5-13-2008

On a conjecture involving Fermat's Little Theorem

John Clark
University of South Florida

On a Conjecture Involving Fermat's Little Theorem

by

John Clark

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Arts
Department of Mathematics and Statistics
College of Arts and Sciences
University of South Florida

Major Professor: Stephen Suen, Ph.D.
Mohamed Elhamdadi, Ph.D.
Arthur Danielyan, Ph.D.

Date of Approval:
May 13, 2008

Keywords: Number Theory, Prime Numbers, Divisibility,
Congruences, Sums of Powers of Consecutive Integers

To my wonderful fiancée Marcia, your love and support kept me going.

ACKNOWLEDGEMENTS

I would like to extend a special thank you to Dr. Stephen Suen. I am truly grateful for your encouragement, guidance, and hard work.

TABLE OF CONTENTS

LIST OF FIGURES

ON A CONJECTURE INVOLVING FERMAT'S LITTLE THEOREM

JOHN CLARK

ABSTRACT

Using Fermat's Little Theorem, it can be shown that $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$ if m is prime. It has been conjectured that the converse is true as well. Namely, that $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$ only if m is prime. We shall present some necessary and sufficient conditions for the conjecture to hold, and we will demonstrate that no counterexample exists for $m \leq 10^{12}$.

1. INTRODUCTION

"Mathematics is the queen of the sciences and number theory is the queen of mathematics." So says Carl Friedrich Gauss, a nineteenth century number theorist. Number theory, the subject of much of his study, is the branch of pure mathematics concerned with the properties and relationships of numbers, specifically integers.

We wish to consider a problem dealing with two concepts from elementary number theory: primality and congruence. Fermat's Little Theorem states that if p is a prime integer and a is a positive integer with $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$. A known consequence of Fermat's Little Theorem is that if p is prime, then $\sum_{i=1}^{p} i^{p-1} \equiv -1 \pmod{p}$. In Kenneth H. Rosen's book *Elementary Number Theory and Its Applications (5th Edition)* [8], readers are tasked to prove this as an exercise on page 221. There, it is conjectured that the converse of the problem is true as well. Namely, that $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$ only if m is prime.

Conjectures like these are common in mathematics. For instance, Wilson's Theorem states that if p is a prime integer, then $(p-1)! \equiv -1 \pmod{p}$. It turned out that the converse was true as well. Namely, that if $n > 1$ is a positive integer, then $(n-1)! \equiv -1 \pmod{n}$ only if n is prime. Our goal is very similar. We know that if p is prime, then $\sum_{i=1}^{p} i^{p-1} \equiv -1 \pmod{p}$, and we would like to prove that if m is a positive integer, then $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$ only if m is prime.

While unable to prove the conjecture, we can prove that m must satisfy some strong conditions in order for the congruence to hold. We state these necessary and sufficient conditions as a theorem.

Theorem 1.1. *Let $m \geq 3$ be an integer. Then, $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$ if and only if m is a product of distinct odd primes such that $m \equiv p \pmod{p^2(p-1)}$ for each prime divisor p of m.*

The next three thoerems are consequences of Theorem 1.1.

Theorem 1.2. *Let $m \geq 3$ be an integer and let p_1, p_2 be any two prime divisors of m. If $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then $p_2 \not\equiv 1 \pmod{p_1}$.*

Theorem 1.3. *Let $m \geq 3$ be an integer. If $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then m cannot be a product of two primes.*

Theorem 1.4. *Let $m \geq 3$ be an integer. If $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then m cannot be a product of three primes.*

We delay these proofs so that we may present some background definitions and theorems in Chapter 2. In Chapter 3 we will prove Theorem 1.1 using a series of smaller theorems, and then we will prove Theorems 1.2, 1.3, and 1.4. Let us now consider some applications of these theorems.

Consider a positive integer $m \geq 3$ satisfying $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$. If $3 \mid m$, then by Theorem 1.2 no other prime divisor p of m may be congruent to 1 modulo 3. Since m must be a product of distinct odd primes by Theorem 1.1, $p \not\equiv 0 \pmod{3}$, meaning $p \equiv 2 \equiv -1 \pmod{3}$. This means that all other prime divisors of m must be of the form $3k-1$, where k is some positive integer. Since m must be odd, we see that all prime divisors of m other than 3 must actually be of the form $6k-1$. Hence, if $3 \mid m$, then $7 \nmid m$, $13 \nmid m$, $19 \nmid m$, $31 \nmid m$, etc.

Similarly, if $5 \mid m$, then by Theorem 1.2 no other prime divisor of m may be of the form $5k+1$, where k is some positive integer. Since m must be odd, we see that no prime divisor of m may actually be of the form $10k+1$. Thus, if $5 \mid m$, then $11 \nmid m$, $31 \nmid m$, $41 \nmid m$, etc.

Note that Theorems 1.3 and 1.4 imply that any composite m would have to be the product of at least four distinct odd primes, so the smallest possible quadruple of prime divisors of m is $3, 5, 17, 23$. In fact, more can be said. Consider the following example.

Example 1.1. *If $m \geq 3$ is an integer satisfying $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then $m \neq 3 \cdot 5 \cdot 17 \cdot p$, for any prime p.*

Proof. Assume for the purpose of contradiction that such an m exists. From above, $m = 3 \cdot 5 \cdot 17 \cdot p$ implies $p \geq 23$. By Theorem 1.1, $m \equiv p \pmod{p^2(p-1)}$, so we may write $m = p^2(p-1)X + p$ for some positive integer X. That is, $3 \cdot 5 \cdot 17 \cdot p = p^2(p-1)X + p$. Dividing through by p leaves $3 \cdot 5 \cdot 17 = p(p-1)X + 1$. This implies that $p(p-1)X = 3 \cdot 5 \cdot 17 - 1 = 254$. But since $p \geq 23$ and $X \geq 1$, we must have $p(p-1)X \geq 23 \cdot (23-1) \cdot 1 = 506$. This is a contradiction, since $254 \ngeq 506$. Hence, no such m can exist. □

Before considering more examples, we wish to generalize the technique we used in the preceding proof.

Lemma 1.5. *Let $m \geq 3$ and $Q \geq 7$ be integers, and let $p_1 < p_2$ be odd primes. Suppose that $m = Qp_1p_2$ and $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$. Then, $p_1 \leq Q-4$ and $p_2 \leq Q-2$.*

Proof. By Theorem 1.1, $m \equiv p_2 \pmod{{p_2}^2(p_2-1)}$, so we may write $m = {p_2}^2(p_2-1)X + p_2$, where X is some positive integer. Since $m = Qp_1p_2$, we have $Qp_1p_2 = {p_2}^2(p_2-1)X + p_2$. Dividing through by p_2 gives $Qp_1 = p_2(p_2-1)X + 1$.

It follows that

$$\begin{aligned}
& Qp_1 = p_2(p_2-1)X + 1 \\
\Rightarrow\ & Qp_1 \geq p_2(p_2-1) + 1 \quad (\text{since } X \geq 1) \\
\Rightarrow\ & Qp_1 \geq (p_1+2)(p_1+2-1) + 1 \quad (\text{since } p_2 \geq p_1 + 2) \\
\Rightarrow\ & Qp_1 \geq (p_1+2)(p_1+1) + 1 \\
\Rightarrow\ & Qp_1 \geq {p_1}^2 + 3p_1 + 3 \\
\Rightarrow\ & {p_1}^2 + 3p_1 - Qp_1 + 3 \leq 0 \\
\Rightarrow\ & {p_1}^2 - (Q-3)p_1 + 3 \leq 0.
\end{aligned}$$

Now by the quadratic formula, this gives

$$\frac{Q-3-\sqrt{(Q-3)^2-12}}{2} \leq p_1 \leq \frac{Q-3+\sqrt{(Q-3)^2-12}}{2}.$$

Hence,

$$\begin{aligned}
& p_1 \leq \frac{Q-3+\sqrt{(Q-3)^2-12}}{2} \\
\Rightarrow\ & p_1 < \frac{Q-3+\sqrt{(Q-3)^2}}{2} \\
\Rightarrow\ & p_1 < \frac{Q-3+(Q-3)}{2} \\
\Rightarrow\ & p_1 < \frac{2(Q-3)}{2} \\
\Rightarrow\ & p_1 < Q-3.
\end{aligned}$$

This implies $p_1 \leq Q-4$, since p_1 is an integer.

It remains to show that $p_2 \leq Q-2$. So, assume for the purpose of contradiction that $p_2 \geq Q-1$. Then,

$$\begin{aligned}
& Qp_1 \geq p_2(p_2-1) + 1 \quad (\text{as before}) \\
\Rightarrow\ & Qp_1 \geq (Q-1)(Q-1-1) + 1 \quad (\text{by assumption}) \\
\Rightarrow\ & Qp_1 \geq (Q-1)(Q-2) + 1 \\
\Rightarrow\ & Qp_1 \geq Q^2 - 3Q + 3 \\
\Rightarrow\ & p_1 \geq Q - 3 + \frac{3}{Q}.
\end{aligned}$$

This implies $p_1 \geq Q-2$ since $3/Q$ is positive and p_1 is an integer.

This contradicts the fact that $p_1 \leq Q-4$. Hence, $p_2 \not\geq Q-1$, meaning $p_2 \leq Q-2$. □

We will use Lemma 1.5 in the next two examples.

Example 1.2. *If $m \geq 3$ is an integer satisfying $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then $m \neq 3 \cdot 5 \cdot p_1 \cdot p_2$, for any two primes p_1 and p_2.*

Proof. Assume for the purpose of contradiction that such an m exists. By Theorem 1.1, m must be a product of distinct odd primes, so we may assume without loss of generality that $5 < p_1 < p_2$. Now letting $Q = 3 \cdot 5 = 15$, we see from Lemma 1.5 that $p_1 \leq 15 - 4 = 11$.

But by Theorem 1.2, $p_1 \neq 7$ and $p_1 \neq 11$ (because $7 \equiv 1 \pmod{3}$ and $11 \equiv 1 \pmod{5}$), so $p_1 > 11$. This contradiction shows that no such m can exist. □

Example 1.3. *If $m \geq 3$ is an integer satisfying $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then $m \neq 5 \cdot 7 \cdot p_1 \cdot p_2$, for any two primes p_1 and p_2.*

Proof. Assume for the purpose of contradiction that such an m exists. By Theorem 1.1, m must be a product of distinct odd primes, and by Theorem 1.2, $p_1, p_2 \neq 3$ (since $7 \equiv 1 \pmod{3}$), so we may assume without loss of generality that $7 < p_1 < p_2$. Now letting $Q = 5 \cdot 7 = 35$, we see from Lemma 1.5 that $p_1 \leq 35 - 4 = 31$ and $p_2 \leq 35 - 2 = 33$.

Now by Theorem 1.2, $p_1, p_2 \neq 11, 29, 31$, so $p_1 > 31$ if $p_1 \neq 13, 17, 19, 23$. Let us consider these four situations.

If $p_1 = 13$, then $5 \cdot 7 \cdot 13 = p_2(p_2 - 1)X + 1$ for some positive integer X. If $p_2 = 17, 19$, or 23, we see that the equality fails to hold, so $p_2 \geq 37$, contradicting the fact that $p_2 \leq 33$. Hence, $p_1 \neq 13$.

Similarly, if $p_1 = 17$, then $5 \cdot 7 \cdot 17 = p_2(p_2 - 1)X + 1$ for some positive integer X. If $p_2 = 19$ or 23, we see that the equality fails to hold, so $p_2 \geq 37$, contradicting the fact that $p_2 \leq 33$. Hence, $p_1 \neq 17$.

If $p_1 = 19$, then $5 \cdot 7 \cdot 19 = p_2(p_2 - 1)X + 1$ for some positive integer X. If $p_2 = 23$, we again see that the equality fails to hold, meaning $p_2 \geq 37$. This contradiction shows that $p_1 \neq 19$.

Finally, if $p_1 = 23$, then $p_2 \geq 37$, contradicting the fact that $p_2 \leq 33$. Hence, $p_1 \neq 23$.

Since $p_1 \neq 13, 17, 19, 23$, we see that $p_1 > 31$, contradicting the fact that $p_1 \leq 31$. This contradiction shows that no such m can exist. □

Using this same technique, with only two cases to check, we can show that $m \neq 3 \cdot 11 \cdot p_1 \cdot p_2$. With significantly more cases to check, we can show that $m \neq 7 \cdot 11 \cdot p_1 \cdot p_2$. Using a slightly different strategy, we can show that $m \neq 3 \cdot 5 \cdot 17 \cdot p_1 \cdot p_2$. This is our next example.

Example 1.4. *If $m \geq 3$ is an integer satisfying $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then $m \neq 3 \cdot 5 \cdot 17 \cdot p_1 \cdot p_2$, for any two primes p_1 and p_2.*

Proof. Assume for the purpose of contradiction that such an m exists. By Theorem 1.1, m must be a product of distinct odd primes, and by Theorem 1.2, $p_1, p_2 \neq 7, 11, 13$, so we may assume without loss of generality that $17 < p_1 < p_2$. Now letting $Q = 3 \cdot 5 \cdot 7 = 255$, we see from Lemma 1.5 that $p_1 \leq 255 - 4 = 251$ and $p_2 \leq 255 - 2 = 253$.

