i$'th cell is empty. Using the Principle of Inclusion-Exclusion, we want the number of distributions of the objects into the cells not having any of the properties $P_1, P_2, \ldots, P_n$. Let $N(P_i')$ be the number of distributions not having property $P_i$ and $N(P_i)$ be the number of distributions having the property $P_i$. Then the Principle of Inclusion-Exclusion gives

$$N(P_1'P_2'\cdots P_n') = a^n - \sum N(P_i) + \sum N(P_iP_j) - \sum N(P_iP_jP_k) + \cdots + (-1)^n N(P_1P_2\cdots P_n).$$

First we determine $\sum N(P_i)$. There are $\binom{n}{1}$ ways to select one of the cells to be empty (i.e. to select one of the properties) and then there are $(a-1)^n$ ways to distribute the $n$ objects in the remaining $a-1$ cells. Thus $\sum N(P_i) = \binom{n}{1}(a-1)^n$.

Similarly, $\sum N(P_iP_j) = \binom{n}{2}(a-2)^n$, $\sum N(P_iP_jP_k) = \binom{n}{3}(a-3)^n$, and so on. Thus in general for $k = 1, 2, \ldots, n$, there are $\binom{n}{k}$ ways to choose $k$ of the properties and then $(a-k)^n$ ways to distribute the $n$ objects into the remaining $(a-k)$ cells. Thus

$$N(P_1'P_2'\cdots P_n') = a^n - \binom{n}{1}(a-1)^n + \binom{n}{2}(a-2)^n - \cdots + (-1)^n\binom{n}{n}(a-n)^n,$$

and it follows that

$$n! = a^n - \binom{n}{1}(a-1)^n + \binom{n}{2}(a-2)^n - \cdots + (-1)^n\binom{n}{n}(a-n)^n.$$

Thus we have established Euler's Formula. □

## Chapter 3: Early Proofs of Fermat's Little Theorem

***Theorem 1*** *(Fermat's Little Theorem) If $p$ is a prime and $\gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.*

In a letter to Bernhard Frénicle de Bessy dated October 18, 1640, Pierre de Fermat first revealed his result stated above. He did not, however, provide a proof, stating to Frénicle, "I would send you the demonstration, if I did not fear its being too long"[5]. The first proof of Fermat's Little Theorem was given nearly 100 years later by Euler. In [5], Burton also tells us that Leibniz did not receive this recognition, "for he left an identical argument in an unpublished manuscript sometime before 1683."

The following proof is given in Beginning Number Theory by Neville Robbins [13, p.102]. It is a proof found in many number theory textbooks, and we see later that it is essentially equivalent to Euler's first two proofs.

***Proof 1.1*** Let $S = \{\ a \mid a^p \equiv a \pmod{p}\ \}$ for $p$ prime and $a \in \mathbf{N}$. Then $0 \in S$ because $0^p = 0$ for all $p$ so $0^p \equiv 0 \pmod{p}$. Now assume $k \in S$ and $k^p \equiv k \pmod{p}$. We want to show that for $k+1 \in S$, $(k+1)^p \equiv (k+1) \pmod{p}$. By the Binomial Theorem,

$$\begin{aligned}(k+1)^p &= k^p + 1^p + \sum_{j=1}^{p-1} \binom{p}{j} k^{p-j} \\ &\equiv k+1 \pmod{p}.\end{aligned}$$

If $\gcd(a,p) = 1$, then by cancellation $a^p \equiv a \pmod{p}$ implies $a^{p-1} \equiv 1 \pmod{p}$. If $a$ is negative, then $a \equiv r \pmod{p}$ for some $r$, where $0 \leq r \leq p-1$. Thus $a^p \equiv r^p \equiv r \equiv a \pmod{p}$. □

In Dickson's History of the Theory of Numbers [7, Chapter 3], the original works to prove Fermat's Little Theorem are given. Among these proofs, works by Leibniz, Euler, Lambert, Ivory, and Thue are inlcuded. We use [7, Chapter 3] as a general reference for this chapter.

The following proof was given by G.W Leibniz (1646-1716).

***Proof 1.2 (Leibniz, 1680)*** Let $p$ be a prime and let $x = a_1 + a_2 + \cdots + a_m$.

Consider $x^p - \sum_{i=1}^{m} {a_i}^p$. We will show that $p \mid (x^p - \sum_{i=1}^{m} {a_i}^p)$.
By the Multinomial Theorem,

$$x^p = (a_1 + a_2 + \cdots + a_m)^p = \sum_{k_1+\cdots+k_m=p} \binom{p}{k_1, k_2, \ldots, k_m} {a_1}^{k_1} \cdot {a_2}^{k_2} \cdots {a_m}^{k_m}.$$

Note that $\binom{p}{k_1,k_2,\ldots,k_m} = \frac{p!}{k_1!\cdots k_m!}$. When $k_i \neq p$ for any $i$, then $k_i < p$ for all $i$. Then there is no factor of $p$ in the denominator of any coefficient, but there is a factor of $p$ in the numerator. Thus for $k_i \neq p$ for all $i$, $\frac{p!}{k_1!\cdots k_m!} \equiv 0 \pmod{p}$. Thus

$$x^p - \sum_{i=1}^{m} {a_i}^p \equiv ({a_1}^p + {a_2}^p + \cdots + {a_m}^p) - ({a_1}^p + {a_2}^p + \cdots + {a_m}^p) = 0 \pmod{p}.$$

Thus $p \mid (x^p - \sum_{i=1}^{m} {a_i}^p)$.

Take $a_1 = a_2 = \cdots = a_m = 1$. Then since $x = a_1 + a_2 + \cdots + a_m$, it follows that $p \mid (x^p - x)$ for any integer $x$ (depending on the value of $m$). Thus $x^p - x \equiv 0 \pmod{p}$, so $x^p \equiv x \pmod{p}$. If $\gcd(x, p) = 1$, then by cancellation $x^{p-1} \equiv 1 \pmod{p}$. □

L. Euler (1707-1783) gave the following three proofs of Fermat's Little Theorem which are included in Dickson.

***Proof 1.3 (Euler, 1736)*** Let $p$ be prime. By the Binomial Theorem,

$$\begin{aligned} 2^p = (1+1)^p &= \binom{p}{0} + \binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-1} + \binom{p}{1} \\ &= 1 + p + \binom{p}{2} + \cdots + p + 1 \\ &= 2 + pm \end{aligned}$$

for some $m \in \mathbb{Z}$ since $p \mid \binom{p}{j}$ for $1 \leq j \leq p-1$.

Similarly, $3^p = (1+2)^p = 1 + 2^p + kp$, for some $k \in \mathbb{Z}$ since each other coefficient has a factor of $p$. Then $3^p - 1 - 2^p = kp$, so adding and subtracting 2 on the left side, we have $3^p - 3 - (2^p - 2) = kp$. In general we have, $(1+a)^p = 1 + a^p + np$ for some $n \in \mathbb{Z}$. Thus $(1+a)^p - 1 - a^p = np$ and by adding and subtracting $a$ on the left side, we have

$$(1+a)^p - (1+a) - (a^p - a) = np.$$

Thus $(1+a)^p - (1+a) = (a^p - a) + np$ for some $n \in \mathbb{Z}$. If $p$ divides $a^p - a$, then $p$ divides $(1+a)^p - (1+a)$. We have shown for $a = 2$, $p$ divides $a^p - a$. Thus for $a > 2$, consider $a+1$. Assume $p$ divides $(a+1)^p - (a+1)$. Then $p$ divides $(a+1+1)^p - (1+1+a) = (a+2)^p - (a+2)$. Then if $p$ divides $(a+2)^p - (a+2)$, then $p$ divides $(a+2+1)^p - (a+2+1) = (a+3)^p - (a+3)$. Continuing inductively, we see that $p$ divides $x^p - x$ for all $x \in \mathbb{Z}$. Thus $x^p - x \equiv 0 \pmod{p}$, so $x^p \equiv x \pmod{p}$. If $\gcd(x, p) = 1$, by cancellation, $x^{p-1} \equiv 1 \pmod{p}$. □

Note that the next proof is essentially the same as Proof 1.1:

***Proof 1.4 (Euler, 1747)*** Let $a, b \in \mathbb{Z}$, and let $p$ be prime. Then $(a+b)^p - a^p - b^p$ is divisible by $p$, for:

$$(a+b)^p - a^p - b^p = a^p + b^p + \sum_{j=1}^{p-1} \binom{p}{j} a^{p-j} b^j - a^p - b^p \equiv 0 \pmod{p}.$$

Then if $a^p - a$ and $b^p - b$ are divisible by $p$, then $(a+b)^p - a - b$ is divisible by $p$, for:

$$(a+b)^p - a - b \equiv a^p - a + b^p - b \equiv 0 \pmod{p}.$$

Take $b = 1$. Then $(a+1)^p - a - 1$ is divisible by $p$ if $a^p - a$ is divisible by $p$ by the reasoning above. Then since $(a+1)^p - (a+1)$ is divisible by $p$, $(a+2) - a - 2$ is divisible by $p$. Then since $(a+2)^p - (a+2)$ is divisible by $p$, $(a+3)^p - a - 3$ is divisible by $p$. Continuing inductively in the manner and letting $a = 1$, we see that $p$ divides $x^p - x$ for all $x \in \mathbb{Z}$. Thus $x^p - x \equiv 0 \pmod{p}$, so $x^p \equiv x \pmod{p}$. If $\gcd(x, p) = 1$, then by cancellation $x^{p-1} \equiv 1 \pmod{p}$. □

***Proof 1.5 (Euler, 1758)*** Let $p$ be prime, $a \in \mathbb{Z}$, and $\gcd(a, p) = 1$. Consider the set $\{ 1, a, a^2, \ldots, a^r \}$ where $r \in \mathbb{Z}$. There are $p - 1$ positive residues less than $p$ that are distinct. Let $a^m$ and $a^n$ have the same residue $\pmod{p}$, for $m > n$. Then $a^m \equiv a^n \pmod{p}$. Then cancelling out $a^n$ on both sides of the congruence, we have $a^{m-n} \equiv 1 \pmod{p}$, so $p$ divides $a^{m-n} - 1$. Let $t$ be the least integer for which $a^t - 1$ is divisible by $p$, i.e. let $t$ be the order of $a \pmod{p}$. Then the set $\{ 1, a, a^2, \ldots, a^{t-1} \}$ has distinct residues $\pmod{p}$. Thus $t \leq p - 1$. If $t = p - 1$, we're done. If $t < p - 1$, then there exists a positive integer $k$ (for $k < p$) which is not the residue of a power of $a$. Then the set $\{ k, ak, a^2k, \ldots, a^{t-1}k \}$ has distinct residues, where no one is the residue of a power of $a \pmod{p}$:

(Proof by Contradiction. Assume $ka^r \equiv ka^s \pmod{p}$ for $r > s$ and $r, s \leq t - 1$. Then $a^r \equiv a^s \pmod{p}$ and $a^{r-s} \equiv 1 \pmod{p}$ by cancellation. Since $r \neq s$, it follows that $r - s \neq 0$. Since $r, s \leq t - 1$, $r - s < t$, but $t$ is the order of $a$. Thus we have a contradiction.)

