Fermat's Little Theorem & Euler's Theorem Proofs

Karim El Shenawy

February 2021

Introduction

This course notebook is the collection of theorem proofs, exercises and answers from Unit 4 of the Number Theory Through Inquiry (Mathematical Association of America Textbooks).

Theorems to Mark

4.3 Theorem

Let a, b and n be natural numbers with $(a, n) = 1$. If $a \equiv b \pmod{n}$, then $(b, n) = 1$.

Proof. Given a, b and n as natural numbers with $(a, n) = 1$. Then by Theorem 1.39, $(a, n) = 1 \implies 1 = ax + ny, \exists x, y \in \mathbf{Z}$. Let's assume that $a \equiv b \pmod{n}$ which also implies that n divides $a - b$ since $a \equiv b \pmod{n} \implies a - b \equiv 0 \pmod{n} \implies n \mid a - b$. By definition, $n \mid a - b$ is also $a - b = nd, \exists d \in \mathbf{Z}$.

Now by direct proof and considering that $1 = ax + ny$ and $a = nd + b$;

$1 = ax + ny$	
$1 = (nd + b)x + ny$	By substituting $a = nd + b$
$1 = ndx + bx + ny$	
$1 = n(dx + y) + bx$	
$1 = nz + bx$	Since $d, x, y \in \mathbf{Z}$, assume that some integer $z = dx + y$
$1 = gcd(b, n)$	By Theorem 1.39

Thus If $(a, n) = 1$ and $a \equiv b \pmod{n}$, then $(b, n) = 1$. □

4.10 Theorem

Let a and n be natural numbers with $(a, n) = 1$, let $k = ord_n(a)$, and let m be a natural number. Then $a^m \equiv 1 \pmod{n}$ if and only if $k \mid m$.

Proof. Let a, n and m $\in \mathbf{N}$ be natural numbers with $(a, n) = 1$, let $k = ord_n(a)$. Suppose $a^m \equiv 1 \pmod{n}$, by the Division Algorithm, we can express $m = qk + r, 0 \leq r < k$. Then,

$$\begin{aligned} a^m &\equiv a^{qk+r} \pmod{n} \\ a^m &\equiv a^{qk} \cdot a^r \pmod{n} \\ a^m &\equiv 1^q \cdot a^r \pmod{n} \\ a^m &\equiv a^r \pmod{n} \\ a^m &\equiv 1 \pmod{n} \qquad\qquad \text{Since } a^m \equiv 1 \pmod{n} \end{aligned}$$

The above implies that r must be 0, which also implies that $m = kq$. Thus, $k \mid m$. Conversely, lets suppose that $k \mid m$, then,

$$\begin{aligned} a^m &\equiv a^{qk} \pmod{n} \\ a^m &\equiv 1^q \pmod{n} \\ a^m &\equiv 1 \pmod{n} \end{aligned}$$

Thus, $a^m \equiv 1 \pmod{n}$ if and only if $k \mid m$. □

4.15 Theorem (Fermat's Little Theorem, Version I)

If p is a prime and a is an integer relatively prime to p, then $a^{(p-1)} \equiv 1 \pmod{p}$.

Proof. Given a prime p, let the set $\{1, 2, 3, ..., p-1\}$ be all the number modulo p, by Theorem 4.14. We can claim that some integer a is in $\{1, 2, 3, ..., p-1\}$ since $(p, a) = 1$.
If we multiply the numbers in the set $\{1, 2, 3, ..., p-1\}$ by a, we obtain $\{a, 2a, 3a, ..., (p-1)a\}$ and we know by Theorem 4.14 that;

$$\begin{aligned} a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a &\equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p} \\ a^{p-1} \cdot (p-1)! &\equiv (p-1)! \pmod{p} \\ a^{p-1} &\equiv 1 \pmod{p} \qquad\qquad (p-1)! \pmod{p} \equiv 1 \end{aligned}$$

Since we know that all values in $\{1, 2, 3, ..., p-1\}$ are all modulo p, thus $(p-1)! \pmod{p} \equiv 1$. Hence, $a^{(p-1)} \equiv 1 \pmod{p}$.holds. □

4.25 Lemma

If p is prime and i is a natural number less than p, then p divides $\binom{p}{i}$.