If we apply the method used in the previous example, there will be a lot of cases for us to check. Instead, we can proceed as follows. Recall, Theorem 1.1 tells us that

$$\begin{cases} m \equiv 3 \pmod{3^2(3-1)} \\ m \equiv 5 \pmod{5^2(5-1)} \\ m \equiv 17 \pmod{17^2(17-1)}. \end{cases}$$

That is,

$$\begin{cases} m \equiv 3 \pmod{18} \\ m \equiv 5 \pmod{100} \\ m \equiv 17 \pmod{4624}. \end{cases}$$

We wish to solve this system of congruences. The third line tells us that $m = 4624q + 17$ for some positive integer q. Substituting this into the second line gives $4624q + 17 \equiv 5 \pmod{100}$, which reduces to $24q + 17 \equiv 5 \pmod{100}$ since $4624 \equiv 24 \pmod{100}$. Now,

$$\begin{aligned} 24q + 17 \equiv 5 \pmod{100} &\Rightarrow 24q \equiv -12 \pmod{100} \\ &\Rightarrow 12 \cdot 2q \equiv 12 \cdot (-1) \pmod{100} \\ &\Rightarrow 2q \equiv -1 \pmod{25} \quad \text{(by Theorem 2.21)} \\ &\Rightarrow 2q \equiv 24 \pmod{25} \quad (\text{since } -1 \equiv 24 \pmod{25}) \\ &\Rightarrow q \equiv 12 \pmod{25} \quad \text{(by Corollary 2.22)} \\ &\Rightarrow q = 25\ell + 12, \end{aligned}$$

for some nonnegative integer ℓ.

Since $m = 4624q + 17$, we see $m = 4624(25\ell + 12) + 17 = 115600\ell + 55505$. Substituting this into the first line of our system of congruences gives $115600\ell + 55505 \equiv 3 \pmod{18}$, which reduces to $4\ell + 11 \equiv 3 \pmod{18}$. Now,

$$\begin{aligned} 4\ell + 11 \equiv 3 \pmod{18} &\Rightarrow 4\ell \equiv -8 \pmod{18} \\ &\Rightarrow \ell \equiv -2 \pmod{9} \quad \text{(by Theorem 2.21)} \\ &\Rightarrow \ell \equiv 7 \pmod{9} \\ &\Rightarrow \ell = 9k + 7, \end{aligned}$$

for some nonnegative integer k.

Since $m = 115600\ell + 55505$, we see $m = 115600(9k+7)+55505 = 1040400k+864705 = 3 \cdot 5 \cdot 17 \cdot (3391 + 4080k)$.

Moreover, $m = 3 \cdot 5 \cdot 17 \cdot p_1 \cdot p_2$, so this implies that $p_1 p_2 = 3391 + 4080k$, for some nonnegative integer k. By Lemma 1.5, $p_1 \leq 251$ and $p_2 \leq 253$, so $p_1 p_2 \leq 63503$. This means that $k \leq 14$. Thus, in order to derive a contradiction, we need only check the fifteen cases, $k = 0, 1, 2, \ldots, 14$.

First, if $k = 0$, we would have $p_1 p_2 = 3391$, a prime number. This contradiction shows that $k \neq 0$.

If $k = 1$, we would have $p_1 p_2 = 3391 + 4080 = 7471 = 31 \cdot 241$. But $31 \equiv 1 \pmod{5}$, contradicting Theorem 1.2. Hence, $k \neq 1$.

If $k = 2$, we would have $p_1 p_2 = 3391 + 2 \cdot 4080 = 11551$, a prime number. This contradiction shows that $k \neq 2$.

If $k = 3$, we would have $p_1 p_2 = 3391 + 3 \cdot 4080 = 15631 = 7^2 \cdot 11 \cdot 29$, a product of four primes. This contradiction shows that $k \neq 3$.

If $k = 4$, we would have $p_1 p_2 = 3391 + 4 \cdot 4080 = 19711 = 23 \cdot 857$, contradicting the fact that $p_2 \leq 253$. Hence, $k \neq 4$.

If $k = 5$, we would have $p_1 p_2 = 3391 + 5 \cdot 4080 = 23791 = 37 \cdot 643$, contradicting the fact that $p_2 \leq 253$. Hence, $k \neq 5$.

If $k = 6$, we would have $p_1 p_2 = 3391 + 6 \cdot 4080 = 27871 = 47 \cdot 593$, contradicting the fact that $p_2 \leq 253$. Hence, $k \neq 6$.

If $k = 7$, we would have $p_1 p_2 = 3391 + 7 \cdot 4080 = 31951 = 89 \cdot 359$, contradicting the fact that $p_2 \leq 253$. Hence, $k \neq 7$.

If $k = 8$, we would have $p_1 p_2 = 3391 + 8 \cdot 4080 = 36031 = 137 \cdot 264$, contradicting the fact that $p_2 \leq 253$. Hence, $k \neq 8$.

If $k = 9$, we would have $p_1p_2 = 3391 + 9 \cdot 4080 = 40111$, a prime number. This contradiction shows that $k \neq 9$.

If $k = 10$, we would have $p_1p_2 = 3391 + 10 \cdot 4080 = 44191 = 7 \cdot 59 \cdot 107$, a product of three primes. This contradiction shows that $k \neq 10$.

If $k = 11$, we would have $p_1p_2 = 3391 + 11 \cdot 4080 = 48271$, a prime number. This contradiction shows that $k \neq 11$.

If $k = 12$, we would have $p_1p_2 = 3391 + 12 \cdot 4080 = 52351 = 13 \cdot 4027$, contradicting the fact that $p_2 \leq 253$. Hence, $k \neq 12$.

If $k = 13$, we would have $p_1p_2 = 3391 + 13 \cdot 4080 = 56431$, a prime number. This contradiction shows that $k \neq 13$.

Finally, if $k = 14$, we would have $p_1p_2 = 3391 + 14 \cdot 4080 = 60511 = 11 \cdot 5501$, contradicting the fact that $p_2 \leq 253$. Hence, $k \neq 14$.

Thus, no positive integer k exists so that $m = 3 \cdot 5 \cdot 17 \cdot (3391 + 4080k)$, meaning $m \neq 3 \cdot 5 \cdot 17 \cdot p_1 \cdot p_2$. □

In general, if m is a positive integer satisfying $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, and $p_1 \cdot p_2 \cdots p_{k-2}$ are distinct odd primes, then by checking finitely many cases we can show that $m \neq p_1 \cdot p_2 \cdots p_{k-2} \cdot p_{k-1} \cdot p_k$ for any two primes p_{k-1}, p_k. This follows directly from Lemma 1.5, which places upper bounds on p_{k-1}, p_k.

We mention that the difficulty in producing more examples like the last three is that as the known prime divisors of m increase in magnitude, Theorem 1.2 becomes less useful at ruling out other potential prime divisors, leaving more cases for us to check. So while we need only check finitely many cases, this may still take quite some time. Note that if we allow m to have more than two unknown prime divisors, the difficulty increases significantly.

Luckily, computers can do these types of calculations quite quickly, so in Chapter 4 we will combine our results with some computer programming to demonstrate that no counterexample to the conjecture exists for m less than or equal to one trillion.

In our final example, we wish to exploit the fact we used earlier that any integer must be congruent to either $-1, 0$, or 1, modulo 3. The "specialness" of the small magnitude of 3 will allow us to (partially) overcome the difficulty of considering cases when m has more than two unknown prime divisors.

Example 1.5. *If $m \geq 3$ is an integer satisfying $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then $m \neq 3 \cdot p_1 \cdot p_2 \cdot p_3 \cdots p_r$, for any odd number of primes $p_1, p_2, p_3, \ldots p_r$.*

Proof. Let $m = 3 \cdot p_1 \cdot p_2 \cdot p_3 \cdots p_r$ be an integer satisfying $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$. We will show that r must be even. By Theorem 1.1, m is a product of distinct odd primes and $m \equiv 3 \pmod{3^2(3-1)}$. Thus,

$$m \equiv 3 \pmod{18} \qquad \text{iff} \qquad \frac{m}{3} \equiv 1 \pmod{6},$$

by Theorem 2.21, since $3 \mid m$. Now let $p > 3$ be a prime divisor of m. Recall, by Theorem 1.2, $p = 6k - 1$ for some positive integer k. So,

$$\frac{m}{3} = (6k_1 - 1)(6k_2 - 1) \cdots (6k_r - 1),$$

for some positive integers $k_1, k_2, \ldots, k_r$. Now observe that

$$(6k_1 - 1)(6k_2 - 1) \cdots (6k_r - 1) \equiv (-1)^r \pmod{6}.$$

Thus,

$$\begin{aligned} & \frac{m}{3} \equiv 1 \pmod{6} \\ \Rightarrow \quad & (6k_1 - 1)(6k_2 - 1) \cdots (6k_r - 1) \equiv 1 \pmod{6} \\ \Rightarrow \quad & (-1)^r \equiv 1 \pmod{6}, \end{aligned}$$

which implies that r must be even. □

Specifically, this shows that if m is an integer satisfying $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then $m \neq 3 \cdot p_1 \cdot p_2 \cdot p_3$, for any three primes $p_1 \cdot p_2 \cdot p_3$.

We conclude this chapter by mentioning that the conjecture that $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$ only if m is prime is similar in a sense to the conjecture that a positive integer is perfect only if it is even (an integer is perfect if it is equal to the sum of its proper positive divisors). While mathematicians have been unable to prove that no odd perfect numbers exist, they have proven many conditions that would have to be met in order for an odd integer to be perfect, and they have shown that no odd perfect number less than 10^{300} exists (for more information on the search for an odd perfect number, see <http://oddperfect.org/index.html> [7]). In our case, while we cannot prove the conjecture that $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$ only if m is prime, we can prove some strong conditions on m that must be satisfied for m to be composite, and we will show that no counterexample exists for $m \leq 10^{12}$.

2. BACKGROUND

In this chapter, we present the definitions and theorems that serve as the foundation for our work. Restated here in our own words, these known results can be found in such number theory texts as *Elementary Number Theory* by Gareth Jones [4], *Elementary Number Theory with Applications* by Thomas Koshy [5], *Elementary Introduction to Number Theory* by Calvin Long [6], and *Elementary Number Theory and Its Applications* by Kenneth Rosen [8]. For brevity, we shall only include some of the more interesting proofs.

We begin with the concept of divisibility.

Definition. *If a and b are integers, then we say that a divides b if there is an integer c such that $b = ac$. If a divides b, we also say that a is a divisor or factor of b and that b is a multiple of a. If a divides b we write $a \mid b$, and if a does not divide b we write $a \nmid b$.*

The following are three well-known properties of divisibility.

Theorem 2.1. *If $a, b,$ and c are integers with $a \mid b$ and $b \mid c$, then $a \mid c$.*

Theorem 2.2. *If $a, b, m,$ and n are integers, and if $c \mid a$ and $c \mid b$, then $c \mid (ma+nb)$.*

Theorem 2.3. *The Division Algorithm. If a and b are integers such that $b > 0$, then there are unique intergers q and r such that $a = bq + r$ with $0 \leq r < b$.*

Definition. *In the division algorithm (above), we call q the quotient and r the remainder. We also call a the dividend and b the divisor.*

We can use divisibility to classify numbers as even or odd.

Definition. *Let n be an integer. If the remainder when n is divided by 2 is 0, then $n = 2k$ for some integer k, and we say that n is even. If the remainder when n is divided by 2 is 1, then $n = 2k + 1$ for some integer k, and we say that n is odd.*

Divisibility can also be used to classify numbers as prime or composite.

Definition. *A prime is a positive integer greater than 1 that is divisible by no positive integers other than 1 and itself.*

Definition. *A positive integer greater than 1 that is not prime is called composite.*

Let us consider some properties of primes.

Theorem 2.4. *Every positive integer greater than* 1 *has a prime divisor.*

Theorem 2.5. *There are infinitely many primes.*

Theorem 2.6. *If n is a composite integer, then n has a prime factor not exceeding $\sqrt{n}$.*

Definition. *If x is a real number, then the prime counting function $\pi(x)$ denotes the number of primes not exceeding x.*

Theorem 2.7. *The Prime Number Theorem. If x is a real number, then $\pi(x)$ is asymptotic to $x/\ln(x)$.*

The Prime Number Theorem has an interesting corollary. Consider the set of all positive integers less than or equal to some large positive integer x. By the theorem, we would expect about $x/\ln(x)$ primes to be in this collection of x integers. So, if we randomly select an integer from this set, the probability that we will select a prime number is approximately

$$\frac{x/\ln(x)}{x} = 1/\ln(x).$$

We now consider greatest common divisors.

Definition. *The greatest common divisor of two integers a and b, which are not both* 0*, is the largest integer that divides both a and b. The greatest common divisor of a and b is denoted* $\gcd(a, b)$*. We define* $\gcd(0, 0) = 0$.

Theorem 2.8. *Let a and p be integers with p prime. If $p \nmid a$, then* $\gcd(a, p) = 1$.

Proof. Since p is prime, the only positive divisors of p are 1 and p. So either $\gcd(a, p) = 1$, or $\gcd(a, p) = p$. If $\gcd(a, p) = p$, then $p \mid a$, contrary to our assumption. Hence, we must have $\gcd(a, p) = 1$. □

Definition. *Two integers a and b are relatively prime if* $\gcd(a, b) = 1$.