Consider both sets $\{ 1, a, a^2, \ldots, a^{t-1} \}$ and $\{ k, ak, a^2k, \ldots, a^{t-1}k \}$. These sets give $2t$ distinct residues $\pmod{p}$, so $2t \leq p - 1$. If $t = \frac{p-1}{2}$, then $t \mid (p-1)$. If $t < \frac{p-1}{2}$, we

start with a new integer $s$ and see that $\{ s, as, a^2s, \ldots, a^{t-1}s \}$ has distinct residues, no one a power of $a$ or $ka^m$. Hence $3t \leq p-1$, so $t \leq \frac{p-1}{3}$. Proceeding in this manner, since $t \leq p-1$, eventually $t$ divides $p-1$. Thus $p-1 = tm$ for some $m \in \mathbb{Z}$, so $a^{p-1} = a^{tm}$. Thus $a^{p-1} \equiv a^{tm} \pmod{p}$, so $a^{p-1} \equiv a^{tm} \equiv (a^t)^m \pmod{p}$. Thus $a^{p-1} \equiv 1 \pmod{p}$.

Note: In this proof, Euler concludes that $a^{p-1} - 1$ is divisible by $a^t - 1$. This follows because $t \mid (p-1)$, and so we know $p - 1 = tm$ for some $m$.

Then $(a^t - 1)(a^{p-1-t} + a^{p-1-2t} + \cdots + a^{p-1-tm+1} + 1) = a^{p-1} - 1$. □

***Example*** Let $p = 11$ and $a = 10$. Consider the set $\{ 1, 10, 10^2, 10^3, \ldots \}$. There are $11 - 1 = 10$ positive residues less than 11 that are distinct. Note that 10 and $10^3$ have the same residue $\pmod{11}$:

$$10 \equiv 10^3 \pmod{11}.$$

Then by cancellation, we have

$$10^2 \equiv 1 \pmod{11}.$$

Note that 2 is the order of 10 $\pmod{11}$. Then the set $\{ 1, 10 \}$ has distinct residues $\pmod{11}$, so $2 \leq 11 - 1$. Since $2 < 11 - 1$, there exists an integer $k$ such that $k < p$ which is not the residue of a power of 10. Let $k = 2$. Then $\{ 2, 10 \cdot 2 \} \equiv \{ 2, 9 \}$ $\pmod{11}$ has distinct residues, where no one is the residue of a power of 10 $\pmod{11}$. Then $\{ 1, 10 \}$ and $\{ 2, 9 \}$ give $2 \cdot 2 = 4$ distinct residues $\pmod{11}$, so $2 \cdot 2 < 11 - 1$. Thus there exists an integer $s$ such that $s < p$ which is not the residue of a power of 10 or $10^2 \cdot 2$. Let $s = 3$. Then $\{ 3, 10 \cdot 3 \} \equiv \{ 3, 8 \}$ $\pmod{11}$ has distinct residues, where no one is the residue of a power of 10 $\pmod{11}$ or $10^2 \cdot 2$ $\pmod{11}$. We now

have $3 \cdot 2 = 6$ distinct residues, but since $6 < 11 - 1$ there are more to be found. Continuing in this manner we see the sets of distinct residues are as follows:

$$\{1, 10\}, \{2, 9\}, \{3, 8\}, \{4, 7\}, \{5, 6\}.$$

Thus there are $5 \cdot 2 = 10 = 11 - 1$ distinct residues $\pmod{11}$. Thus

$$10^{11-1} = 10^{5 \cdot 2} = (10^2)^5 \equiv 1^5 \equiv 1 \pmod{11}.$$

Johann Heinrich Lambert (1728-1777) gave a proof of Fermat's Little Theorem employing the use of the Binomial Theorem and alternating geometric series:

***Proof 1.6 (Lambert, 1769)*** Let $b = c + 1$ and $\gcd(b, p) = 1$, for $p$ an odd prime. (For $p = 2$, Fermat's Little Theorem follows trivially.) By the Binomial Theorem,

$$\begin{aligned} b^{p-1} - 1 = (c+1)^{p-1} - 1 &= -1 + c^{p-1} + (p-1)c^{p-2} + \binom{p-1}{2} c^{p-3} + \cdots + 1 \\ &= -1 + c^{p-1} - c^{p-2} + c^{p-3} - \cdots - c + 1 + Ap, \end{aligned}$$

say, since $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$; that is $\binom{p-1}{k} = (-1)^k + mp$ for some integer $m$. Since the intermediate terms are an alternating geometric series,

$$c^{p-1} - c^{p-2} + \cdots + 1 = \frac{c^p + 1}{c+1} = c^{p-1} - \frac{c^{p-1} - 1}{c+1}.$$

Thus $b^{p-1} - 1 = c^{p-1} - 1 + Ap - \frac{c^{p-1}-1}{c+1}$. Dividing each side by $p$ we have

$$\frac{b^{p-1} - 1}{p} = \frac{c^{p-1} - 1}{p} + A - \frac{c^{p-1} - 1}{p(c+1)}. \tag{3.1}$$

Since $c < b$, if $p \mid c$, then $c \equiv 0 \pmod{p}$ implies that $b \equiv 1 \pmod{p}$ and $1^{p-1} \equiv 1 \pmod{p}$.

If $p \nmid c$, then using induction on integers relatively prime to $p$, let $S = \{\, x \mid x^{p-1} - 1 \equiv 0 \pmod{p}, p \nmid x \,\}$. Then $1 \in S$ since $1^{p-1} \equiv 1 \pmod{p}$. Assume $c \in S$ such that $c^{p-1} - 1 \equiv 0 \pmod{p}$. Then $\frac{c^{p-1}-1}{p} \in \mathbb{Z}$ and since $\gcd(p, c+1) = 1$ and

$c+1 \mid (c^{p-1}-1)$ we see that $p(c+1) \mid (c^{p-1}-1)$ which implies that $p \mid (b^{p-1}-1)$. Thus it follows from (3.1) that

$$b^{p-1}-1 \equiv (c+1)^{p-1}-1 \equiv 0 \pmod{p}.$$

Thus $c+1 \in S$. □

James Ivory (1764-1842) also contributed a proof of Fermat's Little Theorem. It is the proof that is most commonly given in number theory texts.

***Proof 1.7 (Ivory, 1806)***. Let $n \in \mathbb{Z}$ such that $p \nmid n$. Consider the set $T = \{\, n, 2n, 3n, \ldots, (p-1)n \,\}$ and let S be the set of least positive residues $\pmod{p}$ of the elements of $T$. If $j \in \mathbb{Z}$ and $1 \leq j \leq p-1$, then $p \nmid ja$ and each of the elements of $S$ and $T$ are distinct. Therefore $S$ is a permutation of $\{\, 1, 2, \ldots, (p-1) \,\}$. Then

$$\begin{aligned} \prod_{j=1}^{p-1} nj &\equiv \prod_{j=1}^{p-1} j \pmod{p} \\ n \cdot (2n) \cdot (3n) \cdots (p-1)n &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \\ n^{p-1}(p-1)! &\equiv (p-1)! \pmod{p}. \end{aligned}$$

Since $\gcd((p-1)!, p) = 1$, by cancellation $n^{p-1} \equiv 1 \pmod{p}$. □

Our final proof of Fermat's Little Theorem was given by Axel Thue (1863-1922):

***Proof 1.8 (Thue, 1893)*** Let $p$ be an odd prime. Note that

$$(a-b)^p - (a-b-1)^p = (a-b)^p - [(a-b)-1]^p = \sum_{i=0}^{p-1} (-1)^i \binom{p}{i} (a-b)^i \equiv 1 \pmod{p}.$$

This is because

$$\begin{aligned} [(a-b)-1]^p &= \sum_{i=0}^{p} \binom{p}{i} (a-b)^i (-1)^{p-i} \\ &= (-1)^p \binom{p}{0} (a-b)^0 + (-1)^{p-1} \binom{p}{1} (a-b)^1 + \cdots + (-1)^0 \binom{p}{p} (a-b)^p \end{aligned}$$

and subtracting $(a-b-1)^p$ from $(a-b)^p$ leaves

$$\sum_{i=0}^{p-1}(-1)^i\binom{p}{i}(a-b)^i$$

since $p$ is odd. Now by letting $b = 0, 1, 2, \ldots$ we have for any integer $a$:

$$\begin{aligned}
a^p-(a-1)^p &= 1+h_1p\\
(a-1)^p-(a-2)^p &= 1+h_2p\\
(a-2)^p-(a-3)^p &= 1+h_3p\\
&\vdots\\
2^p-1^p &= 1+h_{a-1}p\\
1^p-0^p &= 1+h_ap
\end{aligned}$$

where $h_i$ is an integer. Then adding up the entries in each column, we have

$$a^p = a+hp$$

where $h = h_1+h_2+\cdots+h_a$. Thus we can conclude that $p \mid (a^p-a)$. □

# Chapter 4: A Generalization of Fermat's Little Theorem

A generalization of Fermat's Little Theorem states that if $n = \Phi(N)$ is the number of positive integers not exceeding $N$ and relatively prime to $N$, then $x^{\Phi(N)} \equiv 1 \pmod{N}$.

**Euler phi-function**

Euler defined the phi-function in 1760. $\Phi(n)$ denotes the number of integers $k$ such that $1 \leq k \leq n$ and $\gcd(k, n) = 1$. The following proofs were first proved by Euler in 1760 and while they are Euler's original work, they have been somewhat modified for clarity. We have used Burton as a guide [5, p.113].

***Lemma 14*** *For integers $a, d, n$, if $\gcd(d, n) = 1$, then the $n$ terms $a, a + d, a + 2d, \ldots, a + (n-1)d$ when divided by $n$ have remainders $0, 1, \ldots, n-1$ in some order, i.e. the least residues $\pmod{n}$ are $0, 1, \ldots, n-1$ in some order.*

**Proof** Consider the set$\{\, a, a+d, a+2d, \ldots, a+(n-1)d \,\}$. Suppose that $a+kd \equiv a+jd \pmod{n}$ for $k, d \in \mathbb{Z}$ such that $0 \leq k < j < n$. Then $kd \equiv jd \pmod{n}$. Since $\gcd(d, n) = 1$, then by cancellation $k \equiv j \pmod{n}$, a contradiction. Thus the numbers in the sequence are congruent to $\{\, 0, 1, \ldots, n-1 \,\}$ in some order. □

***Lemma 15*** $\Phi(p^m) = p^{m-1}(p-1)$

**Proof** Note that $\gcd(n, p^m) = 1$ if and only if $p \nmid n$. There are $p^{m-1}$ integers between 1 and $p^m$ which are divisible by $p$ : $\{\, p, 2p, 3p, \ldots, (p^{m-1})p \,\}$. Thus there

are $p^m - p^{m-1}$ integers between 1 and $p^m$ that are relatively prime to $p^m$. Thus $\Phi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$. □

***Lemma 16*** *The Euler phi-function is multiplicative.*

**Proof** A number-theoretic function is defined to multiplicative if $f(mn) = f(n)f(n)$ whenever $\gcd(m,n) = 1$ [12, p.121]. To show that the phi-function is multiplicative, we must show that for relatively prime $m$ and $n$, $\Phi(mn) = \Phi(m)\Phi(n)$. Since $\Phi(1) = 1$, the result holds if $m$ or $n$ is equal to 1. Thus we will assume that $m, n > 1$. Next, arrange the integers from 1 to $mn$ in $m$ columns of $n$ integers each:

$$\begin{array}{ccccccc} 1 & 2 & \cdots & r & \cdots & m \\ m+1 & m+2 & \cdots & m+r & \cdots & 2m \\ 2m+1 & 2m+2 & \cdots & 2m+r & \cdots & 3m \\ \vdots & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+r & \cdots & nm \end{array} .$$