Proof. Given p prime and i, a natural number and less than p, we can expand

$\binom{p}{i}$;

$$\begin{aligned}
\binom{p}{i} &= \frac{p!}{i!(p-i)!} \\
\binom{p}{i} &= \frac{p(p-1)(p-2)\cdots(p-(i-1))(p-i)!}{i!(p-i)!} \\
\binom{p}{i} &= \frac{p(p-1)(p-2)\cdots(p-(i-1))}{i!} \\
\binom{p}{i} \cdot i! &= p(p-1)(p-2)\cdots(p-(i-1))
\end{aligned}$$

Now, p divides p thus we can express it as the following;

$$\begin{aligned}
p \mid p \implies p \mid p(p-1)(p-2)\cdots(p-(i-1)) \implies p \mid \tbinom{p}{i} \cdot i! \\
\implies p \mid \tbinom{p}{i} \cdot i(i-1)(i-2)\cdots 3 \cdot 2 \cdot 1
\end{aligned}$$

Since i is less than p, p can not divide $i!$. Thus we end up with $p \mid \binom{p}{i}$. Therefore, p must divide $\binom{p}{i}$. □

4.38 Theorem

Let p be a prime and let a and b be integers such that $1 < a, b < p-1$ and $ab \equiv 1 \pmod{p}$. Then $a \neq b$.

Proof. Let p be a prime and let a and b be integers such that $1 < a, b < p-1$ and $ab \equiv 1 \pmod{p}$. Now lets assume, by contradiction, that $a = b$. Then, $ab \equiv a^2 \equiv 1 \pmod{p}$. Also, by definition, $a^2 \equiv 1 \pmod{p} \implies p \mid a^2 - 1$ where $a^2 - 1 = (a+1)(a-1)$. Since p is a prime, can divide $a-1$ or $a+1$.
However, since we know that $1 < a < p-1$, which can also be expressed as $1 < a+1 < p$, this implies that p can not divide a. Similarly, since $a < p-1$, p can not divide $a+1$ either. This signifies that $p \nmid a^2 = ab, a = b$. Thus $a \neq b$. □

4.41 Theorem (Wilson's Theorem)

If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. By Theorem, 4.40, suppose p is a prime larger than 2, then $2 \cdot 3 \cdot 4 \cdots \cdot (p-2) \equiv 1 \pmod{p}$. Now, let's multiply (p-1) in both sides;

$$\begin{aligned}
2 \cdot 3 \cdot 4 \cdots \cdot (p-2) &\equiv 1 \pmod{p} \\
2 \cdot 3 \cdot 4 \cdots \cdot (p-2) \cdot (p-1) &\equiv (p-1) \pmod{p} \\
2 \cdot 3 \cdot 4 \cdots \cdot (p-2) \cdot (p-1) &\equiv -1 \pmod{p} \\
(p-1)! &\equiv -1 \pmod{p}
\end{aligned}$$

Thus, if p is a prime, then $(p-1)! \equiv -1 \pmod{p}$. □

Practice Theorems from A Modular World

4.1 Exercise

For $i = 0, 1, 2, 3, 4, 5$ and 6, find the number in the canonical complete residue system to which 2^i is congruent modulo 7. In other words, compute $2^0 \pmod 7, 2^1 \pmod 7, 2^2 \pmod 7, ..., 2^6 \pmod 7$.

- $2^0 \equiv 0 \pmod 7$
- $2^1 \equiv 2 \pmod 7$
- $2^2 \equiv 4 \pmod 7$
- $2^3 \equiv 8 \pmod 7$
- $2^4 \equiv 16 \equiv 5 \pmod 7$
- $2^5 \equiv 32 \equiv 4 \pmod 7$
- $2^6 \equiv 64 \equiv 1 \pmod 7$

4.2 Theorem

Let a and n be natural numbers with $(a, n) = 1$. Then $(a^j, n) = 1$ for any natural number j.

Proof. Given that natural numbers a and n have gcd(a, n) = 1 implies that a and n are relatively prime. Therefore, a^j must also have no primes factors in common with n. □

4.3 Theorem

Let a, b and n be natural numbers with $(a, n) = 1$. If $a \equiv b \pmod n$, then $(b, n) = 1$.

Proof. Given a, b and n as natural numbers with $(a, n) = 1$. Then by Theorem 1.39,$(a, n) = 1 \implies 1 = ax + ny, \exists x, y \in \mathbf{Z}$. Let's assume that $a \equiv b \pmod n$ which also implies that n divides $a - b$ since $a \equiv b \pmod n \implies a - b \equiv 0 \pmod n \implies n \mid a - b$. By definition, $n \mid a - b$ is also $a - b = nd, \exists d \in \mathbf{Z}$.