Theorem 2.9. *If a and b are integers with* $\gcd(a, b) = d$ *and $d \geq 1$, then* $\gcd(a/d, b/d) = 1$.

Theorem 2.10. *If a, b, and c are integers, then* $\gcd(a + cb, b) = \gcd(a, b)$.

Definition. *If a and b are integers, then a linear combination of a and b is a sum of the form $ma + nb$, where both m and n are integers.*

Theorem 2.11. *The greatest common divisor of the integers a and b, not both* 0*, is the least positive integer that is a linear combination of a and b.*

Theorem 2.12. *If a and b are integers, not both* 0*, then a positive integer d is the greatest common divisor of a and b if and only if:*

(i) $d \mid a$ and $d \mid b$.

(ii) if c is an integer with $c \mid a$ and $c \mid b$, then $c \mid d$.

Theorem 2.13. *If a, b, and c are integers with $\gcd(a, c) = 1$, then $\gcd(a, b) = \gcd(a, bc)$.*

Proof. Let $d = \gcd(a, b)$. Clearly $d \leq \gcd(a, bc)$. We want to show that $d \geq \gcd(a, bc)$.

By Theorem 2.11, since $\gcd(a, b) = d$ and $\gcd(a, c) = 1$, we may write $d = as + bt$ and $1 = au + cv$, for some integers s, t, u, v.

Now, $d = (as + bt) = (as + bt) \cdot 1 = (as + bt)(au + cv) = aQ_1 + bcQ_2$ for some integers Q_1, Q_2. This is a linear combination of a and bc, and we know from Theorem 2.11 that $\gcd(a, bc)$ is the *smallest* linear combination of a and bc, so $d \geq \gcd(a, bc)$.

Since $d \geq \gcd(a, bc)$ and $d \leq \gcd(a, bc)$, we conclude that $d = \gcd(a, bc)$. □

The next two definitions allow us to consider the greatest common divisor of more than two integers.

Definition. *Let $a_1, a_2, \ldots, a_n$ be integers, not all zero. The greatest common divisor of these integers is the largest integer that is a divisor of all of the integers in the set. The greatest common divisor of $a_1, a_2, \ldots, a_n$ is denoted $\gcd(a_1, a_2, \ldots, a_n)$. We define $\gcd(0, 0, \ldots, 0) = 0$.*

Definition. *We say that the integers $a_1, a_2, \ldots, a_n$ are mutually relatively prime if $\gcd(a_1, a_2, \ldots, a_n) = 1$. These integers are called pairwise relatively prime if for each pair of integers a_i and a_j from the set (with $i \neq j$), we have $\gcd(a_i, a_j) = 1$.*

The following theorem makes use of the greatest common divisor and will be useful to us in Chapter 3.

Theorem 2.14. *Let a and b be integers with $\gcd(a, b) = d$. Then, the equation $ax + by = c$ has no integer solutions for x and y if $d \nmid c$. If $d \mid c$, then there are infinitely many integer solutions.*

The next three theorems concern the funadmental theorem of arithmetic.

Theorem 2.15. *If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.*

Theorem 2.16. *If p divides $a_1 a_2 \cdots a_n$ where p is a prime and $a_1, a_2, \ldots, a_n$ are positive integers, then there is an integer i with $1 \leq i \leq n$ such that p divides a_i.*

Theorem 2.17. *The Fundamental Theorem of Arithmetic. Every positive integer greater than 1 can be written uniquely as a product of primes, with the prime factors in the product written in nondecreasing order.*

Proof. Our proof is in two parts. First, we shall prove existence. Assume for the purpose of contradiction that there is at least one positive integer greater than 1 that cannot be written as the product of primes. Let n be the smallest such counterexample (the positive integers are well-ordered, so the least element of a nonempty set of positive integers exists). If n is prime, then we are done, so assume that n is composite. Write $n = ab$, with $1 < a < n$ and $1 < b < n$.

Since a and b are less than n, they must each be a product of primes since n is the *smallest* integer that is not a product of primes. But $n = ab$, so if a and b are products of primes, then n must also be a product of primes. This is a contradiction. Thus, no such counterexample n can exist, meaning every positive integer greater than 1 can be written as a product of primes.

It remains to show that every positive integer has a unique factorization. Assume for the purpose of contradiction that there is an integer m that has two different factorizations into primes. Say, $m = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$, with $p_1 \leq p_2 \leq \cdots \leq p_s$ and $q_1 \leq q_2 \leq \cdots \leq q_t$, where $p_1 p_2 \cdots p_s$ and $q_1 q_2 \cdots q_t$ are all primes. We wish to show that such an m cannot exist.

We can remove all common primes from the two factorizations to obtain

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$$

where the primes on the left-hand side of this equation differ from those on the right-hand side, and where $u \geq 1$ and $v \geq 1$. Now since p_{i_1} divides $p_{i_1} p_{i_2} \cdots p_{i_u}$, we have p_{i_1} divides $q_{j_1} q_{j_2} \cdots q_{j_v}$. By Theorem 2.16, p_{i_1} must divide q_{j_k} for some k between 1 and v, but this is impossible since each q_{j_k} is prime and is different from p_{i_1}. Hence, no such m can exist. □

We now consider least common multiples.

Definition. *The least common multiple of two nonzero integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted* $\operatorname{lcm}(a, b)$. *When at least one of a, b is zero, we define* $\operatorname{lcm}(a, b) = 0$.

Theorem 2.18. *If a and b are postive integers, then* $\operatorname{lcm}(a, b) = ab/\gcd(a, b)$.

Definition. *The least common multiple of the nonzero integers $a_1, a_2, \ldots, a_n$ is the smallest positive integer that is divisible by all the integers $a_1, a_2, \ldots, a_n$. It is denoted* $\operatorname{lcm}(a_1, a_2, \ldots, a_n)$. *When at least one of $a_1, a_2, \ldots, a_n$ is zero, we define* $\operatorname{lcm}(a_1, a_2, \ldots, a_n) = 0$.

We now move on to the topic of congruence.

Definition. *Let a, b, and m be integers with $m > 0$. If $m \mid (a - b)$ we say that a is congruent to b modulo m, denoted* $a \equiv b \pmod{m}$. *If $m \nmid (a - b)$, we say that a and b are incongruent modulo m, denoted* $a \not\equiv b \pmod{m}$.

The next two theorems cover some basic properties of congruence.

Theorem 2.19. *If a and b are integers, then $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.*

Theorem 2.20. *Let m be a positive integer. Congruences modulo m satisfy the following properties:*

(i) Reflexive property. If a is an integer, then $a \equiv a \pmod{m}$.
(ii) Symmetric property. If a and b are integers such that $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
(iii) Transitive property. If a, b and c are integers with $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

The next three items concern modular arithmetic.

Theorem 2.21. *Let a, b, c, and m be integers with $m > 0$, and let $d = \gcd(c, m)$. Then,*

$$ac \equiv bc \pmod{m} \qquad \textit{iff} \qquad a \equiv b \pmod{m/d}.$$

Corollary 2.22. *Let a, b, c, and m be integers with $m > 0$, and let $\gcd(c, m) = 1$. Then,*

$$ac \equiv bc \pmod{m} \qquad \textit{iff} \qquad a \equiv b \pmod{m}.$$

Theorem 2.23. *If a, b, c, d, and m are integers such that $m > 0, a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$, then*

(i) $a + c \equiv b + d \pmod{m}$,
(ii) $a - c \equiv b - d \pmod{m}$,
(iii) $ac \equiv bd \pmod{m}$.

We now consider systems of residues.

Definition. *A complete system of residues modulo m is a set of integers such that for each $x \in \mathbb{Z}$, x is congruent modulo m to exactly one integer of the set.*

Lemma 2.24. *A set of m incongruent integers modulo m forms a complete set of residues modulo m.*

Theorem 2.25. *If $r_1, r_2, \ldots, r_m$ is a complete set of residues modulo m, and if a is a positive integer with $\gcd(a, m) = 1$, then*

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

is a complete system of residues modulo m for any integer b.

The next three items concern additional ways to manipulate congruences.

Theorem 2.26. *If a, b, k and m are integers such that $k > 0, m > 0$, and $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$.*

Theorem 2.27. *Let $a, b, m_1, m_2, \ldots, m_k$ be integers with $m_1, m_2, \ldots, m_k$ positive. Then, $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$ if and only if $a \equiv b \pmod{\text{lcm}(m_1, m_2, \ldots, m_k)}$.*

Corollary 2.28. *Let $a, b, m_1, m_2, \ldots, m_k$ be integers with $m_1, m_2, \ldots, m_k$ positive and pairwise relatively prime. Then, $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$ if and only if $a \equiv b \pmod{m_1 m_2 \cdots m_k}$.*

We now move on to the concept of linear congruences.

Definition. *A congruence of the form $ax \equiv b \pmod{m}$, where x is an unknown integer, is called a linear congruence in one variable.*

The following theorem states how many solutions a given linear congruence has, if any.

Theorem 2.29. *Let a, b, x, and m be integers such that $m > 0$, and let $\gcd(a, m) = d$. If $d \nmid b$, then $ax \equiv b \pmod{m}$ has no solutions. If $d \mid b$, then $ax \equiv b \pmod{m}$ has exactly d incongruent solutions modulo m.*

This theorem can be generalized to apply to a system of linear congruences.

Theorem 2.30. *Let $x, a_1, a_2, \ldots, a_r$ be integers and $m_1, m_2, \ldots, m_r$ be positive integers. Then, the system of 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 solution if and only if $\gcd(m_i, m_j) \mid (a_i - a_j)$ for all pairs of integers i, j, where $1 \leq i < j \leq r$. Furthermore, if a solution exists, then it is unique modulo $\text{lcm}(m_1, m_2, \ldots, m_r)$.

We now consider some special congruences.

Theorem 2.31. *Wilson's Theorem. If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.*

Theorem 2.32. *If n is a positive integer with $n \geq 2$ such that $(n-1)! \equiv -1 \pmod{n}$, then n is prime.*

Theorem 2.33. *Fermat's Little Theorem. If p is prime and a is a positive integer with $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Consider the $p-1$ integers $a, 2a, \ldots, (p-1)a$. Since $p \nmid a$, none of these integers is divisible by p, and no two of these integers are congruent modulo p.

Because the integers $a, 2a, \ldots, (p-1)a$ are a set of $p-1$ -many integers all incongruent to 0, and no two are congruent modulo p, by Lemma 2.24 we know that the least positive residues of $a, 2a, \ldots, (p-1)a$, taken in some order, must be the integers $1, 2, \ldots, p-1$. As a consequence, the product of the integers $a, 2a, \ldots, (p-1)a$ is congruent modulo p to the product of the first $p-1$ positive integers. Hence,

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

That is,

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

Now using Corollary 2.22, we may cancel the $(p-1)!$ from both sides leaving

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

□

We now introduce Euler's phi-function and three related theorems.

Definition. *Let n be a positive integer. The Euler phi-function $\phi(n)$ is defined to be the number of positive integers not exceeding n that are relatively prime to n.*

Theorem 2.34. *If p is prime, then $\phi(p) = p - 1$.*

Theorem 2.35. *If p is prime and n is a positive integer, then $\phi(p^n) = p^n - p^{n-1}$.*

Theorem 2.36. *Euler's Theorem. If m is a positive integer and a is an integer with $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Using Euler's phi-function, we can define a reduced residue system.

Definition. *A reduced residue system modulo n is a set of $\phi(n)$ integers such that each element of the set is relatively prime to n, and no two different elements of the set are congruent modulo n.*

Let us now consider orders of integers.

Definition. *Let a and n be relatively prime positive integers. Then, the least positive integer x such that $a^x \equiv 1 \pmod{n}$ is called the order of a modulo n.*

Theorem 2.37. *Let a, n, i, and j be integers such that a and n are relatively prime and n, i, and j are nonnegative. If x is the order of a modulo n, then $a^i \equiv a^j \pmod{n}$ if and only if $i \equiv j \pmod{x}$.*

We now introduce primitive roots.

Definition. *Let r and n be relatively prime integers with $n > 0$. If the order of r modulo n is equal to $\phi(n)$, then r is called a primitive root modulo n.*

Theorem 2.38. *Let r and n be relatively prime positive integers with $n > 0$. If r is a primitive root modulo n, then the integers $r^1, r^2, \ldots, r^{\phi(n)}$ form a reduced residue set modulo n.*

Now, let us consider the roots of polynomial congruences.

Definition. *Let $f(x)$ be a polynomial with integer coefficients. An integer c is a root of $f(x)$ modulo m if $f(c) \equiv 0 \pmod{m}$.*

Theorem 2.39. *Lagrange's Theorem. Let p be prime and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0$ be a polynomial of degree $n \geq 1$ with integer coefficients. If $p \nmid a_n$, then $f(x)$ has at most n incongruent roots modulo p.*

Proof. We use proof by induction. When $n = 1$, we have $f(x) = a_1 x + a_0$ with $p \nmid a_1$. A root of $f(x)$ modulo p is a solution of the linear congruence $a_1 x \equiv -a_0 \pmod{p}$. By Theorem 2.29, since $\gcd(a_1, p) = 1$, we know this linear congruence has exactly one solution. This implies that there is exactly one root modulo p of $f(x)$. Hence, Lagrange's Theorem is true when $n = 1$.