Since it is true that $\gcd(a,bc) = 1 \Leftrightarrow \gcd(a,b) = 1$ and $\gcd(a,c) = 1$, $\Phi(mn)$ is equal not only to the number of entries above which are relatively prime to $mn$, but also $\Phi(mn)$ is equal to the number of integers relatively prime to both $m$ and $n$. Note that $\gcd(qm + r, m) = \gcd(r, m)$, so for a given column $r$, the entries in that column are relatively prime to $m$ if and only if $r$ is relatively prime to $m$. There are $\Phi(m)$ such columns. Now let $\gcd(r,m) = 1$ for some column $r$. The entries in the $r$th column are

$$r, m+r, 2m+r, \ldots, (n-1)m+r.$$

There are $n$ integers in this sequence and no two are congruent (mod $n$). More explicitly, suppose $sm + r \equiv tm + r \pmod{n}$. Then $sm \equiv tm \pmod{n}$ and by cancellation $s \equiv t \pmod{n}$. This implies that the $r$th column contains as many

integers which are relatively prime to $n$ as does the set $\{ 0, 1, 2, \ldots, n-1 \}$, namely $\Phi(n)$ integers. Thus the total number of integers relatively prime to both $m$ and $n$ is $\Phi(m)\Phi(n)$. □

***Example 1***

$\Phi(945) = \Phi(3^3 \cdot 5 \cdot 7) = 3^2 \cdot 5^0 \cdot 7^0 \cdot (3-1) \cdot (5-1) \cdot (7-1) = 432$

***Example 2***

$$13^{433} \equiv ? \pmod{945}$$

Note that $\gcd(13, 945) = 1$ and from above, $\Phi(945) = 432$. Thus

$$13^{433} = 13^{432} \cdot 13 \equiv 13 \pmod{945}.$$

***Theorem 2*** *(The Generalization of Fermat's Little Theorem) If $n = \Phi(N)$ is the number of positive integers not exceeding $N$ and relatively prime to $N$, then $x^n - 1$ is divisible by $N$ for every integer $x$ relatively prime to $N$.*

We first look at Euler's proof of the generalization [7, p.61].

***Proof 2.1 (Euler, 1760)*** Let $v$ be the order of $x$. Then by Lemma 6, $\{ 1, x, x^2, \ldots, x^{v-1} \}$ are distinct $\pmod{N}$ and relatively prime to $N$. Thus $v \leq \Phi(N)$.

(Proof by Contradiction. Assume $v > \Phi(N)$. Then there are more than $\Phi(N)$ integers that are relatively prime to $N$, a contradiction.)

If $v = \Phi(N)$, we're done. If $v < \Phi(N)$, then there is an additional positive integer $a$ less than $N$ and relatively prime to $N$. Then $\{ a, ax, ax^2, \ldots, ax^{v-1} \}$ are distinct from each other and from the powers of $x$:

(Proof by Contradiction. Assume $ax^m \equiv ax^n \pmod{N}$ for $n < m$. Then $x^{m-n} \equiv 1 \pmod{N}$, a contradiction. If $ax^m \equiv x^n \pmod{N}$, then $a \equiv 1 \pmod{N}$ and we know $\{ 1, x, x^2, \ldots, x^{v-1} \}$ are distinct.)

Thus $2v \leq n$. If $2v = n$, we're done. If not, $3v \leq n$. Continuing in this manner, we see that $v$ divides $\Phi(N)$, which implies $\Phi(N) = vm$ for some integer $m$. Then

$$x^n = x^{vm} = (x^v)^m \equiv 1^m \equiv 1 \pmod{N}.$$

□

Laplace also provided a proof to the generalization [7, p.63]. His statement of the generalization is: *If* $gcd(a, n) = 1$, *then* $a^{\Phi(n)} \equiv 1 \pmod{n}$.

***Proof 2.2 (Laplace, 1776)*** Let $s = {p_1}^{e_1} \cdots {p_k}^{e_k}$ where $p_i \neq p_j$ for $i \neq j$ and each $p_i$ is prime. Let $a \in \mathbb{Z}$ and $\gcd(a, s) = 1$. Let

$$\begin{aligned} v &= \Phi(s) = ({p_1}^{e_1-1}) \cdots ({p_k}^{e_k-1})(p_1 - 1) \cdots (p_k - 1) \\ q &= \Phi({p_1}^{e_1}) = ({p_1}^{e_1-1})(p_1 - 1) \\ r &= ({p_2}^{e_2-1})(p_2 - 1) \cdots ({p_k}^{e_k-1})(p_k - 1). \end{aligned}$$

Then $v = qr = s(\frac{p_1-1}{p_1})(\frac{p_2-1}{p_2}) \cdots (\frac{p_k-1}{p_k})$. Let $x = a^q$. Then $a^v - 1 = a^{qr} - 1 = x^r - 1$, which is divisible by $x - 1$ since

$$(x - 1)(x^{r-1} + x^{r-2} + \cdots + x + 1) = x^r - 1.$$

That is, $a^{\Phi(s)} - 1$ is divisible by $a^{\Phi({p_1}^{e_1})} - 1$. We now show by induction that $x - 1$ is divisible by $p_1^{e_1}$:

First, let $e_1 = 1$. Then $x - 1 = a^q - 1 = a^{{p_1}^{(1-1)}(p_1-1)} - 1 = a^{p_1-1} - 1 \equiv 0 \pmod{p_1}$ by Fermat's Little Theorem. Now assume true for $e_1 - 1$. Then $a^{\Phi({p_1}^{e_1-1})} \equiv 1 \pmod{p_1^{e_1-1}}$, and so

$$a^{({p_1}^{e_1-2})(p_1-1)} = a^{\Phi({p_1}^{e_1-1})} = 1 + mp_1^{e_1-1}$$

for some $m \in \mathbb{Z}$. Then

$$\begin{aligned} a^{\Phi({p_1}^{e_1})} &= a^{({p_1}^{e_1-1})(p_1-1)} \\ &= (a^{({p_1}^{e_1-2})(p_1-1)})^{p_1} \\ &= (1 + mp_1^{e_1-1})^{p_1} \\ &= 1 + \binom{p_1}{1} mp_1^{e_1-1} + m{p_1}^{e_1}Q \\ &= 1 + m{p_1}^{e_1} + m{p_1}^{e_1}Q \\ &= 1 + {p_1}^{e_1}(m + mQ). \end{aligned}$$

Thus $x - 1$ is divisible by ${p_1}^{e_1}$. Since ${p_1}^{e_1} \mid (x-1)$ and $(x-1) \mid (x^r - 1)$, it follows that ${p_1}^{e_1} \mid (x^r - 1)$. Similarly, each of ${p_2}^{e_2}, {p_3}^{e_3}, \cdots, {p_k}^{e_k}$ divides $(x^r - 1)$. Since each ${p_i}^{e_i}$ is relatively prime, their product, $s$, must also divide $(x^r - 1)$. Thus

$$a^{\Phi(s)} = a^v = x^r \equiv 1 \pmod{s}.$$

□

## Chapter 5: Early Proofs of Wilson's Theorem

***Theorem 3*** *(Wilson's Theorem) If $p$ is prime, then* $(p-1)! \equiv -1 \pmod{p}$.

The statement of Wilson's Theorem first appeared in *Meditationes Algebraicae* [14] in 1770 in a work by the English mathematician Edward Waring. John Wilson, a former student of Waring, stated the theorem but provided no proof, much like Fermat did for Fermat's Little Theorem. It was assumed by Wilson and Waring that a lack of notation would make the theorem too difficult to prove, but in 1771 Lagrange provided the first proof. Similar to the case of Fermat's Little Theorem, it should be noted that there is evidence Leibniz was aware of this property, but never published on the subject [5, p.97]. Unless otherwise noted, the proofs in this chapter are from [7, Chapter 3].

The following standard proof appears in Robbins' Beginning Number Theory[13, p.107] and many other books. We show later that this proof is a special case of a more general proof by Dirichlet in 1828.

***Proof 3.1*** If $p = 2$ then $(2-1)! = 1 \equiv -1 \pmod{2}$ and if $p = 3$ then $(3-1)! = 2 \equiv -1 \pmod{3}$. Thus assume $p$ is a prime greater than 3. Since $(p-1) \equiv -1 \pmod{p}$ it suffices to show that $(p-2)! \equiv 1 \pmod{p}$. By Lemma 7, for each $j$ such that $1 \leq j \leq p-1$ there exists an integer $k$ such that $1 \leq k \leq p-1$ such that $jk \equiv 1 \pmod{p}$. If $k = j$, then $j^2 \equiv 1 \pmod{p}$ so $j = 1$ or $j = p-1$. Thus if $2 \leq j \leq p-2$, then there exists an integer $k$ such that $j \neq k$ and $2 \leq k \leq p-2$ and $jk \equiv 1 \pmod{p}$. Since there are $\frac{1}{2}(p-3)$ such pairs, multiplying them together yields $(p-2)! \equiv 1 \pmod{p}$. Then

$$(p-1)(p-2)! \equiv (-1)(1) \pmod{p} \Rightarrow (p-1)! \equiv -1 \pmod{p}.$$

□

One of the earliest proofs of Wilson's Theorem came from Lagrange:

***Proof 3.2 (Lagrange, 1773)*** Let

$$(x+1)(x+2)\cdots(x+p-1) = x^{p-1} + A_1 x^{p-2} + \cdots + A_{p-1}. \tag{5.1}$$

Replacing $x$ by $x+1$ and multiplying by $x+1$, we have

$$(x+1)(x+2)\cdots(x+p) = (x+1)^p + A_1(x+1)^{p-1} + A_2(x+1)^{p-2} + \cdots + A_{p-1}(x+1). \tag{5.2}$$

Multiplying (5.1) by $(x+p)$, we see from (5.1) and (5.2) that

$$(x+p)[x^{p-1} + A_1 x^{p-2} + \cdots + A_{p-1}] = (x+1)^p + A_1(x+1)^{p-1} + A_2(x+1)^{p-2} + \cdots + A_{p-1}(x+1). \tag{5.3}$$

Then after expanding both sides of (5.3) and collecting like terms, we equate the coefficients to see that

$$\begin{aligned}
A_1 &= \binom{p}{2} \\
2A_2 &= \binom{p}{3} + A_1\binom{p-1}{2} \\
3A_3 &= \binom{p}{4} + A_1\binom{p-1}{3} + A_2\binom{p-2}{2} \\
&\vdots \\
(p-2)A_{p-2} &= p + (p-1)A_1 + (p-2)A_2 + \cdots + 3A_{p-3} \\
(p-1)A_{p-1} &= A_{p-2} + \cdots + A_3 + A_2 + A_1 + 1.
\end{aligned}$$

Thus in general, for $1 \le k \le p-1$

$$kA_k = \binom{p}{k+1} + A_1\binom{p-1}{k} + A_2\binom{p-2}{k-1} + \cdots + A_{k-1}\binom{p-k+1}{2}.$$

Let $p$ be prime. Then for $0 < k < p$ , $\binom{p}{k}$ is an integer divisible by $p$. Hence inductively $A_1, 2A_2, \ldots, (p-2)A_{p-2}$ are all divisible by $p$. Also

$$\begin{aligned}(p-1)A_{p-1} &= \binom{p}{p} + \binom{p-1}{p-1}A_1 + \binom{p-2}{p-2}A_2 + \cdots + \binom{2}{2}A_{p-2} \\ &= 1 + A_1 + A_2 + \cdots + A_{p-2}.\end{aligned}$$

Thus it follows that

$$\begin{aligned}(p-1)A_{p-1} &\equiv 1 \pmod{p} \\ (-1)A_{p-1} &\equiv 1 \pmod{p},\end{aligned}$$

i.e.

$$A_{p-1} + 1 \equiv 0 \pmod{p}.$$

Thus $1 + A_{p-1}$ is divisible by $p$. Now, recall the original equation

$$(x+1)(x+2)(x+3)\cdots(x+p-1) = x^{p-1} + A_1x^{p-2} + A_2x^{p-3} + \cdots + A_{p-1}.$$

Since from (5.1) $A_{p-1} = (p-1)!$, it follows that $A_{p-1} + 1 \equiv 0 \pmod{p}$. Thus $(p-1)! \equiv (-1) \pmod{p}$. □

Lagrange's proof furnishes another proof of Fermat's Little Theorem:

***Proof 1.9*** Let $x$ be a fixed integer. Since $x, x+1, \ldots, x+p-1$ is a sequence of $p$ consecutive integers, one of them is divisible by $p$. Also, $A_1, A_2, \ldots, A_{p-2}$ are all divisible by $p$ and $A_{p-1} = (p-1)! \equiv -1 \pmod{p}$. Thus

$$x(x+1)\cdots(x+p-1) = x^p + A_1x^{p-1} + \cdots + A_{p-2}x^2 + A_{p-1}x$$

gives us

$$0 \equiv x^p - x \pmod{p},$$

which is Fermat's Little Theorem. □

It is important to note that the numbers $A_k$ are today known as the Stirling numbers of the first kind. A common modern notation is $A_k = s(p, p-k)$ for $k = 1, \ldots, p$. Lagrange was the first to prove $s(p,k) \equiv 0 \pmod{p}$ for $1 \leq k \leq p-1$. Refer to [6, Chapter 5] for an excellent discussion of Stirling numbers.