Now by direct proof and considering that $1 = ax + ny$ and $a = nd + b$;

$1 = ax + ny$	
$1 = (nd + b)x + ny$	By substituting $a = nd + b$
$1 = ndx + bx + ny$	
$1 = n(dx + y) + bx$	
$1 = nz + bx$	Since $d, x, y \in \mathbf{Z}$, assume that some integer $z = dx + y$
$1 = gcd(b, n)$	By Theorem 1.39

Thus If $(a, n) = 1$ and $a \equiv b \pmod n$, then $(b, n) = 1$. □

4.4 Theorem

Let a and n be natural numbers. Then there exist natural numbers i and j, with $i \neq j$, such that $a^i \equiv a^j \pmod{n}$.

Proof. Suppose natural number a, n, m, i and j exist such that $a^m \equiv 1 \pmod{n}$ and $i \neq j$. Now by direct proof;

$$\begin{aligned} a^m &\equiv 1 \pmod{n} && \\ a^m(a^{10}) &\equiv a^{10} \pmod{n} && \text{By multiplying } a^{10} \text{ on both sides} \\ a^{m-10} &\equiv a^{10} \pmod{n} && \text{Exponent Properties} \end{aligned}$$

Therefore there must exist an i and j with $i \neq j$ such that $a^i \equiv a^j \pmod{n}$ since $m - 10 \neq 10$. □

4.5 Theorem

Let a, b, c and n be integers with $n > 0$. If $ac \equiv bc \pmod{n}$ and $(c, n) = 1$, then $a \equiv b \pmod{n}$.

Proof. Given integers a, b, c and n with $n > 0$. Then $ac \equiv bc \pmod{n} \implies n \mid c(a - b)$ by definition. However, assuming that c and n are relatively prime by $(c, n) = 1$, n only divides $a - b$, $n \mid a - b$. Therefore, by definition, $n \mid a - b \implies a - b \equiv 0 \pmod{n} \implies a \equiv b \pmod{n}$. □

4.6 Theorem

Let a and n be natural numbers with $(a, n) = 1$. Then there exists a natural number k such that $a^k \equiv 1 \pmod{n}$.

Proof. Given natural numbers a and n with $(a, n) = 1$. Then by Theorem 4.2, $(a^k, n) = 1, \exists k \in \mathbf{N}$. Also by Theorem 4.4, $a^i \equiv a^j \pmod{n}, \exists i, j \in \mathbf{N}$ with $i \neq j$. Let $k = i - j$, thus $a^i - a^j \equiv a^k \equiv 0 \pmod{n}$. However, since $(a^k, n) = 1$, $a^k \not\equiv 0 \pmod{n}$ and it can only be $a^k \equiv 1 \pmod{n}$. □

4.7 Question

Choose some relatively prime natural numbers a and n and compute the order of a modulo n. Frame a conjecture concerning how large the order of a modulo n can be, depending on n.

- $(a, n) = (5, 12) = 1$
  $5^2 \equiv 1 \pmod{15}$, order $= 2$
- $(a, n) = (2, 3) = 1$
  $2^2 \equiv 1 \pmod{3}$, order $= 2$
- $(a, n) = (7, 10) = 1$
  $7^4 \equiv 1 \pmod{10}$, order $= 4$

Conjecture. *The order of a modulo n will always be under n.*

4.8 Theorem

Let a and n be natural numbers with $(a, n) = 1$ *and let* $k = ord_n(a)$*. Then the numbers* $a^1, a^2, ..., a^k$ *are pairwise incongruent modulo n.*

Proof. Given natural numbers a and n with $(a, n) = 1$ and let $k = ord_n(a)$, lets suppose that there exists integers i and j such that $a^i \equiv a^j \pmod{n}$ and that $1 \leq j < i < k$. By Theorem 4.2, we know that $a^i \equiv a^j \pmod{n} \implies a^{i-j} \equiv 1 \pmod{n}$ with $i - j < k$ since $(a, n) = 1$. However, k is considered to be the smallest natural number where $a^k \equiv 1 \pmod{n}$ by $k = ord_n(a)$. Thus, if $(a, n) = 1$ and $k = ord_n(a)$, then the numbers $a^1, a^2, ..., a^k$ are pairwise incongruent modulo n, i.e. values $\pmod{n}$ never repeat. □