Now, suppose that the theorem is true for polynomials of degree $n - 1$, and let $f(x)$ be a polynomial of degree n with leading coefficient not divisible by p. Assume for the purpose of contradiction that $f(x)$ has $n+1$ -many incongruent roots modulo p, say $c_0, c_1, \ldots, c_n$, so that $f(c_k) \equiv 0 \pmod{p}$ for $k = 0, 1, \ldots, n$. We have

$$\begin{aligned} f(x) - f(c_0) &= a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \cdots + a_1(x - c_0) \\ &= a_n(x - c_0)(x^{n-1} + xn - 2c_0 + \cdots + xc_0^{n-2} + c_0^{n-1}) \\ &\quad + a_{n-1}(x - c_0)(x^{n-2} + xn - 3c_0 + \cdots + xc_0^{n-3} + c_0^{n-2}) \\ &\quad + \cdots + a_1(x - c_0) \\ &= (x - c_0)g(x), \end{aligned}$$

where $g(x)$ is a polynomial of degree $n - 1$ with leading coefficient a_n. We now show that $c_1, c_2, \ldots, c_n$ are all roots of $g(x)$ modulo p. Let k be an integer with $1 \leq k \leq n$. Because $f(c_k) \equiv f(c_0) \equiv 0 \pmod{p}$, we have

$$f(c_k) - f(c_0) = (c_k - c_0)g(c_k) \equiv 0 \pmod{p}.$$

It follows that $g(c_k) \equiv 0 \pmod{p}$, because $c_k - c_0 \not\equiv 0 \pmod{p}$. Hence, c_k is a root of $g(x)$ modulo p. This shows that the polynomial $g(x)$, which is of degree $n-1$ and has leading coefficient not divisible by p, has n -many incongruent roots modulo p. This contradicts our induction hypothesis. Hence, $f(x)$ must have no more than n -many incongruent roots modulo p. Thus, Lagrange's Theorem is true for all $n \geq 1$. □

The remaining items are all consequences of Lagrange's Theorem. Note that Theorem 2.40 is our own work because we do not find it in standard texts.

Theorem 2.40. *Let p be prime and let $f(x)$ be a polynomial of degree $n \geq 1$ with integer coefficients. Let $a_n \not\equiv 0 \pmod{p}$ be the leading coefficient of $f(x)$ and assume that $x_1, x_2, \ldots, x_n$ are n incongruent roots of $f(x)$ modulo p. Now, let $R(x) = f(x) - a_n(x - x_1)(x - x_2)\cdots(x - x_n)$. Then, the coefficients of $R(x)$ are all congruent to 0 modulo p.*

Proof. Let m be the degree of $R(x)$, and write $R(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$, where $m < n$. Since $x_1, x_2, \ldots, x_n$ are n incongruent roots of $f(x)$ modulo p, and $x_1, x_2, \ldots, x_n$ are n incongruent roots of $a_n(x - x_1)(x - x_2)\cdots(x - x_n)$ modulo p, it must be the case that $x_1, x_2, \ldots, x_n$ are n incongruent roots of $R(x) = f(x) - a_n(x - x_1)(x - x_2)\cdots(x - x_n)$ modulo p.

Now if the degree of $R(x)$ is 0, then $R(x) = a_0$. But $x_1, x_2, \ldots, x_n$ are n incongruent roots of $R(x)$ modulo p, so this must mean that $a_0 \equiv 0 \pmod{p}$.

Now assume that the degree of $R(x)$ is greater than 0. That is, assume $m \geq 1$. By Lagrange's Theorem, if $p \nmid a_m$ then $R(x)$ has at most m incongruent roots modulo p. But $x_1, x_2, \ldots, x_n$ are n incongruent roots of $R(x)$ modulo p, and $n > m$, so it cannot be the case that $p \nmid a_m$. This means that we must have $a_m \equiv 0 \pmod{p}$. This implies that $R(x) \equiv a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1 x + a_0 \pmod{p}$.

But $x_1, x_2, \ldots, x_n$ are still n incongruent roots of $a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1 x + a_0$ modulo p, so again by Lagrange we must have $a_{m-1} \equiv 0 \pmod{p}$. Continuing in this manner, we have $a_i \equiv 0 \pmod{p}$ for $i = 1, 2, \ldots, m$. That is, $R(x) \equiv a_0 \pmod{p}$. But as we demonstrated in the case when the degree of $R(x)$ was assumed to be 0, this must mean that $a_0 \equiv 0 \pmod{p}$.

Thus, all the coefficients of $R(x)$ must be congruent to 0 modulo p. □

Theorem 2.41. *Let p be prime and let d be a divisor of $p - 1$. Then, the polynomial $f(x) = x^{\frac{p-1}{d}} - 1$ has exactly $\frac{p-1}{d}$ incongruent roots modulo p.*

Proof. Since d divides $p - 1$, we may write $p - 1 = dq$, for some positive integer q. Then,

$$x^{p-1} - 1 = (x^q - 1)(x^{q(d-1)} + x^{q(d-2)} + \cdots + x^q + 1) = (x^q - 1)g(x).$$

By Fermat's little theorem, $x^{p-1} - 1$ has $p-1$ incongruent roots modulo p. From above, any root of $x^{p-1} - 1$ modulo p must either be a root of $x^q - 1$ modulo p, or a root of $g(x)$ modulo p. Now by Lagrange's theorem, $g(x)$ has at most $q(d-1) = dq - q = p - 1 - q$ incongruent roots modulo p.

Since $x^{p-1} - 1$ has $p - 1$ incongruent roots modulo p, and $g(x)$ has at most $p - 1 - q$ roots modulo p, this means that $x^q - 1$ has at least $p - 1 - (p - 1 - q) = q$ incongruent roots modulo p. But by Lagrange's theorem, $x^q - 1$ has at most q incongruent roots modulo p. Hence, $x^q - 1$ has exactly q incongruent roots modulo p.

Now $p-1 = dq$ implies $q = \frac{p-1}{d}$, so $x^{\frac{p-1}{d}} - 1$ has exactly $\frac{p-1}{d}$ incongruent roots modulo p, as desired. $\square$

Lemma 2.42. *Let p be prime and let d be a positive divisor of $p-1$. Then, the number of positive integers less than p of order d modulo p does not exceed $\phi(d)$.*

Theorem 2.43. *Let p be prime and let d be a divisor of $p-1$. Then, the number of incongruent integers of order d modulo p is equal to $\phi(d)$.*

Corollary 2.44. *Every prime has a primitive root.*

3. RESULTS

3.1 Overview

The tools we have presented in the previous chapter will allow us to prove Theorems 1.1, 1.2, 1.3, and 1.4. Recall, Theorem 1.1 states:

Let $m \geq 3$ be an integer. Then, $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$ if and only if m is a product of distinct odd primes such that $m \equiv p \pmod{p^2(p-1)}$ for each prime divisor p of m.

Our proof of this theorem relies on four smaller results. We list them here, and prove them in the subsequent sections of this chapter.

Theorem 3.1. *Let $m \geq 3$ be an integer. If $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then m must be a product of distinct primes.*

Theorem 3.2. *Let $m \geq 3$ be an integer. If $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then m must be odd.*

Theorem 3.3. *Let $m \geq 3$ be an integer. If $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then $m \equiv p \pmod{p^2(p-1)}$ for each prime divisor p of m.*

Theorem 3.4. *Let $m \geq 3$ be an integer. If m is a product of distinct odd primes such that $m \equiv p \pmod{p^2(p-1)}$ for each prime divisor p of m, then $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$.*

Clearly these four theorems imply Theorem 1.1. Succeeding the proofs of these four theorems, we will prove the three consequences of Theorem 1.1:

Theorem 1.2. Let $m \geq 3$ be an integer and let p_1, p_2 be any two prime divisors of m. If $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then $p_2 \not\equiv 1 \pmod{p_1}$.

Theorem 1.3. Let $m \geq 3$ be an integer. If $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then m cannot be a product of two primes.

Theorem 1.4. Let $m \geq 3$ be an integer. If $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then m cannot be a product of three primes.

3.2 Proof of Theorem 3.1

In this section, we wish to prove that if $m \geq 3$ is an integer with $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then m must be a product of distinct primes. To this end, we will use the following lemma which will prove helpful throughout the rest of this chapter.

Lemma 3.5. *If m and d are positive integers such that $d \mid m$, then $\sum_{i=1}^{m} i^{m-1} \equiv \frac{m}{d} \sum_{i=1}^{d} i^{m-1} \pmod{d}$.*

Proof. Because $d \mid m$, we may write

$$\sum_{i=1}^{m} i^{m-1} = \sum_{j=0}^{\frac{m}{d}-1} \sum_{i=1}^{d} (jd+i)^{m-1} \equiv \sum_{j=0}^{\frac{m}{d}-1} \sum_{i=1}^{d} i^{m-1} \pmod{d},$$

since $jd + i \equiv i \pmod{d}$. And, since j assumes m/d different values, we have

$$\sum_{j=0}^{\frac{m}{d}-1} \sum_{i=1}^{d} i^{m-1} = \frac{m}{d} \sum_{i=1}^{d} i^{m-1}.$$

□

We are now ready to prove Theorem 3.1, which is stated above.

Proof. With m as in the theorem, write $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ (its prime-power factorization) and let $p^e \in \{p_1^{e_1}, p_2^{e_2}, \ldots, p_k^{e_k}\}$. Assume for the purpose of contradiction that $e \geq 2$.

Since $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$ and $p \mid m$, by Lemma 3.5 we have $\frac{m}{p} \sum_{i=1}^{p} i^{m-1} \equiv -1 \pmod{p}$.

Recall, $p^e \mid m$, so we may write $m = p^e q$ for some $q \in \mathbb{Z}$. Now because $e \geq 2$ it follows that

$$\frac{m}{p} \sum_{i=1}^{p} i^{m-1} = \frac{p^e q}{p} \sum_{i=1}^{p} i^{m-1} = p^{e-1} q \sum_{i=1}^{p} i^{m-1} \equiv 0 \pmod{p}.$$

Since $p \mid m$, we have

$$\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m} \Rightarrow \sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{p},$$

and since $0 \not\equiv -1 \pmod{p}$, we have a contradiction. Hence $e \not\geq 2$, meaning m must be a product of distinct primes. $\square$

In the preceding proof, we showed that $\sum_{i=1}^{m} i^{m-1} \equiv 0 \pmod{p}$. In fact, when $m = p^n$, where p is an odd prime and $n \geq 2$ is an integer, we can actually prove something stronger.

Theorem 3.6. *If p is an odd prime and $n \geq 2$ is an integer, then $\sum_{i=1}^{p^n} i^{p^n-1} \equiv -p^{n-1} \pmod{p^n}$.*

Proof. First, note:

$$\begin{aligned}
\sum_{i=1}^{p^n} i^{p^n-1} &= \sum_{j=0}^{p^{n-1}-1} \sum_{i=1}^{p} (jp+i)^{p^n-1} \\
&= \sum_{j=0}^{p^{n-1}-1} \sum_{i=1}^{p-1} (jp+i)^{p^n-1} + \sum_{j=0}^{p^{n-1}-1} (jp+p)^{p^n-1} \\
&\equiv \sum_{j=0}^{p^{n-1}-1} \sum_{i=1}^{p-1} (jp+i)^{p^n-1} + 0 \pmod{p^n}.
\end{aligned}$$

This congruence holds because

$$\sum_{j=0}^{p^{n-1}-1} (jp+p)^{p^n-1} = \sum_{j=0}^{p^{n-1}-1} ((j+1)p)^{p^n-1} = \sum_{j=1}^{p^{n-1}} (jp)^{p^n-1} = p^{p^n-1} \sum_{j=1}^{p^{n-1}} j^{p^n-1},$$

which is congruent to 0 modulo p^n since it can be shown by induction that $p^n - 1 > n$.

Thus,

$$\sum_{i=1}^{p^n} i^{p^n-1} \equiv \sum_{j=0}^{p^{n-1}-1} \sum_{i=1}^{p-1} (jp+i)^{p^n-1} \pmod{p^n}.$$

Now using binomial expansion, we get

$$\begin{aligned}
\sum_{i=1}^{p^n} i^{p^n-1} &\equiv \sum_{j=0}^{p^{n-1}-1} \sum_{i=1}^{p-1} (jp+i)^{p^n-1} \pmod{p^n} \\
&= \sum_{j=0}^{p^{n-1}-1} \sum_{i=1}^{p-1} \sum_{k=0}^{p^n-1} \binom{p^n-1}{k} (jp)^k i^{p^n-1-k} \\
&= \sum_{j=0}^{p^{n-1}-1} \sum_{i=1}^{p-1} \sum_{k=0}^{p^n-1} \binom{p^n-1}{k} p^k j^k i^{p^n-1-k}.
\end{aligned}$$

Note that when $k \geq n$, this sum is congruent to 0 modulo p^n because of the p^k term. Hence,

$$\sum_{i=1}^{p^n} i^{p^n-1} \equiv \sum_{j=0}^{p^{n-1}-1} \sum_{i=1}^{p-1} \sum_{k=0}^{n-1} \binom{p^n-1}{k} p^k j^k i^{p^n-1-k} \pmod{p^n}.$$

We will now show that when $k > 0$, this sum is congruent to 0 modulo p^n.