Lagrange also provided a second proof, which makes use of Euler's Formula (refer to Chapter 2):

***Proof 3.3 (Lagrange, 1773)*** Recall Euler's Formula (Lemma 11):

$$x! = a^x - x(a-1)^x + \binom{x}{2}(a-2)^x - \binom{x}{3}(a-3)^x + \cdots .$$

When $x = p-1$ and $a = p$, we have

$$\begin{aligned}(p-1)! &= p^{p-1} - (p-1)(p-1)^{p-1} + \binom{p-1}{2}(p-2)^{p-1} \\ &- \binom{p-1}{3}(p-3)^{p-1} + \cdots - \binom{p-1}{p-2}(2^{p-1}) + (-1)^{p-1}.\end{aligned}$$

Then modding out by $p$ and using Fermat's Little Theorem, we have

$$(p-1)! \equiv 0 - (p-1) + \binom{p-1}{2} - \binom{p-1}{3} + \cdots - \binom{p-1}{p-2} + (-1)^{p-1} \pmod{p}.$$

Note that

$$(1-1)^{p-1} = \binom{p-1}{0}1^{p-1} - (p-1)1^{p-2} + \binom{p-1}{2}1^{p-3}(-1)^2 - \cdots + (-1)^{p-1}.$$

Thus

$$(p-1)! \equiv (1-1)^{p-1} - 1 \equiv -1 \pmod{p}.$$

□

Euler provided a proof of Wilson's Theorem using primitive roots:

***Proof 3.4 (Euler, 1783)*** Let $a$ be a primitive root of $p$. Then $\gcd(a,p) = 1$, the order of $a$ is $\Phi(p) = p-1$, and $a^{p-1} \equiv 1 \pmod{p}$. Consider the set $\{1, a, a^2, \ldots, a^{p-2}\}$. Since $p-1$ is the order of $a$, this set is congruent to the set $\{1, 2, 3, \ldots, p-1\}$ in some order. Then the products of the set elements must be congruent, and hence

$$\begin{aligned} a^{p-2} \cdot a^{p-1} \cdots a^2 \cdot a \cdot 1 &\equiv (p-1)! \pmod{p} \\ a^{\frac{(p-1)(p-2)}{2}} &\equiv (p-1)! \pmod{p}. \end{aligned}$$

Suppose $p > 2$, and let $p = 2n+1$ for some integer $n$. Then

$$a^n = a^{\frac{p-1}{2}}.$$

Since $a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$, we see from Fermat's Little Theorem that $p \mid (a^{\frac{p-1}{2}} - 1)$ or $p \mid (a^{\frac{p-1}{2}} + 1)$. Since $a$ is a primitive root, $p$ must divide $(a^{\frac{p-1}{2}} + 1)$, i.e. $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Then

$$a^{\frac{(p-1)(p-2)}{2}} = a^{\frac{2n(2n-1)}{2}} = a^{n(2n-1)} = (a^n)^{2n-1} \equiv (-1)^{2n-1} \pmod{p}.$$

Since $2n-1$ is odd, this implies $(p-1)! \equiv -1 \pmod{p}$. □

The next proof of Wilson's Theorem is originally due to Dirichlet.

***Proof 3.5 (Dirichlet, 1828)*** Let us say that $m, n$ are corresponding numbers if $m, n < p$ and $mn \equiv a \pmod{p}$, where $p$ is a prime, $a$ is a fixed integer, and $\gcd(a,p) = 1$. Now, each number $1, 2, \ldots, p-1$ has only one corresponding number. To see this note that for any given linear congruence, where $d = \gcd(a,n)$, $ax \equiv b \pmod{n}$ has $d$ solutions if $d \mid b$. In our case, $ax \equiv b \pmod{p}$ has 1 solution since $\gcd(a,p) = 1$. Hence there is a unique integer $n$ with $1 \leq n \leq p-1$ such that $mn \equiv a \pmod{p}$.

**Case 1:** If $x^2 \equiv a \pmod{p}$ has no integer solution, the corresponding numbers are distinct and so

$$1 \cdot 2 \cdot 3 \cdots (p-1) = (p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}$$

since there are $\frac{p-1}{2}$ factors of $a$.

**Case 2:** If $k$ is a positive integer less than $p$ such that $k^2 \equiv a \pmod{p}$, then $(p-k)^2 = p^2 - 2pk + k^2 \equiv a \pmod{p}$. Then omitting $k$ and $p-k$ from our product,

$$(1)(2)\cdots(k-1)(k+1)\cdots(p-k-1)(p-k+1)\cdots(p-1) \equiv a^{\frac{p-3}{2}} \pmod{p}.$$

Thus

$$\begin{aligned}(p-1)! &\equiv k(p-k)\cdot a^{\frac{p-3}{2}} \pmod{p} \\ &\equiv (pk-k^2)\cdot a^{\frac{p-3}{2}} \pmod{p} \\ &\equiv -a \cdot a^{\frac{p-3}{2}} \pmod{p} \\ &\equiv -(a^{\frac{p-1}{2}}) \pmod{p}.\end{aligned}$$

Let $a = 1$. Then since 1 is a square, Wilson's Theorem follows from Case 2:

$$(p-1)! \equiv -(1^{\frac{p-1}{2}}) \equiv -1 \pmod{p}.$$

If $p$ is an odd prime, then Euler's Criterion is satisfied: If $a$ is a quadratic residue (mod $p$), i.e. if the congruence $x^2 \equiv a \pmod{p}$ has solutions, then by Case 2 and Wilson's Theorem $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. If $a$ is a quadratic nonresidue (mod $p$), then following Case 1 and Wilson's Theorem $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Since $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$, squaring we obtain Fermat's Little Theorem: $a^{p-1} \equiv 1 \pmod{p}$. Thus Dirichlet provided proofs of three major theorems. □

Stern also provided an interesting proof, making use of the Maclaurin series of $\log(\frac{1}{1-x})$.

***Proof 3.6 (Stern, 1860)*** Let $f$ be a real-valued function. In general, if $f$ has derivatives of all orders at $x_0$, then the Taylor Series for $f$ about $x = x_0$ is

$$\sum_{k=0}^{\infty} \frac{f^{(k)}(x_0)}{k!}(x-x_0)^k = f(x_0)+f'(x_0)(x-x_0)+\frac{f''(x_0)}{2!}(x-x_0)^2+\cdots+\frac{f^k(x_0)}{k!}(x-x_0)^k+\cdots .$$

When $x_0 = 0$, we have the Maclaurin series for $f$:

$$\sum_{k=0}^{\infty} \frac{f^{(k)}(0)}{k!}(x)^k = f(0) + f'(0)(x) + \frac{f''(0)}{2!}(x)^2 + \cdots + \frac{f^k(0)}{k!}(x)^k + \cdots .$$

Consider $\log(\frac{1}{1-x}) = -\log(1-x)$. The Maclaurin series of $-\log(1-x)$ is:

$$0 + x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots .$$

Note we have

$$e^{x+\frac{x^2}{2}+\frac{x^3}{3}+\cdots} = e^{\log(\frac{1}{1-x})} = \frac{1}{1-x}$$

Note also that $1 + x + x^2 + \cdots = \frac{1}{1-x}$ (infinite geometric series). Thus we have

$$e^{x+\frac{x^2}{2}+\frac{x^3}{3}+\cdots} = 1 + x + x^2 + \cdots \tag{5.4}$$

Now expanding the left side of (5.4) in a power series, we have:

$$\begin{aligned}
e^{x} &= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \\
e^{\frac{x^2}{2}} &= 1 + \frac{\frac{x^2}{2}}{1!} + \frac{(\frac{x^2}{2})^2}{2!} + \frac{(\frac{x^2}{2})^3}{3!} + \cdots \\
&\vdots \\
e^{\frac{x^p}{p}} &= 1 + \frac{\frac{x^p}{p}}{1!} + \frac{(\frac{x^p}{p})^2}{2!} + \frac{(\frac{x^p}{p})^3}{3!} + \cdots \\
&\vdots \quad .
\end{aligned}$$

Thus

$$
\begin{aligned}
& e^{x+\frac{x^2}{2}+\cdots} \\
& = (1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots)(1+\frac{\frac{x^2}{2}}{1!}+\frac{(\frac{x^2}{2})^2}{2!}+\frac{(\frac{x^2}{2})^3}{3!}+\cdots) \\
& \cdots(1+\frac{\frac{x^p}{p}}{1!}+\frac{(\frac{x^p}{p})^2}{2!}+\frac{(\frac{x^p}{p})^3}{3!}+\cdots)\cdots \\
& = 1+\frac{x}{1!}+x^2\left(\frac{1}{2!}+\frac{1}{2}\right)+x^3\left(\frac{1}{3!}+\frac{1}{1!}\cdot\frac{\frac{1}{2}}{1!}+\frac{\frac{1}{3}}{1!}\right)+ \\
& \cdots+x^p\left(\frac{1}{p!}+\frac{1}{(p-2)!}\cdot\frac{\frac{1}{2}}{1!}+\cdots+\frac{\frac{1}{p}}{1}\right)+\cdots\ .
\end{aligned}
$$

The $x^p$ term is the sum of all terms of the following form:

$$
\frac{x^{a_1}}{a_1!}\cdot\frac{(\frac{x^2}{2})^{a_2}}{a_2!}\cdot\frac{(\frac{x^3}{3})^{a_3}}{a_3!}\cdots\frac{(\frac{x^p}{p})^{a_p}}{a_p!}=\frac{x^{a_1+2a_2+3a_3+\cdots+pa_p}}{a_1!a_2!a_3!\cdots a_p!2^{a_2}3^{a_3}\cdots p^{a_p}}
$$

where $a_1+2a_2+3a_3+\cdots+pa_p=p$.