4.9 Theorem

Let a and n be natural numbers with $(a, n) = 1$ *and let* $k = ord_n(a)$*. For any natural number m,* a^m *is congruent modulo n to one of the numbers* $a^1, a^2, ..., a^k$*.*

Proof. Given the natural numbers a and n with $(a, n) = 1$ and let $k = ord_n(a)$, we know that $a^k \equiv 1 \pmod{n}$. Suppose m exists and is any natural number with $1 < k < m$. By the Division Algorithm, we can express $m = qk + r, 0 \leq r < k$. Now, $a^m \equiv a^{qk+r} \equiv a^{kq} \cdot a^r \equiv 1^q \cdot a^r \pmod{n}$. Thus a^m is congruent modulo n to one of the numbers $a^1, a^2, ..., a^k$. □

4.10 Theorem

Let a and n be natural numbers with $(a, n) = 1$*, let* $k = ord_n(a)$*, and let m be a natural number. Then* $a^m \equiv 1 \pmod{n}$ *if and only if* $k \mid m$*.*

Proof. Let a, n and m $\in \mathbf{N}$ be natural numbers with $(a, n) = 1$, let $k = ord_n(a)$. Suppose $a^m \equiv 1 \pmod{n}$, by the Division Algorithm, we can express $m = qk + r, 0 \leq r < k$. Then,

$$\begin{aligned}
a^m &\equiv a^{qk+r} \pmod{n} \\
a^m &\equiv a^{qk} \cdot a^r \pmod{n} \\
a^m &\equiv 1^q \cdot a^r \pmod{n} \\
a^m &\equiv a^r \pmod{n} \\
a^m &\equiv 1 \pmod{n} \qquad \text{Since } a^m \equiv 1 \pmod{n}
\end{aligned}$$

The above implies that r must be 0, which also implies that $m = kq$. Thus, $k \mid m$. Conversely, lets suppose that $k \mid m$, then,

$$\begin{aligned}
a^m &\equiv a^{qk} \pmod{n} \\
a^m &\equiv 1^q \pmod{n} \\
a^m &\equiv 1 \pmod{n}
\end{aligned}$$

Thus, $a^m \equiv 1 \pmod{n}$ if and only if $k \mid m$. □

4.11 Theorem

Let a and n be natural numbers with $(a, n) = 1$. *Then* $ord_n(a) < n$.

Proof. Let a and n $\in \mathbf{N}$ with $(a, n) = 1$ and suppose that that $ord_n(a) \mid k$. Then $k = ord_n(a) \cdot d, \exists d \in \mathbf{Z}$. Now,

$$\begin{aligned} a^k &\equiv a^{ord_n(a)\cdot d} \pmod{n} \\ a^k &\equiv 1^d \pmod{n} && \text{By Definition} \\ a^k &\equiv 1 \pmod{n} \end{aligned}$$

Conversely, if $a^k \equiv 1 \pmod{n}$, we can show that $ord_n(a) \mid k$ by the Division Algorithm with $k = ord_n(a) \cdot d + r, \exists d, r \in \mathbf{Z}$ where $0 \leq r < ord_n(a)$. Then,

$$\begin{aligned} a^k &\equiv a^{ord_n(a)\cdot d + r} \pmod{n} \\ a^k &\equiv a^{ord_n(a)\cdot d} \cdot a^r \pmod{n} \\ a^k &\equiv 1^d \cdot a^r \pmod{n} && \text{By Definition} \\ a^k &\equiv a^r \pmod{n} \end{aligned}$$

Since we know that $0 \leq r < ord_n(a)$ and $a^k \equiv 1 \pmod{n}$, r must be 0. Thus, $ord_n(a) \mid k$.

Now, if $ord_n(a) \mid k$ then $ord_n(a) \leq k$ where k is the smallest natural number $k < n$. Thus, $ord_n(a) \leq k < n$ and $ord_n(a) < n$. □

4.12 Exercise

Compute $a^{p-1} \pmod{p}$ *for various numbers a and primes p, and make a conjecture.*

- $3^{2-1} \equiv 3 \pmod{2}$
- $4^{2-1} \equiv 4 \pmod{2}$
- $4^{3-1} \equiv 4^2 \pmod{2}$
- $4^{5-1} \equiv 4^4 \pmod{2}$
- $4^{7-1} \equiv 4^6 \pmod{2}$
- $4^{11-1} \equiv 4^{10} \pmod{2}$

Conjecture. *If a is a prime different from p, then* $a^{p-1} \equiv 1 \pmod{p}$.