Consider,

$$\begin{aligned} & \sum_{j=0}^{p^{n-1}-1} \sum_{i=1}^{p-1} \sum_{k=1}^{n-1} \binom{p^n-1}{k} p^k j^k i^{p^n-1-k} \\ = & \sum_{i=1}^{p-1} \sum_{k=1}^{n-1} \binom{p^n-1}{k} i^{p^n-1-k} \cdot p^k \sum_{j=0}^{p^{n-1}-1} j^k, \end{aligned}$$

and since $\sum_{j=0}^{t-1} j^k = \frac{1}{k+1} \sum_{j=0}^{k} \binom{k+1}{j} B_j (t)^{k-j+1}$, where B_j is the jth Bernoulli number (see for instance page 283 of Graham, Knuth, and Patashnik's *Concrete Mathematics* [3], or <http://mathworld.wolfram.com/BernoulliNumber.html> [9]), we have

$$\begin{aligned} & \sum_{i=1}^{p-1} \sum_{k=1}^{n-1} \binom{p^n-1}{k} i^{p^n-1-k} \cdot p^k \sum_{j=0}^{p^{n-1}-1} j^k \\ = & \sum_{i=1}^{p-1} \sum_{k=1}^{n-1} \binom{p^n-1}{k} i^{p^n-1-k} \cdot \frac{p^k}{k+1} \sum_{j=0}^{k} \binom{k+1}{j} B_j (p^{n-1})^{k-j+1} \\ = & \sum_{i=1}^{p-1} \sum_{k=1}^{n-1} \binom{p^n-1}{k} i^{p^n-1-k} \cdot \frac{1}{k+1} \sum_{j=0}^{k} \binom{k+1}{j} B_j \cdot p^{(n-1)(k-j+1)} \cdot p^k \\ = & \sum_{i=1}^{p-1} \sum_{k=1}^{n-1} \binom{p^n-1}{k} i^{p^n-1-k} \cdot \frac{1}{k+1} \sum_{j=0}^{k} \binom{k+1}{j} B_j \cdot p^{(n-1)(k-j+1)+k} \\ = & \sum_{i=1}^{p-1} \sum_{k=1}^{n-1} \binom{p^n-1}{k} i^{p^n-1-k} \cdot \frac{1}{k+1} \sum_{j=0}^{k} \binom{k+1}{j} B_j \cdot p^{(n-1)(k-j)+n-1+k}. \end{aligned}$$

Now in order to see that this sum is congruent to 0 modulo p^n, consider the largest integer r such that p^r divides $k+1$, the denominator of the fraction. We want to show $p^{(n-1)(k-j)+n-1+k-r} \equiv 0 \pmod{p^n}$ for $k = 1, 2, \ldots, n-1$ and $j = 0, 1, \ldots, k$. So, we need to show $(n-1)(k-j) + n - 1 + k - r \geq n$.

After subtracting n from both sides of this inequality, we see that we only need to show $(n-1)(k-j)+k-1-r \geq 0$.

Recall, it can be shown by induction that for any odd prime p and any positive integer k, $p^k > k+1$. Now since $p^r \mid (k+1)$ implies $p^r \leq k+1$, we must have $r < k$. That is, $r \leq k-1$. So,

$$\begin{aligned}(n-1)(k-j)+k-1-r &\geq (n-1)(k-j)+k-1-(k-1)\\ &= (n-1)(k-j)\\ &\geq 0,\end{aligned}$$

since $n \geq 1$ and $k \geq j \geq 0$.

Thus, we have

$$\begin{aligned}\sum_{i=1}^{p^n} i^{p^n-1} &\equiv \sum_{j=0}^{p^{n-1}-1}\sum_{i=1}^{p-1}\sum_{k=0}^{n-1}\binom{p^n-1}{k}p^k j^k i^{p^n-1-k} \pmod{p^n}\\ &= \sum_{j=0}^{p^{n-1}-1}\sum_{i=1}^{p-1}\sum_{k=1}^{n-1}\binom{p^n-1}{k}p^k j^k i^{p^n-1-k} + \sum_{j=0}^{p^{n-1}-1}\sum_{i=1}^{p-1} i^{p^n-1}\\ &\equiv 0 + \sum_{j=0}^{p^{n-1}-1}\sum_{i=1}^{p-1} i^{p^n-1} \pmod{p^n}\\ &= p^{n-1}\sum_{i=1}^{p-1} i^{p^n-1}.\end{aligned}$$

Now consider the sum $\sum_{i=1}^{p-1} i^{p^n-1}$. Let $q = 1+p+p^2+\cdots+p^{n-1}$ and note that $(p-1)q = p^n-1$. Then,

$$\sum_{i=1}^{p-1} i^{p^n-1} = \sum_{i=1}^{p-1} i^{(p-1)q} = \sum_{i=1}^{p-1}(i^{p-1})^q \equiv \sum_{i=1}^{p-1} 1^q \pmod{p}$$

by Fermat's Little Theorem, since $i^{p-1} \equiv 1 \pmod{p}$ for $i = 1, 2, \ldots, p-1$. Now,

$$\sum_{i=1}^{p-1} 1^q = \sum_{i=1}^{p-1} 1 = p-1 \equiv -1 \pmod{p},$$

so $\sum_{i=1}^{p-1} i^{p^n-1} = Qp - 1$, for some positive integer Q. Thus,

$$\begin{aligned}
\sum_{i=1}^{p^n} i^{p^n-1} &\equiv p^{n-1} \sum_{i=1}^{p-1} i^{p^n-1} \pmod{p^n} \\
&= p^{n-1}(Qp-1) \\
&= Qp^n - p^{n-1} \\
&\equiv 0 - p^{n-1} \pmod{p^n} \\
&= -p^{n-1}.
\end{aligned}$$

Our proof is complete. □

We mention that Theorem 3.6 can alternatively be proved using Stirling numbers of the second kind, instead of Bernoulli numbers (for more information on Stirling numbers, see page 50 of Aigner and Martin's *Discrete Mathematics* [1]).

Note that Theorem 3.6 can be viewed as a generalization of an earlier result. Recall, for any prime p it follows that $\sum_{i=1}^{p} i^{p-1} \equiv -1 \pmod{p}$. Since $\phi(p) = p - 1$, this implies that $\sum_{i=1}^{p} i^{p-1} \equiv \phi(p) \pmod{p}$. More generally, since $\phi(p^n) = p^n - p^{n-1}$, Theorem 3.6 implies that for any positive integer n, we have $\sum_{i=1}^{p^n} i^{p^n-1} \equiv \phi(p^n) \pmod{p^n}$.

3.3 Proof of Theorem 3.2

Now we will show that if $m \geq 3$ is an integer with $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then m must be odd.

Proof. First, m must be a product of distinct primes by Theorem 3.1. Now assume for the purpose of contradiction that m is even. Write $m = 2k$, where $k \geq 3$ is an odd positive integer. Then,

$$\begin{aligned}
\sum_{i=1}^{m-1} i^{m-1} &= \sum_{i=1}^{\frac{m}{2}-1} i^{m-1} + \left(\frac{m}{2}\right)^{m-1} + \sum_{i=\frac{m}{2}+1}^{m-1} i^{m-1} \\
&= \sum_{i=1}^{\frac{m}{2}-1} i^{m-1} + \left(\frac{m}{2}\right)^{m-1} + \sum_{i=1}^{\frac{m}{2}-1} (m-i)^{m-1} \\
&\equiv \sum_{i=1}^{\frac{m}{2}-1} i^{m-1} + \left(\frac{m}{2}\right)^{m-1} + \sum_{i=1}^{\frac{m}{2}-1} (-i)^{m-1} \pmod{m} \\
&= \sum_{i=1}^{\frac{m}{2}-1} i^{m-1} + \left(\frac{m}{2}\right)^{m-1} - \sum_{i=1}^{\frac{m}{2}-1} i^{m-1} \\
&= \left(\frac{m}{2}\right)^{m-1}.
\end{aligned}$$

Recall, $m = 2k$, so

$$\left(\frac{m}{2}\right)^{m-1} = \left(\frac{2k}{2}\right)^{m-1} = k^{m-1}.$$

Now on the one hand, $k^{m-1} \equiv k \pmod{k}$ because $k \mid (k^{m-1} - k)$.

On the other hand, $k^{m-1} \equiv k \pmod{2}$ because $2 \mid (k^{m-1} - k)$ since the difference of two odd integers is even.

Hence, $k^{m-1} \equiv k \pmod{2k}$ by Corollary 2.28.

Since $2k = m$, we have

$$\sum_{i=1}^{m} i^{m-1} \equiv k^{m-1} \equiv k \pmod{m}.$$

But this is a contradiction since we said $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, and $k \not\equiv -1 \pmod{m}$ for $m \geq 3$. Hence, m must be odd. $\square$

3.4 Proof of Theorem 3.3

In this section, we want to prove Theorem 3.3, that if $m \geq 3$ is an integer with $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then $m \equiv p \pmod{p^2(p-1)}$ for each prime divisor p of m. We present the proof as two lemmas.

Lemma 3.7. *Let $m \geq 3$ be an integer. If $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then $m \equiv 1 \pmod{p-1}$ for each prime divisor p of m.*

Proof. By Theorems 3.1 and 3.2, we know that m must be a product of distinct odd primes. By Lemma 3.5, $\sum_{i=1}^{m} i^{m-1} \equiv \frac{m}{p} \sum_{i=1}^{p} i^{m-1} \pmod{p}$, and since $p \equiv 0 \pmod{p}$, we may write

$$\frac{m}{p} \sum_{i=1}^{p} i^{m-1} \equiv \frac{m}{p} \sum_{i=1}^{p-1} i^{m-1} \pmod{p}.$$

Thus,

$$\sum_{i=1}^{m} i^{m-1} \equiv \frac{m}{p} \sum_{i=1}^{p-1} i^{m-1} \equiv -1 \pmod{p}.$$

Now by Corollary 2.44, there exists a primitive root modulo p. Let r be such a primitive root. Recall, by Theorem 2.34 $\phi(p) = p-1$, so by Theorem 2.38 the integers $r^1, r^2, \ldots, r^{p-1}$ form a reduced residue set modulo p. Thus, we may write

$$\frac{m}{p} \sum_{i=1}^{p-1} i^{m-1} \equiv \frac{m}{p} \sum_{j=1}^{p-1} (r^j)^{m-1} = \frac{m}{p} \sum_{j=1}^{p-1} r^{j(m-1)} \pmod{p}.$$

Since r is a primitive root, the order of r modulo p is $p-1$. Hence, by Theorem 2.37 we have

$$r^{j_1(m-1)} \equiv r^{j_2(m-1)} \pmod{p} \qquad \text{iff} \qquad j_1(m-1) \equiv j_2(m-1) \pmod{p-1}.$$

We shall show $m \equiv 1 \pmod{p-1}$ by showing that $\gcd(p-1, m-1) = p-1$, which implies $(p-1) \mid (m-1)$. So, let $d = \gcd(p-1, m-1)$ and assume for the purpose of contradiction that $d < p-1$.

By Theorem 2.21,

$$j_1(m-1) \equiv j_2(m-1) \pmod{p-1} \qquad \text{iff} \qquad j_1 \equiv j_2 \pmod{\frac{p-1}{d}},$$

so it follows that

$$r^{j_1(m-1)} \equiv r^{j_2(m-1)} \pmod{p} \qquad \text{iff} \qquad j_1 \equiv j_2 \pmod{\frac{p-1}{d}}.$$

Now, recall:

$$\sum_{i=1}^{m} i^{m-1} \equiv \frac{m}{p} \sum_{i=1}^{p-1} i^{m-1} \equiv \frac{m}{p} \sum_{j=1}^{p-1} (r^j)^{m-1} = \frac{m}{p} \sum_{j=1}^{p-1} r^{j(m-1)} \pmod{p}.$$

Since $d \mid (p-1)$, we may write

$$\frac{m}{p} \sum_{j=1}^{p-1} r^{j(m-1)} = \frac{m}{p} \sum_{\ell=0}^{d-1} \sum_{j=1}^{\frac{p-1}{d}} r^{(\ell \frac{p-1}{d} + j)(m-1)}.$$

Note that for $\ell = 0, 1, 2, \ldots, d-1$, we have $\ell(\frac{p-1}{d}) + j \equiv j \pmod{\frac{p-1}{d}}$. So, referring to the iff statement above, and letting $j_1 = \ell(\frac{p-1}{d}) + j$ and $j_2 = j$, we see that

$$r^{(\ell \frac{p-1}{d} + j)(m-1)} \equiv r^{j(m-1)} \pmod{p}.$$

Thus,

$$\begin{aligned} \sum_{i=1}^{m} i^{m-1} &\equiv \frac{m}{p} \sum_{\ell=0}^{d-1} \sum_{j=1}^{\frac{p-1}{d}} r^{(\ell \frac{p-1}{d} + j)(m-1)} \pmod{p} \\ &\equiv \frac{m}{p} \sum_{\ell=0}^{d-1} \sum_{j=1}^{\frac{p-1}{d}} r^{j(m-1)} \pmod{p} \\ &= d\Big(\frac{m}{p}\Big) \sum_{j=1}^{\frac{p-1}{d}} r^{j(m-1)}. \end{aligned}$$

In order to derive a contradiction, we will show that $\sum_{j=1}^{\frac{p-1}{d}} r^{j(m-1)} \equiv 0 \pmod{p}$.