**Case 1:** $a_1=p, a_i=0$ for all $i>1$. This gives $\frac{x^p}{p!}$.

**Case 2:** $a_p=1, a_i=0$ for all $i<p$. This gives $\frac{\frac{x^p}{p}}{1!}=\frac{x^p}{p}$.

**Case 3:** $a_1\neq p, a_p=0$. In this case $a_i<p$, so $p$ does not divide the denominator $a_1!a_2!a_3!\cdots a_p!2^{a_2}3^{a_3}\cdots p^{a_p}$.

Thus the coefficient of $x^p$ is $\frac{1}{p!}+\frac{1}{p}+\frac{r}{s}$, where $p$ does not divide $s$ and $\gcd(r,s)=1$. Then since coefficients of (5.4) must be equal on both sides of the equation:

$$
\begin{aligned}
\frac{1}{p!}+\frac{1}{p}+\frac{r}{s} &= 1 \\
\frac{p!s}{1}(\frac{1}{p!}+\frac{1}{p}) &= \frac{p!s}{1}(1-\frac{r}{s}) \\
s(1+(p-1)!)=p!s-p!r &= p!(s-r)=p(p-1)!(s-r).
\end{aligned}
$$

Since $p\nmid s$, it follows that $p\mid(1+(p-1)!)$, so

$$(p-1)! \equiv -1 \pmod{p}.$$

□

For a more detailed discussion of Stern's proof, see Topics from the Theory of Numbers by Emil Grosswald, [10, pages 44-46]. Also, all of the formulas and manipulations for the power series expansions of $e^x$ and $\log(1-x)$ can be justified by the theory of formal power series. See [6, pages 36-43].

The following proof by Thue in Dickson involves the use of the "difference operator" $\Delta$, defined by $\Delta f(x) = f(x+1) - f(x)$ for any function $f$. Note that

$$\begin{aligned}
\Delta(f(x)+g(x)) &= (f(x+1)+g(x+1)) - (f(x)+g(x)) \\
&= (f(x+1)-f(x)) + (g(x+1)-g(x)) \\
&= \Delta f(x) + \Delta g(x).
\end{aligned}$$

Also, we define $\Delta^k f(x) = \Delta^{k-1}(\Delta f(x)) = \Delta(\Delta^{k-1} f(x))$. We will show that

$$\begin{aligned}
\Delta^k f(x) &= f(x+k) - \binom{k}{k-1} f(x+k-1) + \binom{k}{k-2} f(x+k-2) - \cdots + (-1)^k f(x) \\
&= \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} f(x+j). \qquad (5.5)
\end{aligned}$$

Now we use induction to prove that $\Delta^k f(x) = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} f(x+j)$ for all integers $k$, and then prove Wilson's Theorem.

***Proof 3.7 (Thue, 1893)*** Let $S = \{\, k \mid \Delta^k f(x) = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} f(x+j) \}$.

(1) $1 \in S$:

$$\begin{aligned}\Delta^1 f(x) = f(x+1) - f(x) &= (-1)^{1-0}\binom{1}{0} f(x+0) + (-1)^0\binom{1}{1} f(x+1) \\ &= -f(x) + f(x+1)\end{aligned}$$

$2 \in S$:

$$\begin{aligned}\Delta^2 f(x) = \Delta^1(\Delta f(x)) &= \Delta(f(x+1) - f(x)) \\ &= (f(x+2) - f(x+1)) - (f(x+1) - f(x)) \\ &= f(x+2) - \binom{2}{1} f(x+1) + f(x)\end{aligned}$$

(2) Assume true for $k-1$ such that

$$\Delta^{k-1} f(x) = \sum_{j=0}^{k-1} (-1)^{k-1-j}\binom{k-1}{j} f(x+j).$$

Then

$$\begin{aligned}\Delta^k f(x) &= \Delta(\Delta^{k-1} f(x)) \\ &= \Delta(\sum_{j=0}^{k-1} (-1)^{k-1-j}\binom{k-1}{j} f(x+j)) \\ &= \Delta[(-1)^{k-1-0}\binom{k-1}{0} f(x+0)] + \Delta[(-1)^{k-1-1}\binom{k-1}{1} f(x+1)] + \\ \cdots + &\ \Delta[(-1)^{k-1-(k-1)}\binom{k-1}{k-1} f(x+k-1)] \\ &= (-1)^{k-1}\binom{k-1}{0}(f(x+1) - f(x)) + (-1)^{k-2}\binom{k-1}{1}(f(x+2) - f(x+1)) + \\ \cdots + &\ (-1)^0\binom{k-1}{k-1}(f(x+k) - f(x+k-1)) \\ &= \sum_{j=0}^{k-1} (-1)^{k-1-j}\binom{k-1}{j}(f(x+j+1) - f(x+j)).\end{aligned}$$

For $1 \le j \le k-1$, by Pascal's Identity, the coefficient of $f(x+j)$ is

$$(-1)^{k-j}\left[\binom{k-1}{j} + \binom{k-1}{j-1}\right] = (-1)^{k-j}\binom{k}{j}.$$

It is easy to see that the coefficient of $f(x+k)$ is 1:

$$(-1)^{k-k}\binom{k}{k} = 1,$$

and the coefficient of $f(x)$ is $(-1)^k$:

$$(-1)^{k-0}\binom{k}{0} = (-1)^k.$$

If $f(x) = x^n$ the formula is

$$\Delta^k x^n = \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}(x+j)^n.$$

When $x = 0$ this gives

$$\Delta^k 0^n = \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}(j)^n.$$

Here we note that $\Delta^k 0^n = k!S(n,k)$, where $S(n,k)$ is the Stirling number of the second kind. See [6, p.14].

Let $f(x) = x^{p-1}$, where $p$ is prime. From formula (5.5), Fermat's Little Theorem, and the Binomial Theorem, we have for $k = 1, 2, 3, \ldots, p-2$:

$$\Delta^k f(1) = \sum_{j=1}^{k}(-1)^{k-j}\binom{k}{j}(1+j)^{p-1} \equiv \sum_{j=1}^{k}(-1)^{k-j}\binom{k}{j} \equiv (1-1)^k \equiv 0 \pmod{p}.$$

Now note that:

$$\begin{aligned}
\Delta^2 f(0) &= \Delta f(1) - \Delta f(0) \\
\Delta^3 f(0) &= \Delta^2 f(1) - \Delta^2 f(0) \\
\Delta^4 f(0) &= \Delta^3 f(1) - \Delta^3 f(0) \\
&\vdots \\
\Delta^{p-2} f(0) &= \Delta^{p-3} f(1) - \Delta^{p-3} f(0) \\
\Delta^{p-1} f(0) &= \Delta^{p-2} f(1) - \Delta^{p-2} f(0).
\end{aligned} \tag{5.6}$$

Employing (5.6), we find that

$$\begin{aligned}
\Delta^{p-1}f(0) &= \Delta^{p-2}f(1) - \Delta^{p-3}f(1) + \Delta^{p-4}f(1) - \cdots + \Delta^3 f(1) - \Delta^2 f(1) + \Delta f(1) - \Delta f(0) \\
&\equiv -\Delta f(0) \\
&= -f(1) + f(0) \\
&= -1^{p-1} \\
&\equiv -1 \pmod{p}.
\end{aligned}$$

Now we notice that by (5.5)

$$\begin{aligned}
\Delta^{p-1}f(0) &= \Delta^{p-1}0^{p-1} = \sum_{j=0}^{p-1}(-1)^{p-1-j}\binom{p-1}{j}j^{p-1} \\
&= (p-1)^{p-1} - \binom{p-1}{1}(p-2)^{p-1} + \binom{p-1}{2}(p-3)^{p-1} - \cdots - \binom{p-1}{p-2}1^{p-1}.
\end{aligned}$$

which by Euler's Formula is equal to $(p-1)!$. Thus $(p-1)! \equiv -1 \pmod{p}$. $\square$

## Chapter 6: Gauss' Generalization of Wilson's Theorem

Gauss [7, p.65] was evidently the first person to state the following generalization of Wilson's Theorem:

***Theorem 4*** Let $P$ be the product of the $\Phi(A)$ integers $n_1, n_2, \ldots, n_{\Phi(A)}$, all less than $A$ and $\gcd(n_i, A) = 1$ for all $i$. Let $A = 2^j {p_1}^{e_1} {p_2}^{e_2} \cdots {p_k}^{e_k}$ where $p_i$ are all distinct odd primes and $\Phi(A) > 0$. If $A = 4$ or $A = 2^j p^m$ with $j = 0$ or $j = 1$, then $P \equiv -1 \pmod{A}$. Otherwise $P \equiv 1 \pmod{A}$.

***Proof 4.1 (Minding, 1832)***

Take quadratic non-residue $t$ of $p_1$ and use the Chinese Remainder Theorem to determine $a$ so that $a \equiv t \pmod{p_1}$ and $a \equiv 1 \pmod{2p_2p_3 \cdots p_k}$. Then $a$ is an odd quadratic non-residue of $A$.

Let $n_1 x \equiv a \pmod{A}$ and $n_2 y \equiv a \pmod{A}$ such that $n_1 \neq n_2$ and $n_2 \neq a$. Then $y \neq n_1, x, n_2$. In this way the $\Phi(A)$ integers $n_1, n_2, \ldots, n_{\Phi(A)}$ can be paired $n_1 x, n_2 y, \ldots$ so that the product of the two in any pair is congruent to $a \pmod{A}$. Since there are $\Phi(A)/2$ pairs, $P \equiv a^{\Phi(A)/2} \pmod{A}$.

**Case 1:** $A = 2^j p^m$ with $j = 0$ or $j = 1$

Then $\Phi(A) = \Phi(2^j p^m) = \Phi(2^j)\Phi(p^m) = (p^{m-1})(p-1)$, and $a^{\Phi(A)} = a^{(p^{m-1})(p-1)} = a^{\Phi(p^m)} \equiv 1 \pmod{p^m}$ since $\gcd(a, p^m) = 1$ by the Generalization of Fermat's Little Theorem. Thus by Euler's Criterion

$$a^{\Phi(A)/2} = (a^{\frac{p-1}{2}})^{p^{m-1}} \equiv (-1)^{p^{m-1}} \equiv -1 \pmod{p}.$$

Thus $p^m$ either divides $a^{\Phi(A)/2} - 1$ or $a^{\Phi(A)/2} + 1$. From above we also know that $p$

divides $a^{\Phi(A)/2}+1$. If $p \mid (a^{\Phi(A)/2})-1$ then $p \mid [(a^{\Phi(A)/2}+1)-(a^{\Phi(A)/2}-1)]$, which implies $p \mid 2$, a contradiction since $p$ is odd. Thus $p \mid (a^{\Phi(A)/2}+1)$ which implies $p^m \mid (a^{\Phi(A)/2}+1)$. Thus $a^{\Phi(A)/2} \equiv -1 \pmod{p^m} \equiv -1 \pmod{A}$.

If $A = 2p^m$ then since $a$ is odd, $a^{\Phi(A)/2} \equiv (-1) \pmod 2$. Thus $P = a^{\Phi(A)/2} \equiv -1 \pmod{A}$.

**Case 2:** $A = 2^j p^m$ with $j \geq 2$

Then $\Phi(A) = 2^{j-1}(p^{m-1})(p-1)$, and

$$a^{\Phi(A)/2} = a^{(2^{j-1})(p^{m-1})(p-1)/2} = (a^{\frac{p^{m-1}(p-1)}{2}})^{2^{j-1}} \equiv (-1)^{2^{j-1}} \equiv 1 \pmod{p^m},$$

and

$$a^{\Phi(A)/2} = (a^{2^{j-1}})^{(p^{m-1})(p-1)/2} \equiv 1^{p^{m-1}(p-1)/2} \equiv 1 \pmod{2^j}.$$

Note: By the Generalization of Fermat's Little Theorem, $a^{2^{j-1}} \equiv 1 \pmod{2^j}$.