4.13 Theorem

Let p be a prime and let a be an integer not divisible by p; that is, $(a, p) = 1$. *Then* $\{a, 2a, 3a, ..., pa\}$ *is a complete residue system modulo p.*

Proof. Let p be a prime where $(p, a) = 1$ with $a \in \mathbf{Z}$ and also consider the set $P = \{1, 2, 3, ..., p\}$. For elements p_1 and $p_2 \in P$, suppose that $p_1 a \equiv p_2 a \pmod{p}$. Then $p_1 a - p_2 a \equiv 0 \pmod{p} \implies p \mid (p_1 a - p_2 a) \implies p \mid a(p_1 - p_2)$. Since $(p, a) = 1$, we can conclude that $p \mid (p_1 - p_2)$. However, since p_1 and $p_2 \in P$, then $(p_1 - p_2)$ must be smaller then p. Therefore, $p \nmid (p_1 - p_2)$. This implies that every element in P is not congruent to each other modulo o. Hence they are all distinct elements as modulo p.

Now, let's consider the set $\{a, 2a, 3a, ..., pa\}$. The same implication above follows the as well, as;

$$\begin{aligned}
&\implies p_1 a \equiv p_2 a \pmod{p} && p_1 \text{ and } p_2 \in P \\
&\implies p_1 \equiv p_2 \pmod{p} \\
&\implies p_1 - p_2 \equiv 0 \pmod{p} \\
&\implies p \mid (p_1 - p_2)a \\
&\implies p \mid (p_1 - p_2) && \text{Since, } (p, a) = 1.
\end{aligned}$$

However, since p_1 and $p_2 \in P$, then $(p_1 - p_2)$ must be smaller then p. Each element in the set $\{a, 2a, 3a, ..., pa\}$ is distinct modulo p and thus is a complete residue system modulo p. □

4.14 Theorem

Let p be a prime and let a be an integer not divisible by p. Then

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

Proof. Let p be a prime where $(p, a) = 1$ with $a \in \mathbf{Z}$. Let $a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a$ be multiples of a. Also lets assume that xa, ya are multiples of a and that $xa \equiv ya \pmod{p}$, then;

$$\begin{aligned}
&xa \equiv ya \pmod{p} \\
&xa - ya \equiv 0 \pmod{p} \\
&p \mid (xa - ya) \\
&p \mid (x - y)a \\
&p \mid (x - y) && \text{Since, } (p, a) = 1. \\
&x - y \equiv 0 \pmod{p} \\
&x \equiv y \pmod{p}
\end{aligned}$$

Therefore, $a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a$ are distinct multiples of a. They must be congruent to $1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)$ in some order $\implies na \equiv a_n \pmod{p}, n = 1, 2, 3, ..., p-1$ where $a_n \in 1, 2, 3, ..., p-1$. Thus, the claim $a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p}$ is true. □

4.15 Theorem (Fermat's Little Theorem, Version I)

If p is a prime and a is an integer relatively prime to p, then $a^{(p-1)} \equiv 1 \pmod{p}$.

Proof. Given a prime p, let the set $\{1, 2, 3, ..., p-1\}$ be all the number modulo p, by Theorem 4.14. We can claim that some integer a is in $\{1, 2, 3, ..., p-1\}$ since $(p, a) = 1$.
If we multiply the numbers in the set $\{1, 2, 3, ..., p-1\}$ by a, we obtain $\{a, 2a, 3a, ..., (p-1)a\}$ and we know by Theorem 4.14 that;

$$\begin{aligned} a \cdot 2a \cdot 3a \cdot \cdots (p-1)a &\equiv 1 \cdot 2 \cdot 3 \cdot \cdots (p-1) \pmod{p} \\ a^{p-1} \cdot (p-1)! &\equiv (p-1)! \pmod{p} \\ a^{p-1} &\equiv 1 \pmod{p} \qquad \text{Since, } (p-1)! \pmod{p} \equiv 1 \end{aligned}$$

Since we know that all values in $\{1, 2, 3, ..., p-1\}$ are all modulo p, thus $(p-1)! \pmod{p} \equiv 1$. Hence, $a^{(p-1)} \equiv 1 \pmod{p}$.holds. □

4.16 Theorem (Fermat's Little Theorem, Version II)

If p is a prime and a is any integer; then $a^p \equiv a \pmod{p}$.