To see this, first consider the polynomial congruence $f(x) = x^{\frac{p-1}{d}} - 1 \equiv 0 \pmod{p}$. Since $d \mid (m-1)$ and $j = 1, 2, \ldots, \frac{p-1}{d}$, it follows that

$$(r^{j(m-1)})^{\frac{p-1}{d}} = (r^{p-1})^{\frac{j(m-1)}{d}} \equiv 1^{\frac{j(m-1)}{d}} \pmod{p},$$

by Fermat's Little Theorem.

So, we may think of $x = r^{m-1}, r^{2(m-1)}, \ldots, r^{(\frac{p-1}{d})(m-1)}$ as $\frac{p-1}{d}$ solutions to the polynomial congruence $f(x) = x^{\frac{p-1}{d}} - 1 \equiv 0 \pmod{p}$.

Now since any pair of distinct elements from the set $\{1, 2, \ldots, \frac{p-1}{d}\}$ are incongruent to each other modulo $\frac{p-1}{d}$, it follows from the iff statement above that $r^{j_1(m-1)} \not\equiv r^{j_2(m-1)} \pmod{p}$ for $j = 1, 2, \ldots, \frac{p-1}{d}$.

Hence, $x = r^{m-1}, r^{2(m-1)}, \ldots, r^{(\frac{p-1}{d})(m-1)}$ are $\frac{p-1}{d}$ incongruent solutions to the polynomial congruence $f(x) = x^{\frac{p-1}{d}} - 1 \equiv 0 \pmod{p}$. Since this polynomial has *exactly* $\frac{p-1}{d}$ incongruent solutions by Corollary 2.41, we know we have them all.

Now we may use Theorem 2.40, which states that the coefficients of

$$R(x) = f(x) - (x - r^{m-1})(x - r^{2(m-1)}) \cdots (x - r^{(\frac{p-1}{d})(m-1)})$$

are all congruent to 0 modulo p.

Since $\sum_{j=1}^{\frac{p-1}{d}} r^{j(m-1)}$ is the coefficient of the $x^{\frac{p-1}{d}-1}$ term in $R(x)$, it follows from Theorem 2.40 that

$$\sum_{j=1}^{\frac{p-1}{d}} r^{j(m-1)} \equiv 0 \pmod{p}.$$

Thus, we have

$$\sum_{i=1}^{m} i^{m-1} \equiv d\Big(\frac{m}{p}\Big) \sum_{j=1}^{\frac{p-1}{d}} r^{j(m-1)} \equiv 0 \pmod{p}.$$

This is a contradiction since $0 \not\equiv -1 \pmod{p}$, and we said $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{p}$. Thus $d \not< p - 1$, meaning $d = p - 1$. Since $d = \gcd(p - 1, m - 1)$, this means $(p - 1) \mid (m - 1)$, and hence $m \equiv 1 \pmod{p - 1}$. □

Lemma 3.8. *Let $m \geq 3$ be an integer. If $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then $m \equiv p \pmod{p^2}$ for each prime divisor p of m.*

Proof. By Theorems 3.1 and 3.2, we know that m must be a product of distinct odd primes. Recall, $\sum_{i=1}^{m} i^{m-1} \equiv \frac{m}{p} \sum_{i=1}^{p} i^{m-1} \equiv \frac{m}{p} \sum_{i=1}^{p-1} i^{m-1} \pmod{p}$. Now by Lemma 3.7, $(p - 1) \mid (m - 1)$, so we may write $m - 1 = (p - 1)q$ for some $q \in \mathbb{Z}^+$. It follows that

$$\frac{m}{p} \sum_{i=1}^{p-1} i^{m-1} = \frac{m}{p} \sum_{i=1}^{p-1} i^{(p-1)q} = \frac{m}{p} \sum_{i=1}^{p-1} (i^{p-1})^q.$$

Now by Fermat's Little Theorem, $i^{p-1} \equiv 1 \pmod{p}$ for $i = 1, 2, \ldots, p - 1$. So,

$$\frac{m}{p} \sum_{i=1}^{p-1} (i^{p-1})^q \equiv \frac{m}{p} \sum_{i=1}^{p-1} 1^q = \frac{m}{p} \sum_{i=1}^{p-1} 1 = \frac{m}{p}(p - 1) \equiv -\frac{m}{p} \pmod{p}.$$

That is, $\sum_{i=1}^{m} i^{m-1} \equiv -m/p \pmod{p}$.

Now, $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$ implies $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{p}$, so we must have $m/p \equiv 1 \pmod{p}$. This implies $m/p = pk+1$, for some $k \in \mathbb{Z}^+$. Multiplying through by p gives $m = p^2k + p$, which means $m \equiv p \pmod{p^2}$. □

By Lemma 3.7 $m \equiv 1 \pmod{p-1}$, and since $1 \equiv p \pmod{p-1}$, we have $m \equiv p \pmod{p-1}$. By Lemma 3.8 $m \equiv p \pmod{p^2}$, so by Corollary 2.28 we conclude that $m \equiv p \pmod{p^2(p-1)}$, and our proof of Theorem 3.3 is complete.

3.5 *Proof of Theorem* 3.4

Our proof of Theorem 3.4 will complete the remaining direction of Theorem 1.1. We need to prove that if $m \geq 3$ is an integer such that m is a product of distinct odd primes with $m \equiv p \pmod{p^2(p-1)}$ for each prime divisor p of m, then $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$.

Proof. Recall, $\sum_{i=1}^{m} i^{m-1} \equiv \frac{m}{p} \sum_{i=1}^{p} i^{m-1} \equiv \frac{m}{p} \sum_{i=1}^{p-1} i^{m-1} \pmod{p}$. Now since $m \equiv p \pmod{p^2(p-1)}$ by hypothesis, $m = p^2(p-1)X + p$ for some nonnegative integer X. Thus,

$$\begin{aligned}
\frac{m}{p} \sum_{i=1}^{p-1} i^{m-1} &= \frac{p^2(p-1)X + p}{p} \sum_{i=1}^{p-1} i^{p^2(p-1)X+p-1} \\
&= (p(p-1)X + 1) \sum_{i=1}^{p-1} i^{(p-1)p^2X+(p-1)} \\
&\equiv \sum_{i=1}^{p-1} i^{(p-1)p^2X+(p-1)} \pmod{p} \\
&= \sum_{i=1}^{p-1} i^{(p-1)(p^2X+1)} \\
&= \sum_{i=1}^{p-1} (i^{p-1})^{p^2X+1}.
\end{aligned}$$

Now by Fermat's Little Theorem, we have

$$\begin{aligned}
\sum_{i=1}^{p-1} (i^{p-1})^{p^2X+1} &\equiv \sum_{i=1}^{p-1} 1^{p^2X+1} \pmod{p} \\
&= \sum_{i=1}^{p-1} 1 \\
&= p - 1 \\
&\equiv -1 \pmod{p}.
\end{aligned}$$

Since this holds for all prime divisors p of m, and m is a product of distinct primes by hypothesis, Corollary 2.28 implies that

$$\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}.$$

□

Our proof of Theorem 1.1 is now complete.

3.6 Proof of Theorem 1.2

We are now ready to prove some consequences of Theorem 1.1. We begin with Theorem 1.2. We want to show that that if $m \geq 3$ is an integer such that $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then any two prime divisors of m, say p_1 and p_2, must satisfy $p_2 \not\equiv 1 \pmod{p_1}$.

Proof. This is trivial when $p_1 = p_2$, so assume that m is composite and $p_1 \neq p_2$. Clearly $p_2 \not\equiv 1 \pmod{p_1}$ if $p_2 < p_1$, so assume $p_1 < p_2$.

By Theorem 1.1, m is a product of distinct odd primes and $m = p_1^2(p_1-1)X_{p_1} + p_1 = p_2^2(p_2-1)X_{p_2} + p_2$ for some positive integers X_{p_1} and X_{p_2}.

This implies that $p_1^2(p_1-1)X_{p_1} - p_2^2(p_2-1)X_{p_2} = p_2 - p_1$. Now by Theorem 2.14, integers X_{p_1} and X_{p_2} exist if and only if

$$\gcd(p_1^2(p_1-1), p_2^2(p_2-1)) \mid (p_2 - p_1).$$

Since $\gcd(p_1, p_2) = 1$, Theorem 2.13 implies $\gcd(p_1^2(p_1-1), p_2^2(p_2-1)) = \gcd(p_1^2(p_1-1), p_2-1)$. Hence, we must have

$$\gcd(p_1^2(p_1-1), p_2-1) \mid (p_2 - p_1).$$

Now assume for the purpose of contradiction that $p_2 \equiv 1 \pmod{p_1}$. Then, $p_1 \mid (p_2-1)$ by the definition of congruence. But then,

$$\begin{aligned} p_1 \mid (p_2-1) &\Rightarrow p_1 \mid \gcd(p_1^2(p_1-1), p_2-1) \\ &\Rightarrow p_1 \mid (p_2-p_1) \quad \text{(from above)} \\ &\Rightarrow p_1 \mid p_2, \end{aligned}$$

contradicting the fact that p_1 and p_2 are primes.

This contradiction shows that $p_2 \not\equiv 1 \pmod{p_1}$. □

3.7 Proof of Theorem 1.3

We will now prove Theorem 1.3, that if $m \geq 3$ is an integer with $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then m cannot be a product of two primes.

Proof. From Theorem 1.1, we know that m must be a product of distinct odd primes. Assume for the purpose of contradiction that m is a product of two such primes, say p_1 and p_2 with $p_1 < p_2$. By Theorem 1.1, m must be of the form $p_2^2(p_2 - 1)X + p_2$, where X is some positive integer (if $X = 0$ then $m = p_2$ and m would not be a product of *two* distinct primes). Since $m = p_1 p_2 = {p_2}^2(p_2 - 1)X + p_2$, dividing through by p_2 gives $p_1 = p_2(p_2 - 1)X + 1$. But since $X \geq 1$, we have $p_2(p_2 - 1)X + 1 > p_2$, which is to say $p_1 > p_2$. This is a contradiction because we assumed $p_1 < p_2$. Hence, m cannot be a product of two primes. □

3.8 Proof of Theorem 1.4

We can also show that if $m \geq 3$ is an integer with $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, then m cannot be a product of three primes. Here is our proof of Theorem 1.4.

Proof. From Theorem 1.1, we know that m must be a product of distinct odd primes. Assume for the purpose of contradiction that m is a product of three such primes, say p_1, p_2, and p_3 with $p_1 < p_2 < p_3$. By Theorem 1.1, we know that m must be of the form ${p_3}^2(p_3-1)X+p_3$, where X is some positive integer ($X \neq 0$ since m is a product of more than one prime). Since $m = p_1p_2p_3 = p_3^2(p_3-1)X + p_3$, dividing through by p_3 gives $p_1p_2 = p_3(p_3-1)X + 1$, and since $X \geq 1$, we have $p_1p_2 \geq p_3(p_3-1)+1$.

Yet, consider the product p_1p_2. Because p_1, p_2, and p_3 are all odd primes, we know that $p_1p_2 \leq (p_3-4)(p_3-2)$, but $(p_3-4)(p_3-2) < p_3(p_3-1)+1$, so $p_1p_2 < p_3(p_3-1)+1$. This is a contradiction because we said $p_1p_2 \geq p_3(p_3-1)+1$. Hence, m cannot be a product of three primes. □

4. COMPUTATIONS

While we have proven some strong conditions on m for $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$, we have not been able to verify the conjecture that m must be prime if $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$.

Nevertheless, using Maple and the theorems we proved in Chapter 3, we can demonstrate that there is no counterexample to the conjecture less than or equal to one trillion. Figures 4.1, 4.2, and 4.3 on pages 42, 43, and 44 contain the actual Maple code for the program we developed to show this.

We provide a summary of how the program works. The user inputs the largest integer to be verified (called N), and the program outputs any counterexamples to the conjecture less than or equal to N (if any), as well as the number of factorizations performed. We count the number of factorizations because factorization is a time-consuming step. The program is split into a top-down portion and a bottom-up portion (see Figure 4.4 on page 45) in order to minimize the total run time of the program.

The flowchart detailing the top-down part is listed as Figure 4.5 on page 46. We are searching for a hypothetical composite integer $m \leq N$ that satisfies $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$. Since m is composite, Theorem 1.1 implies that $m = p^2(p-1)X_p + p$ for all prime divisors p of m, where X_p is some positive integer. Let p_{max} be the largest prime divisor of m. In the flowcharts and the Maple code, we are calling p_{max} "BP," which stands for "biggest prime," because this notation is easier to enter into Maple. We claim that p_{max} cannot exceed $\lfloor \sqrt[3]{N} \rfloor + 1$.