Thus $P \equiv a^{\Phi(A)/2} \equiv 1 \pmod{A}$.

**Case 3:** $A = 2^j p^m q^n \cdots$ with $m, n, j > 0$ and $p, q$ are distinct

Then

$$\begin{aligned} a^{\Phi(A)/2} &= [a^{(p^{m-1})(p-1)/2}]^{2^{j-1}q^{n-1}(q-1)\cdots} \\ &\equiv (-1)^{2^{j-1}q^{n-1}(q-1)\cdots} \\ &\equiv 1 \pmod{p^m} \end{aligned}$$

since $q-1$ is even.

Similarly:

$$\begin{aligned} a^{\Phi(A)/2} &= [a^{q^{n-1}(q-1)}]^{2^{j-1}p^{m-1}(p-1)/2\cdots} \\ &\equiv 1^{2^{j-1}p^{m-1}(p-1)/2\cdots} \pmod{q^n} \\ &\equiv 1 \pmod{q^n} \end{aligned}$$

and

$$a^{\Phi(A)/2} = (a^{2^{j-1}})^{p^{m-1}\frac{(p-1)}{2}(q^{n-1})(q-1)\cdots} \equiv 1 \pmod{2^j}.$$

Thus $P \equiv a^{\Phi(A)/2} \equiv 1 \pmod{A}$ by the Chinese Remainder Theorem.

**Case 4:** $A = 2^j$ with $j \geq 2$

Since $x^2 \equiv -1 \pmod{4}$ has no solutions, $x^2 \equiv -1 \pmod{2^j}$ has no solutions since $4 \mid 2^j$. So we can pair off the odd integers less than $2^j$ such that $x_1 \cdot x_2 \equiv -1 \pmod{2^j}$. Since $\Phi(2^j) = 2^{j-1}$, there are $2^{j-2}$ pairs. Thus

if $A = 2^2$ :

$$P \equiv a^{\Phi(A)/2} \equiv (-1)^{2^{j-2}} \equiv -1 \pmod{A}$$

and if $A = 2^j$ for $j > 2$ :

$$P \equiv a^{\Phi(A)/2} \equiv (-1)^{2^{j-2}} \equiv +1 \pmod{A}.$$

□

The generalization of Wilson's Theorem can also be stated in the following way:

***Theorem 4*** *Suppose $n > 1$ and define $Q$ via $\{a \mid 1 \leq a \leq n-1, \gcd(a,n) = 1\}$. Let $P$ be the product of all the elements of $Q$. If $n = 2, 4, p^e$, or $2p^e$, where $p$ is an odd prime, then $P \equiv -1 \pmod{n}$. Otherwise $P \equiv 1 \pmod{n}$.*

***Proof 4.2 (Howard and Turnage, 2007)*** We will use the ideas of Crelle (1840), Prouhot (1845), and Arndt (1846).

**Case 1:** $n = 2, 4, p^e,$ or $2p^e$

Then by Lemma 12 $n$ has a primitive root, call it $r$. Then applying Lemma 11, $Q \equiv \{r, r^2, \ldots, r^{\Phi(n)}\} \pmod{n}$, so the product of these elements is congruent to $P$,

and we have

$$\begin{aligned} P \equiv r \cdot r^2 \cdots r^{\Phi(n)} \pmod{n} &= r^{1+2+3+\cdots+\Phi(n)} \\ &= r^{\frac{\Phi(n)(1+\Phi(n))}{2}} \\ &= (r^{\Phi(n)/2})^{(1+\Phi(n))} \equiv (-1)^{(1+\Phi(n))} \equiv -1 \pmod{n}. \end{aligned}$$

We have used the facts that:

- $\Phi(n)$ is even for $n > 2$

**Proof** [5, p.128] If $n$ is a power of 2, let $n = 2^k$ for $k \geq 2$. Then $\Phi(n) = \Phi(2^k) = 2^k(1-\frac{1}{2}) = 2^{(k-1)}$, an even integer. If $n$ is not a power of 2, then it is divisible by some odd prime $p$. Then $n = p^k m$ for $k \geq 1$ and $\gcd(p^k, m) = 1$. Since $\Phi$ is multiplicative, $\Phi(n) = \Phi(p^k) \cdot \Phi(m) = p^k(1-\frac{1}{p}) \cdot \Phi(m) = (p^k - p^{k-1})\Phi(m) = p^{k-1}(p-1)\Phi(m)$. Since $2 \mid (p-1)$, $\Phi(n)$ is even.

- $r^{\Phi(n)/2} \equiv -1 \pmod{n}$

**Proof** The cases $n = 2$ and $n = 4$ are trivial, so let $n = p^e$. Then

$$(r^{\Phi(n)/2} - 1)(r^{\Phi(n)/2} + 1) = r^{\Phi(n)} - 1 \equiv 0 \pmod{n}$$

implies $p \mid (r^{\Phi(n)/2} - 1)$ or $p \mid (r^{\Phi(n)/2} + 1)$. Note that $p$ does not divide both factors: if $p$ divided both factors, it would divide their difference, which implies $p \mid 2$, a contradiction. Since $r$ is a primitive root $\pmod{n}$ we cannot have $(r^{\Phi(n)/2} - 1) \equiv 0 \pmod{n}$. Thus with $n = p^e$,

$$r^{\Phi(n)/2} + 1 \equiv 0 \pmod{n}.$$

The proof is similar if $n = 2p^e$. In that case $r$ is odd, so $2 \mid (r^{\Phi(n)/2} \pm 1)$. Again we conclude that $r^{\Phi(n)/2} + 1 \equiv 0 \pmod{n}$.

**Case 2:** $4 \mid n$ and $n > 4$

Consider $x^2 \equiv -1 \pmod{4}$. Since $x^2 \equiv -1 \pmod{4}$ has no solutions, $x^2 \equiv -1$

(mod $n$) has no solutions, since 4 divides $n$. Thus for each element $a$ in $Q$, the congruence $ax \equiv -1 \pmod{n}$ has a unique solution $x = b$ in $Q$, and $b \neq a$. We pair off all the elements $a$ and $b$ in $Q$ so that $ab \equiv -1 \pmod{n}$. Then since $n$ is divisible by 4, $n = 2^j m$ for some integer $m$ and $j \geq 2$. Then

$$n = \begin{cases} 2^j m & j \geq 3, m \in \mathbb{Z} \\ 4p \mid n & p \text{ an odd prime} \end{cases}$$

and so

$$\Phi(n) = \begin{cases} 2^{j-1}\Phi(m) \\ 2(p-1)\cdots \end{cases} .$$

It thus follows that $4 \mid \Phi(n)$, so $\frac{\Phi(n)}{2}$ is even. Then

$$P \equiv (-1)^{\Phi(n)/2} \equiv 1 \pmod{n}.$$

**Case 3:** $n = 2^j {p_1}^{e_1} {p_2}^{e_2} \cdots {p_k}^{e_k}$, where $j = 0$ or $j = 1$, each $p_i$ is an odd prime, and $k \geq 2$.

Now we show that $x^2 \equiv 1 \pmod{n}$ has $2^k$ solutions. To see this, we use the fact that $x^2 \equiv 1 \pmod{{p_i}^{e_i}}$ has exactly two solutions: $x = 1$ and $x = -1$. Note that $x^2 \equiv 1 \pmod{2^j {p_1}^{e_1} \cdots {p_k}^{e_k}}$ if and only if $x^2 \equiv 1 \pmod{2^j}$ and $x^2 \equiv 1 \pmod{{p_i}^{e_i}}$ for $i = 1, \ldots, k$. Thus, applying the Chinese Remainder Theorem to the system

$$\begin{aligned} x &\equiv 1 \pmod{2^j} \\ x &\equiv \pm 1 \pmod{{p_i}^{e_i}}, i = 1, \ldots, k \end{aligned}$$

we find that the solutions occur in pairs $a$ and $(n - a)$ with $a(n - a) \equiv -(a)^2 \equiv -1 \pmod{n}$.

Let $S$ be the product of all the solutions to $x^2 \equiv 1 \pmod{n}$. Since there are $2^{k-1}$ pairs, $S \equiv (-1)^{2^{k-1}} \equiv 1 \pmod{n}$. If $a$ is an element of $Q$ not in $S$ then $ax \equiv 1$

(mod $n$) has a unique solution $x = b$ in $Q$, and $b \neq a$. We pair off the elements $a$ and $b$ in $Q - S$ so that $ab \equiv 1 \pmod{n}$. Hence $P \equiv 1 \pmod{n}$. □

Note 1: According to Dickson [7, p.65], Gauss stated the generalized theorem and remarked that primitive roots can be used in the proof. That is one reason we included Case 1 in our proof. However we note that the method of Case 3 can easily be used for $n = p^3$ and $n = 2p^e$. In those cases, $x^2 \equiv 1 \pmod{n}$ has only two solutions, $x \equiv \pm 1 \pmod{n}$. We can pair off the other elements $a, b$ so that $ab \equiv 1 \pmod{n}$, so $P \equiv -1 \pmod{n}$. Thus we can shorten out proof by considering the cases $4 \mid n$ and $4 \nmid n$.

Note 2: In Case 3, suppose ${p_1}^{e_1} \mid n$ with $p_1 \equiv 3 \pmod{4}$. Then $x^2 \equiv -1 \pmod{n}$ has no solutions, since $x^2 \equiv -1 \pmod{p_i}$ has no solutions. As in Case 2, we can pair off all the elements $a$ and $b$ in $Q$ such that $ab \equiv -1 \pmod{n}$. Thus $P \equiv (-1)^{\Phi(n)/2} \equiv 1 \pmod{n}$. This means in Case 3 we could assume that each $p_i$ is congruent to 1 (mod 4).

***Example*** Suppose $n = 130 = 2 \cdot 5 \cdot 13$. Then $k = 2$. We want to show that $x^2 \equiv 1 \pmod{130}$ has $2^k = 4$ solutions. To do this, we use the Chinese Remainder Theorem to solve the systems

$$\begin{array}{llll} x \equiv 1 \pmod{2} & x \equiv 1 \pmod{2} & x \equiv 1 \pmod{2} & x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{5} & x \equiv 1 \pmod{5} & x \equiv -1 \pmod{5} & x \equiv -1 \pmod{5} \\ x \equiv 1 \pmod{13} & x \equiv -1 \pmod{13} & x \equiv 1 \pmod{13} & x \equiv -1 \pmod{13} \end{array} .$$

Then we get the four solutions to $x^2 \equiv 1 \pmod{n}$:

$$1, 51, -51 \equiv 79, -1 \equiv 129.$$

## Chapter 7: Recent Combinatorial Proofs

The following proofs of Fermat's Little Theorem and Wilson's Theorem show that the theorems are currently being considered. The first proofs come from *Combinatorial Proofs of Fermat's, Lucas's, and Wilson's Theorems*, by Peter G. Anderson, Arthur T. Benjamin, and Jeremy A. Rouse [2]. The final proofs are given in Proofs that Really Count by Arthur T. Benjamin and Jennifer J. Quinn. [3]

We begin with the following lemma [2]:

***Lemma 17*** *Let $S$ be a finite set, let $p$ be prime, and suppose $f : S \to S$ has the property that $f^p(x) = x$ for any $x$ in $S$, where $f^p$ is the $p$-fold composition of $f$. Then $|S| \equiv |F| \pmod{p}$ , where $F$ is the set of fixed points of $f$.*

**Proof** First we must show that $S$ is the disjoint union of sets of the form $\{ x, f(x), \ldots, f^{p-1}(x) \}$. Suppose not, i.e. suppose we have two distinct subsets of $S$ such that

$$\{ x, f(x), \ldots, f^{p-1}(x) \} \cap \{ y, f(y), \ldots, f^{p-1}(y) \} \neq \varnothing.$$

Then there exists $i, j \in \mathbb{Z}$ where $0 \leq j < i \leq p-1$ such that

$$f^i(x) = f^j(y).$$

Then:

$$\begin{aligned} f^{i+1}(x) &= f^{j+1}(y) \\ f^{i+2}(x) &= f^{j+2}(y) \\ &\vdots \\ f^{p}(x) &= f^{j+k}(y), \quad j+k<p, \quad \text{and } p=i+k. \end{aligned}$$

Then:

$$\begin{aligned} x &= f^{j+k}(y) \\ f(x) &= f^{j+k+1}(y) \\ f^2(x) &= f^{j+k+2}(y) \\ &\vdots \end{aligned}$$

i.e. $\{\, x, f(x), \ldots, f^{p-1}(x) \,\} = \{\, y, f(y), \ldots, f^{p-1}(y) \,\}$.

Thus either $\{\, x, f(x), \ldots, f^{p-1}(x) \,\} \cap \{\, y, f(y), \ldots, f^{p-1}(y) \,\} = \varnothing$ or $\{\, x, f(x), \ldots, f^{p-1}(x) \,\} = \{\, y, f(y), \ldots, f^{p-1}(y) \,\}$. Now we need to show that every cycle length of $x$ either has size 1 or size $p$. Let $x \in S$. Then the permutation generated by $x$ is $\{\, x, f(x), \ldots, f^{p-1}(x) \,\}$. If $x$ is a fixed point of $f$, then $f(x) = x$, which implies the length of the cycle of $x$ is size 1. By assumption, $f^p(x) = x$ for all $x \in S$, which implies the length of the cycle of $x$ is at most size $p$. Now, suppose the length of the cycle of $x$ is $k$ such that $1 < k \leq p-1$. Then $\{\, x, f(x), \ldots, f^{k-1}(x) \,\}$ is the permutation generated by $x$, and we have:

| $x$ | $f(x)$ | $f^2(x)$ | $\cdots$ | $f^{k-1}(x)$ | $x$ | $f(x)$ | $\cdots$ | $f^{k-1}(x)$ | $x$ | $f(x)$ | $\cdots$ | $f^{p-1}(x)$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

There are $p$ total boxes divided into $m$ sets of $k$ terms. Thus $p = mk$, which contradicts the fact that $p$ is prime. Thus every cycle length of $x$ has either size 1 or size $p$. Finally, we must show that $|S| \equiv |F| \pmod{p}$. From above, every cycle length of $x$ is either size 1 or size $p$. In $S$, either $x$ is a fixed point or it is not. The size of $S$ is thus composed of the number of fixed points, $|F|$, plus the number of other points, $|N|$. Since the length of the cycle of a non-fixed point is $p$, the non-fixed points come in multiples of $p$. Thus

$$|S| = |F| + |N| = |F| + pn \equiv |F| \pmod{p}.$$

□

Now we can use this lemma to prove Fermat's Little Theorem:

***Proof 1.10 (Anderson, Benjamin, and Rouse, 2005)*** Let $S$ be the set of all colored bracelets of length $p$, where there are $a$ color choices for beads of length one. Let $f : S \to S$ such that $f(x) = x_1$, where $x_1$ is $x$ rotated clockwise by one unit. Thus $|S| = a^p$. There are $a$ colored bracelets of length $p$ with a monochromatic coloring. Since each rotation of such a bracelet yields the same bracelet, i.e. $f(x) = x$, these are our fixed points. That is, $|F| = a$. Thus by the previous lemma, $a^p \equiv a \pmod{p}$. □

***Example*** Let $p = 3 =$ number of length one beads and let $a = 2 =$ number of colors of beads. We want to illustrate that the number of colored bracelets of length $p$ with $a$ color choices for beads of length one is $a^p = 8$. Figure 1 illustrates all possible

bracelets:

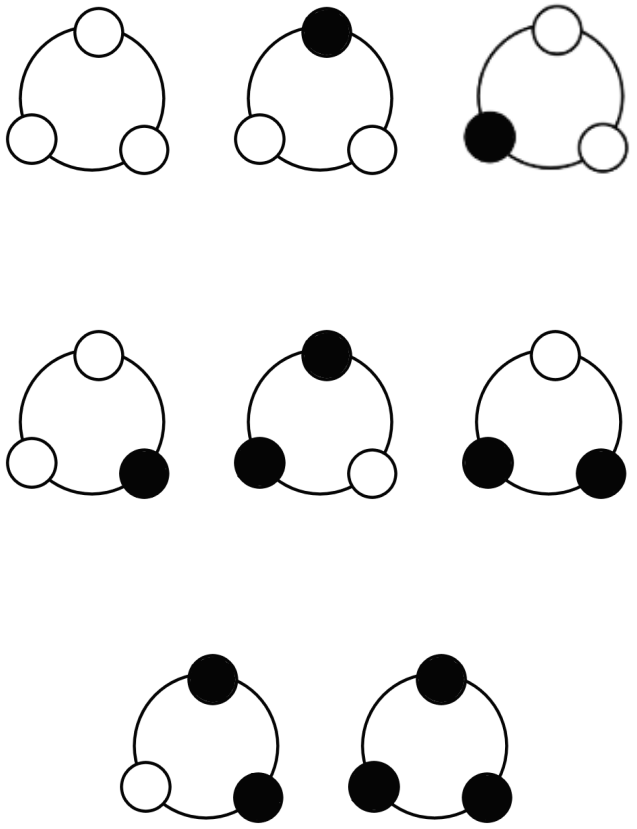

Figure 1

Thus the number of colored bracelets of length 3 with 2 color choices for breads of length one is $2^3 = 8$. There are 2 colored bracelets of length 3 with a monochromatic coloring. Since each rotation of such a bracelet yields the same bracelet, by the lemma

$$2^3 = 8 \equiv 2 \pmod 3.$$

Now we can use the same lemma to prove Wilson's Theorem:

***Proof 3.8 (Anderson, Benjamin, and Rouse, 2005)*** First let us ask ourselves, how many permutations of $\{\, 0, 1, \ldots, p-1 \,\}$ have exactly one cycle?

| | | | | | |
|---|---|---|---|---|---|
| 0 | $p-1$ | $p-2$ | $p-3$ | $\ldots$ | 1 |

Note: Each entry in a cell denotes the number of choices one has when building a permutation.

All permutations begin with 0, so there are $(p-1)!$ permutations of $\{\,0, 1, \ldots, p-1\,\}$ having exactly one cycle.

Let $S$ be the set of $(p-1)!$ permutations of $\{\,0, 1, \ldots, p-1\,\}$ with exactly one cycle, and define a function $f$ on $S$ as follows:

Let $(0, a_1, a_2, \ldots, a_{p-1})$ be a permutation in $S$. Then $f((0, a_1, a_2, \ldots, a_{p-1})) = (1, a_1 + 1, a_2 + 1, \ldots, a_{p-1} + 1) \in S$ where all sums are reduced modulo $p$. Note that $f^p((0, a_1, a_2, \ldots, a_{p-1})) = (0, a_1, a_2, \ldots, a_{p-1})$.

From the previous lemma, we know that $|S| \equiv |F| \pmod{p}$. Thus we must show that there are $p-1$ fixed points of $f$.

**Claim:** All permutations of the form $(0, a, 2a, 3a, \ldots, (p-1)a)$ where $1 \leq a \leq p-1$ are the only fixed points of $f$, where all terms are reduced modulo $p$. Here is our proof:

First show that $(0, a, 2a, \ldots, (p-1)a)$ is a fixed point: by the definition of $f$, we have

$$f(0, a, \ldots, (p-1)a) = (1, 1+a, 1+2a, \ldots, 1+ka, 1+(k+1)a, \ldots, 1+(p-1)a).$$

Now $1 + ka \equiv 0 \pmod{p}$ for some $k$, so

$$\begin{aligned} 1 + (k+1)a &= 1 + ka + a \equiv a \pmod{p} \\ 1 + (k+2)a &= 1 + ka + 2a \equiv 2a \pmod{p} \\ &\vdots \\ 1 + (k + (p-1))a &= 1 + ka - a \equiv (p-1)a \pmod{p}. \end{aligned}$$

Thus $(0, a, \ldots, (p-1)a)$ is a fixed point.

Now suppose $(0, a_1, a_2, \ldots, a_{p-1})$ is a fixed point of $f$. Then

$$\begin{aligned} f(0, a_1, a_2, \ldots, a_{p-1}) &= (1, 1 + a_1, \ldots, 1 + a_{p-1}) \\ f^{(2)}(0, a_1, a_2, \ldots, a_{p-1}) &= (2, 2 + a_1, \ldots, 2 + a_{p-1}) \\ &\vdots \\ f^{(a_1)}(0, a_1, a_2, \ldots, a_{p-1}) &= (a_1, 2a_1, \ldots, a_1 + a_{p-1}) \end{aligned}$$

so $a_2 = 2a_1$. Continuing in this manner,

$$f^{(2a_1)}(0, a_1, a_2, \ldots, a_{p-1}) = (2a_1, 3a_1, \ldots, 2a_1 + a_{p-1})$$

so $a_3 = 3a_1$. In general

$$f^{(ka_1)}(0, a_1, a_2, \ldots, a_{p-1}) = (ka_1, (k+1)a_1, \ldots, ka_1 + a_{p-1})$$

so $a_{k+1} = (k+1)a_1$. Since $(0, a_1, a_2, \ldots, a_{p-1})$ is a fixed point, we have

$$(0, a_1, a_2, \ldots, a_{k+1}, \ldots, a_{p-1}) = (0, a_1, 2a_1, \ldots, (k+1)a_{k+1}, \ldots, (p-1)a_1)$$

which implies all fixed points of $S$ are of this form. Since there are $(p-1)$ choices for $a_1$, there are $(p-1)$ fixed points of $f$. Thus

$$\begin{aligned} |S| &\equiv |F| \pmod{p} \\ (p-1)! &\equiv (p-1) \pmod{p} \\ &\equiv -1 \pmod{p}. \end{aligned}$$

□

***Example*** As an illustration of Proof 3.8, let $p = 5$ and define $\Pi = (0, 3, 1, 4, 2)$. Note

that $f(\Pi) = (1, 4, 2, 0, 3) = (0, 3, 1, 4, 2)$, so $\Pi$ is a fixed point with $\Pi(0) = 3$. Then

$$\begin{aligned}
\Pi &= f^{(3)}(\Pi) = (3, 6, 4, 7, 5) \text{ , so } \Pi(3) = 6 \\
\Pi &= f^{(6)}(\Pi) = (6, 9, 7, 10, 8) \text{ , so } \Pi(6) = 9 \\
\Pi &= f^{(9)}(\Pi) = (9, 12, 10, 13, 11) \text{ , so } \Pi(9) = 12 \\
\Pi &= f^{(12)}(\Pi) = (12, 15, 13, 16, 14) = (12, 0, 13, 16, 14)
\end{aligned}$$

so $\Pi(12) = 0$.

Thus $(0, 3, 1, 4, 2) = (0, 3, 6, 9, 12)$ which illustrates Proof 3.8 for $a_1 = 3$.