To see this, we will show that $p_{max} < \sqrt[3]{N} + 1$, which gives $p_{max} \leq \lfloor \sqrt[3]{N} \rfloor + 1$. Assume for the purpose of contradiction that m has a largest prime divisor $p_{max} \geq \sqrt[3]{N} + 1$. Then,

$$
\begin{aligned}
& m = (p_{max})^2(p_{max}-1)X_{p_{max}} + p_{max} \quad \text{(by Theorem 1.1)} \\
\Rightarrow \quad & m \geq (p_{max})^2(p_{max}-1) + p_{max} \quad \text{(since } X_{p_{max}} \geq 1\text{)} \\
\Rightarrow \quad & m \geq (\sqrt[3]{N}+1)^2 \cdot (\sqrt[3]{N}+1-1) + \sqrt[3]{N} + 1 \quad \text{(by assumption)} \\
\Rightarrow \quad & m \geq [(\sqrt[3]{N})^2 + 2\sqrt[3]{N} + 1] \cdot \sqrt[3]{N} + \sqrt[3]{N} + 1 \\
\Rightarrow \quad & m \geq (\sqrt[3]{N})^3 + 2(\sqrt[3]{N})^2 + \sqrt[3]{N} + \sqrt[3]{N} + 1 \\
\Rightarrow \quad & m \geq (\sqrt[3]{N})^3 + 2(\sqrt[3]{N})^2 + 2\sqrt[3]{N} + 1 \\
\Rightarrow \quad & m \geq N + 2(\sqrt[3]{N})^2 + 2\sqrt[3]{N} + 1 \\
\Rightarrow \quad & m > N.
\end{aligned}
$$

This is a contradiction because we chose m such that m was less than or equal to N. Thus,

$$
\begin{aligned}
p_{max} \not\geq \sqrt[3]{N} + 1 \quad & \Rightarrow \quad p_{max} < \sqrt[3]{N} + 1 \\
& \Rightarrow \quad p_{max} \leq \lfloor \sqrt[3]{N} + 1 \rfloor \\
& \Rightarrow \quad p_{max} \leq \lfloor \sqrt[3]{N} \rfloor + 1.
\end{aligned}
$$

With our claim proved, we continue to discuss the top-down portion of the program. Theorem 1.1 and its consequences tell us that since m is composite, m must be a product of four or more distinct odd primes. So, our first goal is to set p_{max} to be as large as possible (given N), and then show that no m can exist whose largest prime divisor is p_{max}. Then, we will set p_{max} to be the largest prime less than p_{max}'s current value, and repeat the process. We will continue as long as $p_{max} > 75$. Once $p_{max} < 75$, we will exit the top-down portion and begin the bottom-up portion of the program. After much experimentation, we chose 75 as the cut-off integer in order to minimize the total run time of the program. If the cut-off number is too large or too small, either the first part or the second part of the program will take much longer to run. On a late-2006 notebook computer (2.16 GHz Intel Core 2 Duo processor with 2.00 GB of RAM) running Windows XP, the program takes 43 minutes to run when $N = 10^{12}$ (32 minutes for the top-down portion and 11 minutes for the bottom-up portion).

In the top-down portion, for each $m \leq N$, we have $m = (p_{max})^2(p_{max}-1)X_{p_{max}} + p_{max}$. In the flowcharts and Maple code, we simply write $X_{p_{max}}$ as "X". Now let $maxX_{p_{max}}$ represent the largest possible value that any $X_{p_{max}}$ can assume for a given m. In the flowcharts and Maple code, we call $maxX_{p_{max}}$ "$maxX$." It follows that

$$
maxX_{p_{max}} = \left\lfloor \frac{N - p_{max}}{(p_{max})^2(p_{max}-1)} \right\rfloor.
$$

Now, for each $X_{p_{max}}$ from 1 to $maxX_{p_{max}}$ we let $m = (p_{max})^2(p_{max}-1)X_{p_{max}} + p_{max}$, and then we factor m/p_{max} to check that m is a product of distinct odd primes (this is faster than just factoring m). If m is a product of distinct odd primes, then for each prime divisor p of m we check that $m = p^2(p-1)X_p + p$ for some positive integer X_p. In the Maple code, we simply call X_p "x". If X_p is a positive integer, we add m to our list of counterexamples. Once we have run through all $X_{p_{max}}$ for each $p_{max} > 75$, we exit the top-down portion of the program.

The purpose of the bottom-up portion of the program is to show that m cannot be a product of distinct odd primes less than 75. Its flowchart is listed as Figure 4.6 on page 47. For this part, we let $SP1$ stand for the smallest prime divisor of m. We start with $SP1 = 3$ since m must be odd. Let $SP2$ represent the second smallest prime divisor of m. By Theorem 1.2, $SP2 \not\equiv 1 \pmod{SP1}$. Now let $LIST$ be the set of all primes p with $SP2 < p < 75$ such that $p \not\equiv 1 \pmod{SP1}$ and $p \not\equiv 1 \pmod{SP2}$. Let $powerLIST$ be the powerset of $LIST$. Now for each set in $powerLIST$ with at least two elements, we let m equal the product of $SP1$, $SP2$, and the elements of the set. For each prime divisor p of m, we check that $m = p^2(p-1)X_p + p$ for some positive integer X_p. As before, if X_p is a positive integer, then we add m to our list of counterexamples.

Now we set $SP2$ to be the next largest prime such that $SP2 \not\equiv 1 \pmod{SP1}$, and we repeat the steps above. Then, we advance $SP2$ again, and again, until $SP2 > 67$ (we stop here because if $SP2 > 67$, then m would have to have a prime divisor larger than 75). Once this occurs, we advance $SP1$ to the next prime larger than $SP1$'s current value, reset $SP2$, and repeat the steps. Then, we advance $SP1$ again, and again, until $SP1 > 61$ (if $SP1 > 61$, then m would have to have a prime divisor larger than 75). Once this happens, we have finished the bottom-up portion of the program, and together with the top-down portion, we have exhausted our search for a composite integer $m \leq N$ satisfying $\sum_{i=1}^{m} i^{m-1} \equiv -1 \pmod{m}$. The program concludes by printing the number of factorizations performed and listing any counterexamples discovered.

We can show heuristically that the number of factorizations performed is approximately equal to $N \int_a^\infty 1/(x^3 \ln x)\, dx$, where a represents the cut-off integer separating the top-down and bottom-up parts of the program (e.g. $a = 75$ above). This shows that the number of factorizations performed increases linearly as N increases (when a is independent of N).

Note that there are $maxX_{p_{max}}$ factorizations for each value of p_{max}, and that p_{max} assumes a value for each prime between a and $\lfloor \sqrt[3]{N} \rfloor + 1$. Furthermore,

$$maxX_{p_{max}} = \left\lfloor \frac{N - p_{max}}{(p_{max})^2(p_{max}-1)} \right\rfloor \approx \left\lfloor \frac{N}{(p_{max})^3} \right\rfloor \approx \frac{N}{(p_{max})^3}.$$

So, if we let $M = \lfloor \sqrt[3]{N} \rfloor + 1$ and let F_N equal the total number of factorizations performed for a given N, then

$$F_N \approx \sum_{x=a}^{M} [\chi(x) \cdot (N/x^3)] = N \sum_{x=a}^{M} \frac{\chi(x)}{x^3},$$

where

$$\chi(x) = \begin{cases} 1, & \text{if } x \text{ is prime} \\ 0, & \text{otherwise.} \end{cases}$$

At this point, we turn to a common heuristic argument in order to continue approximating this sum. Recall, for a real number n, the function $\pi(n)$ denotes the number of primes not exceeding n, and by the prime number theorem, $\pi(n)$ is asymptotically equal to $n/\ln(n)$. Now consider a large positive integer x and a small real number ϵ. By the prime number theorem, we have the following three facts,

$$\begin{aligned} \pi(x) &= \frac{x}{\ln x}(1 + o(1)), \\ \pi((1-\epsilon)x) &= \frac{(1-\epsilon)x}{\ln((1-\epsilon)x)}(1 + o(1)) = \frac{(1-\epsilon)x}{\ln x + \ln(1-\epsilon)}(1 + o(1)), \\ \pi((1+\epsilon)x) &= \frac{(1+\epsilon)x}{\ln((1+\epsilon)x)}(1 + o(1)) = \frac{(1+\epsilon)x}{\ln x + \ln(1+\epsilon)}(1 + o(1)), \end{aligned}$$

where $o(g(x))$ means $\frac{o(g(x))}{g(x)} \to 0$ as $x \to \infty$. In particular, $o(1)$ denotes a function of x that goes to 0 as $x \to \infty$. Each appearance of $o(1)$ can represent a different function.

Now consider the interval $[(1-\epsilon)x, (1+\epsilon)x]$. The number of primes in this interval is given by $\pi(x+\epsilon) - \pi(x-\epsilon)$. From above, this is equal to

$$\frac{(1+\epsilon)x}{\ln x + \ln(1+\epsilon)}(1 + o(1)) - \frac{(1-\epsilon)x}{\ln x + \ln(1-\epsilon)}(1 + o(1)),$$

which is equal to

$$\frac{2\epsilon x}{\ln x}(1 + o(1)).$$

Since there are $2\epsilon x$ integers in the interval $[(1-\epsilon)x, (1+\epsilon)x]$, we may say that the probability that a randomly selected integer from this interval is prime is about

$$\frac{\frac{2\epsilon x}{\ln x}(1 + o(1))}{2\epsilon x} = \frac{1}{\ln x}(1 + o(1)).$$

In other words, given a large enough x and a relatively small enough interval around x, the probability that a randomly selected integer from that interval is prime is aymptotic to $1/\ln(x)$.

Using this heuristic, we have

$$F_N \approx N \sum_{x=a}^{M} \frac{\chi(x)}{x^3} \approx N \sum_{x=a}^{M} \frac{1/\ln x}{x^3} = N \sum_{x=a}^{M} \frac{1}{x^3 \ln x}.$$

We wish to approximate this sum by an integral so that we may study it more. Consider each term in the sum as an $N/(x^3 \ln x)$ by 1 rectangle. If we orient these rectangles vertically and center them on the integers on the x-axis of a coordinate plane, then $N \sum_{x=a}^{M} 1/(x^3 \ln x)$ is equal to the area occupied by all of these rectangles. Now for $a \leq x \leq M$, the function $f(x) = N/(x^3 \ln x)$ passes through the midpoint of the top of each rectangle, so the area under this curve is about equal to the area the rectangles occupy.

Hence,

$$\begin{aligned}
& F_N \approx N \sum_{x=a}^{M} \frac{1}{x^3 \ln x} \\
\Rightarrow \quad & F_N \approx N \int_a^M \frac{1}{x^3 \ln x}\, dx \\
\Rightarrow \quad & \frac{F_N}{N} \approx \int_a^M \frac{1}{x^3 \ln x}\, dx \\
\Rightarrow \quad & \frac{F_N}{N} \approx \int_a^\infty \frac{1}{x^3 \ln x}\, dx - \int_M^\infty \frac{1}{x^3 \ln x}\, dx.
\end{aligned}$$

However,

$$0 \leq \int_M^\infty \frac{1}{x^3 \ln x}\, dx \leq \int_M^\infty \frac{1}{x^3}\, dx = \frac{1}{2M^2},$$

and $1/(2M^2) \to 0$ as $M \to \infty$.

Now since $M = \lfloor \sqrt[3]{N} \rfloor + 1 \approx \sqrt[3]{N}$, we may say that $1/(2M^2) \to 0$ as $N \to \infty$. Thus, as $N \to \infty$,

$$\frac{F_N}{N} \approx \int_a^\infty \frac{1}{x^3 \ln x}\, dx.$$

Now let us evaluate $\int_a^\infty 1/(x^3 \ln x)\,dx$ using substituation of variables. Let $t = 2\ln x$. Then, $\ln x = t/2$ and $x^2 = \mathrm{e}^t$. Also, $dx = (x\,dt)/2$. Thus,

$$\begin{aligned}
\int_a^\infty \frac{1}{x^3 \ln x}\,dx &= \int_a^\infty \frac{1}{x \cdot x^2 \cdot \ln x}\,dx \\
&= \int_{2\ln a}^\infty \frac{1}{x \cdot \mathrm{e}^t \cdot (t/2)}\left(\frac{x\,dt}{2}\right) \\
&= \int_{2\ln a}^\infty \frac{1}{\mathrm{e}^t \cdot t}\,dt \\
&= \int_{2\ln a}^\infty \frac{\mathrm{e}^{-t}}{t}\,dt \\
&= E_1(2\ln a),
\end{aligned}$$

where $E_1(2\ln a)$ is the *exponential integral* $E_1(x)$ evaluated at $2\ln a$ (for more information on this function, see <http://mathworld.wolfram.com/En-Function.html> [10], <http://mathworld.wolfram.com/ExponentialIntegral.html> [11], and/or page 2 of Bleistein and Handlesman's *Asymptotic Expansions of Integrals* [2]).

Thus,

$$\frac{F_N}{N} \approx \int_a^\infty \frac{1}{x^3 \ln x}\,dx = E_1(2\ln a),$$

which implies

$$F_N \approx N \cdot E_1(2\ln a).$$

With $N = 10^{12}$ and $a = 75$, Maple gives $10^{12} \cdot E_1(2\ln(75)) \approx 18,621,914$. Note that the actual number of factorizations performed with $N = 10^{12}$ and $a = 75$ was $16,580,031$.

```
BEGIN Intro
> restart :
  with(combinat, powerset) :
  N := 1000000000000;
  counterexamples := NULL;
  LIST := NULL;
  fcount := 0 :
```

$$N := 1000000000000 \tag{1}$$

```
> Check1 := proc(L1)
  local i;
  global flag1;
  flag1 := true;
  i := 1;
  while flag1 and i ≤ nops(L1) do
    if nops(op(i, L1)) ≠ 1 then flag1 := false; end if;
  i := i + 1;
  end do;
  if flag1 = true and op(op(nops(L1), L1)) = LP then
  flag1 := false;
  end if;
  end:
> Check2 := proc(L2)
  local p, x, i;
  global flag2;
  flag2 := true :
  i := 1 :
  while flag2 and i ≤ nops(L2) do
  p := op(op(i, L2)) :
  x := (m - p)/(p^2 · (p - 1)) :
  flag2 := type(x, integer) :
  i := i + 1 :
  end do:
  end:
> Check3 := proc(L3)
  local p, x, i;
  global flag3;
  flag3 := true :
  i := 1 :
  while flag3 and i ≤ nops(L3) do
  p := op(i, L3) :
  x := (m - p)/(p^2 · (p - 1)) :
  flag3 := type(x, integer) :
  i := i + 1 :
  end do:
  end:
END Intro
```

Fig. 4.1: Maple Code (Part 1)

```
BEGIN Top-Down
> if isprime(floor(N^(1/3)) + 1) then BP := floor(N^(1/3)) + 1 :
  else BP := prevprime(floor(N^(1/3)) + 1) :
  end if:
  while BP ≥ 75 do
    maxX := floor((N - BP)/(BP^2 · (BP - 1)));
    for X from 1 to maxX do
      m := BP · (BP · (BP - 1)X + 1);
      f := ifactor(m/BP);
      fcount := fcount + 1 :
      if nops(f) ≥ 3 then
        Check1(f);
        if flag1 then
          Check2(f);
          if flag2 then counterexamples := counterexamples, m; end if:
        end if;
      end if;
    end do;
  BP := prevprime(BP) :
  end do:
END Top-Down
```

Fig. 4.2: Maple Code (Part 2)

```
BEGIN Bottom-Up
> SP1 := 3 :
  while SP1 ≤ 61 do
    SP2 := nextprime(SP1);
    while SP2 modp SP1 = 1 do
      SP2 := nextprime(SP2) :
    end do:
    while SP2 ≤ 67 do
      k := nextprime(SP2) :
      while k ≤ 73 do
        if k modp SP1 ≠ 1 and k modp SP2 ≠ 1 then
          LIST := LIST, k :
        end if:
        k := nextprime(k) :
      end do:
      powerLIST := powerset({LIST}) :
      for J in powerLIST do
        if (nops(J) ≥ 2) then
          m := SP1·SP2 :
          for j in J do
            m := m·j :
          end do:
          w := SP1, SP2, op(J) :
          Check3([w]) :
          if flag3 then
            counterexamples := counterexamples, m :
          end if:
        end if:
      end do:
      SP2 := nextprime(SP2) :
    end do:
    SP1 := nextprime(SP1) :
  end do:
END Bottom-Up

BEGIN Outro
> counterexamples;
  writeline(default, "Number of counterexamples found:" ) :
  nops([counterexamples]);
  writeline(default, "Number of factorizations performed:" ) :
  fcount;
Number of counterexamples found:
                              0

Number of factorizations performed:
                          16580031                          (2)
END Outro
```

Fig. 4.3: Maple Code (Part 3)

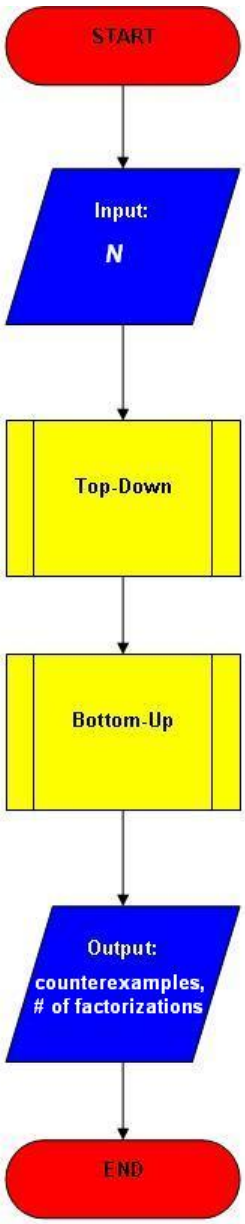

Fig. 4.4: Overview Flowchart

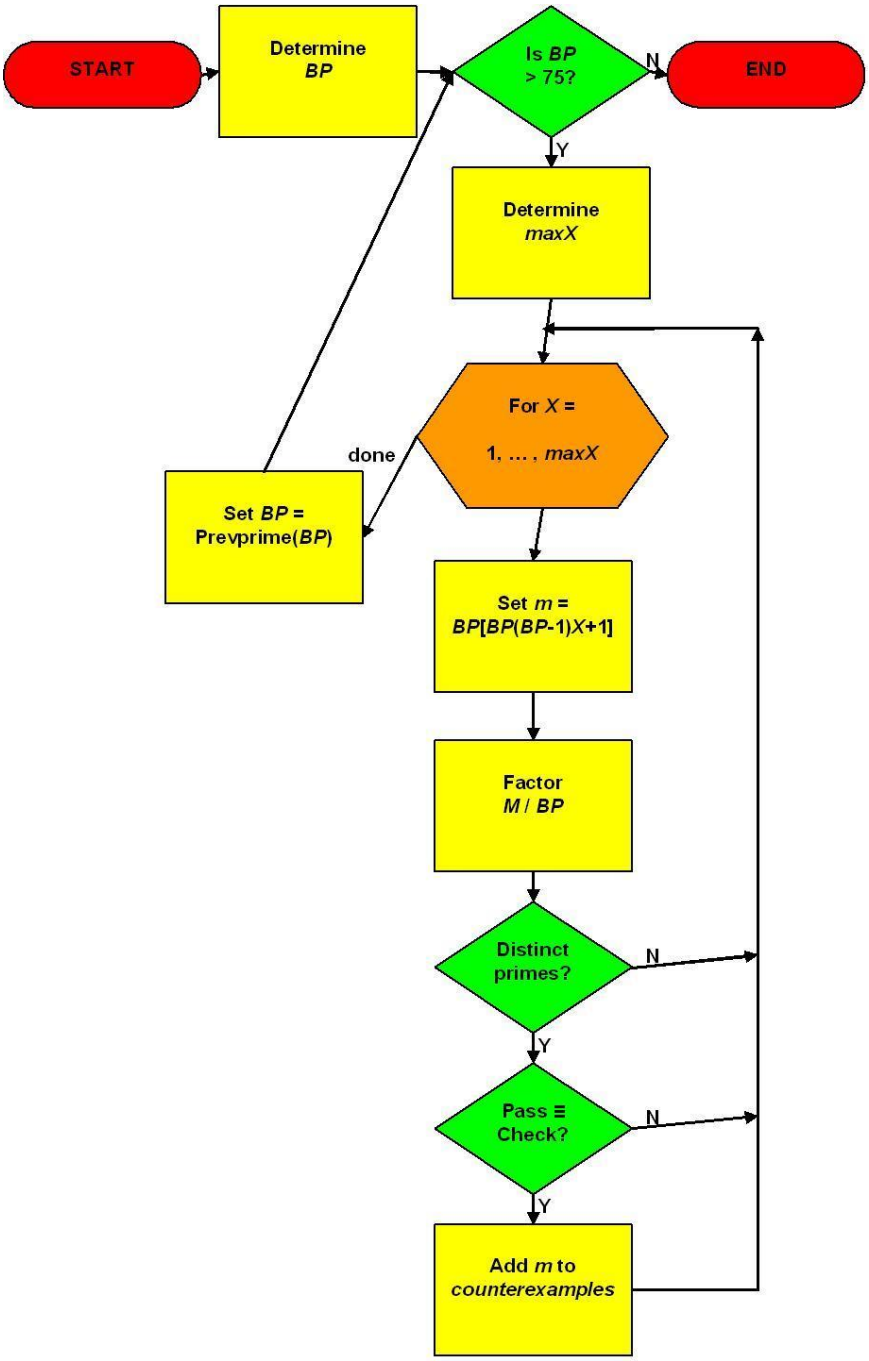

Fig. 4.5: Top-Down Flowchart

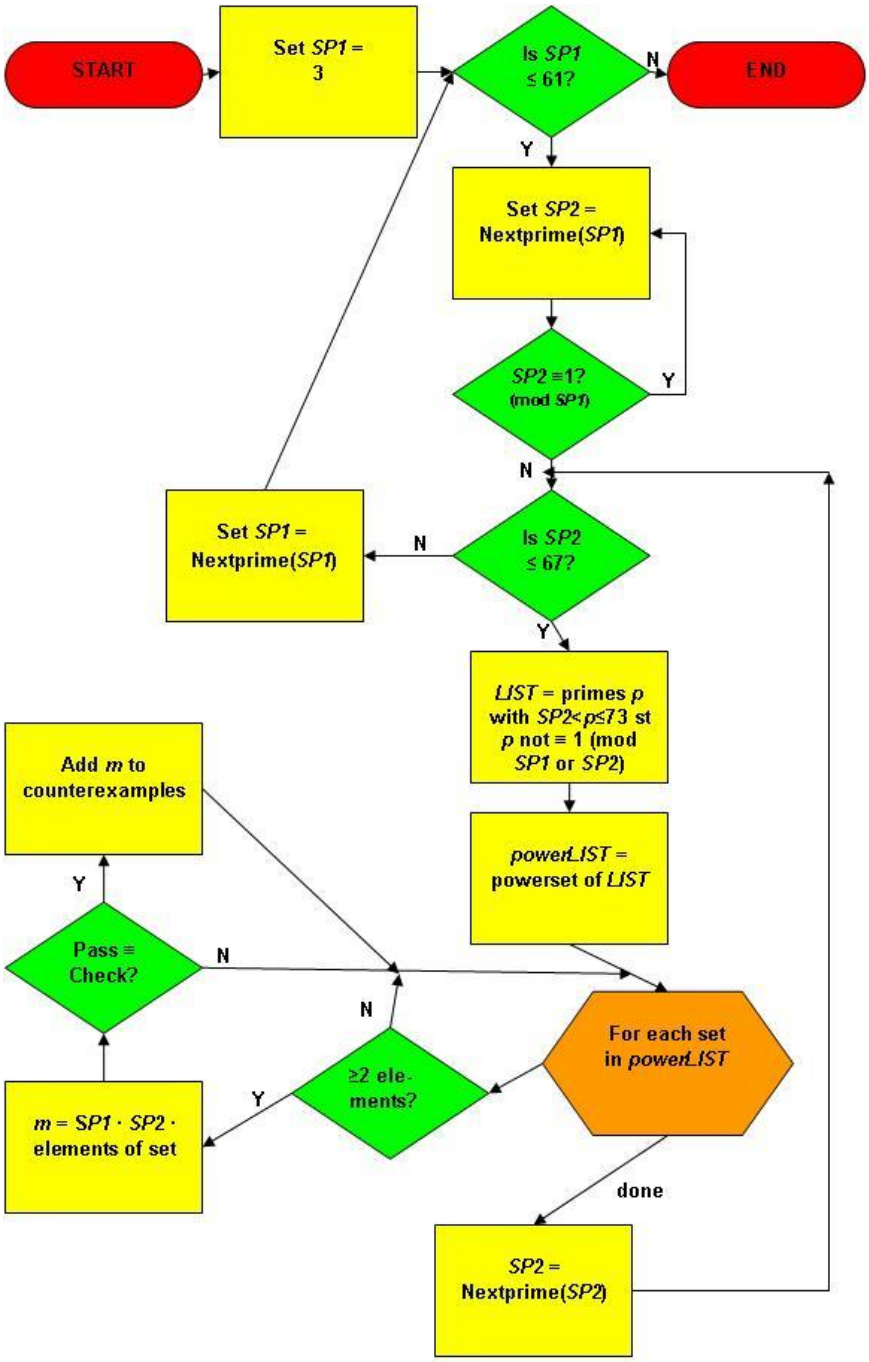

Fig. 4.6: Bottom-Up Flowchart

BIBLIOGRAPHY

[1] Aigner, Martin. (2007). *Discrete Mathematics.* American Mathematical Society.

[2] Bleistein, N. and Handlesman, R. (1975). *Asymptotic Expansions of Integrals.* Dover.

[3] Graham, Knuth, and Patashnik. (1994). *Concrete Mathematics: A Foundation for Computer Science (2nd Edition).* Addison Wesley.

[4] Jones, Gareth A. (1998). *Elementary Number Theory.* Springer.

[5] Koshy, Thomas. (2007). *Elementary Number Theory with Applications, Second Edition.* Academic Press.

[6] Long, Calvin T. (1995). *Elementary Introduction to Number Theory.* Waveland Press.

[7] *Odd Perfect Number Search.* (2008). <http://oddperfect.org/index.html> .

[8] Rosen, Kenneth H. (2005). *Elementary Number Theory and Its Applications (5th Edition).* Addison Wesley.

[9] Weisstein, Eric W. (2008). "Bernoulli Number." *MathWorld–A Wolfram Web Resource.* <http://mathworld.wolfram.com/BernoulliNumber.html>.

[10] Weisstein, Eric W. (2008). "En-Function." *MathWorld–A Wolfram Web Resource.* <http://mathworld.wolfram.com/En-Function.html>.

[11] Weisstein, Eric W. (2008). "Exponential Integral." *MathWorld–A Wolfram Web Resource.* <http://mathworld.wolfram.com/ExponentialIntegral.html>.