Now we look at another combinatorial perspective of Fermat's Little Theorem:

***Proof 1.11 (Benjamin and Quinn, 2003)*** [3, p.115] First, we ask the following question: How many ways can the numbers $\{ 1, 2, \ldots, p \}$ each be assigned one of $a$ colors, where not all numbers are allowed to be assigned the same color? Now we prove that the answer gives us Fermat's Little Theorem.

One way to look at this is to consider a box of $p$ cells, each cell representing one of the numbers in the set $\{ 1, 2, \ldots, p \}$. Then for each cell, we can choose any of the $a$ colors. Thus the total number of color combinations is $a^p$, but we must subtract the $a$ cases where we have a monochromatic coloring. Thus the ways to color the numbers $\{ 1, 2, \ldots, p \}$ each being assigned one of $a$ colors, where not all numbers are allowed to be assigned the same color is $a^p - a$. □

# Chapter 8: Final Comments

While the work detailed previously show how diverse the proofs of Fermat's Little Theorem and Wilson's Theorem can be, it is important to note the theorems' practical applications.

In his text, An Introduction to Cryptography [12] Richard A. Mollin defines cryptography and *the study of methods for sending messages . . . in enciphered or disguised form. . . so that only the intended recipient can . . . decipher it.* One specific type of cryptography is Public-Key Cryptography. Mollin defines this as

*a cryptosystem consisting of a set of enciphering transformations . . . and a set of deciphering transformations . . . [where] for each pair* $(e, d)$ *the enciphering key* $e$*, called the public key, is made publicly available, while the deciphering key* $d$*, called the private key, is kept secret. The cryptosystem must satisfy the property that it is computationally infeasible to compute* $d$ *from* $e$ [12, p.137].

The most widely used public-key cryptosystem is the RSA Algorithm, named after its developers R. Rivest, A. Shamir, and L. Adleman. The algorithm was invented in 1978 and relies heavily on Fermat's Little Theorem and the Chinese Remainder Theorem.

The following description of the RSA Cryptosystem can be found in Burton's Elementary Number Theory [5], however it has been edited for clarity for the reader:

First, a user of the RSA system much choose a pair of distinct primes $p$ and $q$ large enough so that their product, $n$, is unable to be factored with current computer technology, i.e. the primes should be more than 100 digits in length. Their product $n$ is denoted as the *enciphering modulus*. Next, the user must choose an integer, $k$,

referred to as the *enciphering exponent* such that $\gcd(k, \Phi(n)) = 1$. Then the pair $(n, k)$ is placed in a public file as the user's encryption key.

Before a message is encrypted, a "digital alphabet" must be determined, where each letter, space, and punctuation mark is given a numerical representation. Burton [5, p.142] gives the following as a standard assignment:

| | | | |
|---|---|---|---|
| A=01 | K=11 | U=21 | 1=31 |
| B=02 | L=12 | V=22 | 2=32 |
| C=03 | M=13 | W=23 | 3=33 |
| D=04 | N=14 | X=24 | 4=34 |
| E=05 | O=15 | Y=25 | 5=35 |
| F=06 | P=16 | Z=26 | 6=36 |
| G=07 | Q=17 | ,=27 | 7=37 |
| H=08 | R=18 | .=28 | 8=38 |
| I=09 | S=19 | ?=29 | 9=39 |
| J=10 | T=20 | 0=30 | !=40 |

with 00 indicating a space between words. Thus with this alphabet, the message

*Leibniz deserves more credit.*

is transformed into

$$M = 1205090214092600040519051822051900131518050003180504092028 \quad .$$

For a person wishing to send a message to a user, he must first obtain the user's public key and then translate $M$ to the ciphertext number $r$ by raising $M$ to the $k$th power and then reducing the result modulo $n$ :

$$M^k \equiv r \pmod{n}.$$

The intended recipient must first determine the integer $j$, the recovery exponent, such that

$$kj \equiv 1 \pmod{\Phi(n)}.$$

Since $\gcd(k, \Phi(n)) = 1$, there must be a unique solution modulo $\Phi(n)$. Using the Euclidean Algorithm, one can find this $j$. Since the recovery exponent can only be found by the person who knows $k$ and the prime factorization of $n$ (needed to find $\Phi(n)$, the value of $j$ is secure. Finally, in order to translate $r$ back to $M$, the recipient can find $M$, for

$$r^j \equiv (M^k)^j \equiv M^{(1+\Phi(n)t)} \equiv M(M^{\Phi(n)})^t \equiv M \cdot 1^t \equiv M \pmod{n}.$$

Note that this crucial step is where Fermat's Little Theorem comes into play. We assume that $\gcd(M, n) = 1$. If $M$ and $n$ are not relatively prime, then one can reach the same conclusion via the Chinese Remainder Theorem. (See [5, p. 143])

The following example shows the workings of the RSA Algorithm, but uses unrealistically small primes in order for clarity.

***Example.*** Let $p = 13$ and $q = 29$. Then $n = 377$ which implies

$$\Phi(n) = (13 - 1)(29 - 1) = 336.$$

Now we must choose an integer $k$, the enciphering exponent, such that $\gcd(k, \Phi(n)) = 1$. The number 67 will work. The deciphering exponent, $j$, must satisfy

$$kj \equiv 1 \pmod{\Phi(n)}.$$

Thus by the Euclidean Algorithm, we may take $j = -5 \equiv 331 \pmod{336}$.

We can encrypt the following message using the digital alphabet listed above:

HELP!

to

$$M = 0805121640 \quad .$$

We next split $M$ into blocks to code, so that each block of numbers is less than $\Phi(n) = 336$. Thus we can split $M$ into blocks of length 2. The first block, 08 encrypts as

$$8^{67} \equiv 148 \pmod{377}.$$

The total encrypted message reads as follows:

$$148216220315300.$$

To decipher the message, for a block $b$, the recipient computes

$$b^{331} \pmod{377}.$$

For example, we can decode 148:

$$148^{331} \equiv 8 \pmod{377}.$$

Another practical application of Fermat's Little Theorem appears in Contemporary Abstract Algebra, Sixth Edition, by Joseph A. Gallian [8, p.142]:

*Fermat's Little Theorem has been used in conjunction with computers to test for primality of certain numbers. One case concerned the number* $p = 2^{257} - 1$. *If* $p$ *is prime we know from Fermat's Little Theorem that* $10^p \equiv 10 \pmod{p}$ *and therefore* $10^{p+1} \equiv 100 \pmod{p}$. *Using multiple precision and a simple loop, a computer was able to calculate* $10^{p+1} \equiv 10^{2^{257}} \pmod{p}$ *in a few seconds. The result was not 100, and so* $p$ *is not prime.*

Thus we have demonstrated two practical applications of Fermat's Little Theorem, the former which was developed in the 1970's shows the relevance to today's mathematical work.

Wilson's Theorem is also very valuable because it is used to prove many other important theorems. Dirichlet's proof of Wilson's Theorem demonstrates this. While

Wilson's Theorem can be used to prove the primality of an integer, $n$, it is not recommended due to the difficulty of such a task for large $n$.

Interesting results also arise when considering the converse of both Fermat's Little Theorem and Wilson's Theorem.

First let us note that the converse of Wilson's Theorem is actually true:

***Theorem 5.1 - Converse of Wilson's Theorem*** *Suppose* $(p-1)! \equiv -1 \pmod{p}$. *Then* $p$ *is a prime.*

**Proof** Assume $p$ is not a prime. For $p = 4$ we have $3! \equiv 2 \pmod{4}$. Assume $p > 4$. Then $p$ can be expressed by two nontrivial factors $m, n$ such that $p = mn$. First, assume that $1 < m < n < p$. Then $mn$ must divide $(p-1)!$. Then $mn \nmid [(p-1)!+1]$, and $(p-1)! \equiv 0 \pmod{p}$. Second, assume that $1 < m = n < p$. Then $m \mid (p-1)!$ which implies $m \nmid [(p-1)!+1]$. Then $mn \nmid [(p-1)!+1]$, and since $2m < m^2 = p$, $(p-1)! \equiv 0 \pmod{p}$. Thus in both cases we have a contradiction, so $p$ must be prime. □

The converse of Fermat's Little Theorem, however, is not true. The converse states: *Let* $\gcd(a, p) = 1$ *and* $a^{p-1} \equiv 1 \pmod{p}$. *Then* $p$ *is a prime.*

In 1909 Carmichael proved there are composite values of $n$ such that $a^{n-1} \equiv 1 \pmod{n}$ holds for every $a$ relatively prime to $n$ [5, p.94]. Such numbers $n$ are aptly named Carmichael numbers, and there are an infinite number of these [1]. An example of a Carmichael number is $561 = 3 \cdot 11 \cdot 17$. Note that if $\gcd(a, 561) = 1$ then

$$\begin{aligned} a^{560} &= (a^2)^{280} \equiv 1 \pmod{3} \\ a^{560} &= (a^{10})^{56} \equiv 1 \pmod{11} \\ a^{560} &= (a^{16})^{35} \equiv 1 \pmod{17}. \end{aligned}$$

By the Chinese Remainder Theorem, $a^{560} \equiv 1 \pmod{561}$.

# Bibliography


[1] Alford, W.R., A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. Math. 140 (1994), 703-722

[2] Anderson, Peter G., Arthur T. Benjamin, and Jeremy A Rouse, *Combinatorial Proofs of Fermat's, Lucas's, and Wilson's Theorems*. The American Mathematical Monthly 112 (2005) No. 3, pg. 266-267.

[3] Benjamin, Arthur T. and Jennifer J. Quinn Proofs that Really Count. The Mathematical Association of America, 2003

[4] Bogart, Kenneth P. Introductory Combinatorics, Third Edition. Academic Press, San Diego, 2000.

[5] Burton, David M. Elementary Number Theory, Third Edition. Wm. C. Brown Publishers, 1994.

[6] Comtet, Louis Advanced Combinatorics. D. Reidel Publishing Company, Dordrecht, Holland,1974

[7] Dickson, L.E. History of the Theory of Numbers, Volume 1. Chelsea Publishing Company, New York, 1952

[8] Gallian, Joseph A. Contemporary Abstract Algera, Sixth Edition. D. C. Heath and Company, 1990.

[9] Gauss, Carl Friedrich (tr. Arthur A. Clarke). Disquisitiones Aritmeticae. Yale University Press, 1965

[10] Grosswald, Emil Topics from the Theory of Numbers, Second Edition. Birkauser Boston, 1984

[11] Hillman, Abraham P. and Gerald L. Alexanderson Abstract Algebra A First Undergraduate Course, Fifth Edition. International Thomas Publishing, 1994

[12] Mollin, Richard A. An Introduction to Cryptography. Chapman & Hall/CRC, Boca Raton, 2001

[13] Robbins, Neville Beginning Number Theory, Second Edition. Jones and Bartlett Publishers, Inc., Sudbury, MA. 2006

[14] Waring, E. Meditationes Algebraicae Cambridge, England, 1770.

# Vita

Caroline LaRoche Turnage grew up in Gaffney, South Carolina. She graduated in 2006 from Wofford College, Spartanburg, South Carolina with a Bachelor of Arts in Mathematics and French, *magna cum laude*. She was honored as a Wofford Scholar, Presidential Seminar member, and recipient of the South Carolina LIFE Scholarship, 1854 Scholarship, E. B. Hamer, Jr. Scholarship, and Hucks-Jones Scholarship. After graduation she entered Wake Forest University as a full time student, obtaining a Master of Arts degree in Mathematics in 2008. At Wake Forest she was inducted into the Mathematical honor society Pi Mu Epsilon. She is also a member of the American Mathematical Society and the Association for Women in Mathematics.