Proof. Let p be a prime and $a \in \mathbf{Z}$. Assume that $a^p \equiv a \pmod{p}$, thus we need to prove that p divides $a^p - a$ which can be expressed as $p \mid a^p - a \implies p \mid a(a^{p-1} - 1)$. Thus, we must either prove that $p \mid a$ or $p \mid a^{p-1} - 1$.
For $p \mid a^{p-1} - 1$, this can be proven by Theorem 4.15, if $(p, a) = 1$ or in other words $p \nmid a$. The theorem 4.15 fails if $p \mid a$. In that case where $p \mid a$, then $p \mid a(a^{p-1} - 1)$. Thus $a^p \equiv a \pmod{p}$ holds. □

4.17 Theorem

The two versions of Fermat's Little Theorem stated above are equivalent to one another, that is, each one can be deduced from the other.

Proof. By direct proof, given that by theorem 4.15, let p is a prime and a is an integer relatively prime to p, then $a^{(p-1)} \equiv 1 \pmod{p}$;

$$\begin{aligned} a^{(p-1)} &\equiv 1 \pmod{p} \\ a^p a^- 1 &\equiv 1 \pmod{p} \\ a^p a^- 1 \cdot a &\equiv a \pmod{p} \quad \text{Multiplying Both sides with the inverse of } a^{-1} \\ a^p &\equiv a \pmod{p} \end{aligned}$$

Thus both theorems are the same. □

4.18 Theorem

If p is a prime and a be an integer. If $(a, p) = 1$, then $ord_p(a)$ divides $p - 1$, that is, $ord_p(a) \mid p - 1$.

Proof. Let p is a prime and a be an integer where $(a, p) = 1$. □

4.19 Exercise

Compute each of the following without the aid of a calculator or computer.

1. $512^{372} \pmod{13}$ $512^{12 \cdot 13} \pmod{13}$
   $512^{12 \cdot 13} \pmod{13}$
   $512^1 2^1 3 \pmod{13}$
   $1^1 3 \pmod{13}$
   $1 \pmod{13}$

2. $3444^{3233} \pmod{17}$
   $3444^{202(16)+1} \pmod{17}$
   $3444^{202(16)} 3444^1 \pmod{17}$
   $3444^1 \pmod{17}$

3. $123^{456} \pmod{23}$ $123^{20(22)+16} \pmod{23}$
   $123^{20(22)} 123^1 6 \pmod{23}$
   $123^1 6 \pmod{23}$

4.20 Exercise

Find the remainder upon division of 314^{159} by 31.

Using Fermat's Little Theorem, we can deduce that $314^{30} \equiv 1 \pmod{31}$. Also we can deduce that $159 = 30(5) + 9$. Now,

$$
\begin{aligned}
&\implies 314^{159} \pmod{31} \\
&\implies 314^{30(5)+9} \pmod{31} \\
&\implies 314^{30(5)} 314^9 \pmod{31} && \text{By Fermat's Little Theorem} \\
&\implies 314^9 \pmod{31}
\end{aligned}
$$

Now, we can calculate that $314 \equiv 4 \pmod{31}$ by $314 = 31(10) + 4$. Therefore, we can manipulate $314 \equiv 4 \pmod{31}$ to achieve $314^9 \pmod{31}$;

$$314 \equiv 4 \pmod{31}$$
$$314^3 \equiv 4^3 \pmod{31}$$
$$314^3 \equiv 2 \pmod{31}$$
$$314^{33} \equiv 2^3 \pmod{31}$$
$$314^9 \equiv 8 \pmod{31}$$

4.21 Theorem

Let n and m be natural numbers that are relatively prime, and let a be an integer. If $x \equiv a \pmod{n}$ and $x \equiv a \pmod{m}$, then $x \equiv a \pmod{nm}$.

Proof. By Theroem 2.25, let a, n, and m be integers. If $n \mid (x-a)$, $m \mid (x-a)$, and $(n, m) = 1$, then $nm, \mid (x-a)$.

Also can be proven by the Chinese Remainder Theorem. □

4.22 Exercise

Find the remainder when 4^{72} is divided by $91 (= 7 \cdot 13)$.

We are attempting to solve $4^{72} \pmod{91}$. We can deduce that $72 = (7-1)(13-1) = 6 * 12$. By Theorem, 4.21, we can express this as $x \equiv 4^{72} \pmod{7}$ and $x \equiv 4^{72} \pmod{13}$. Thus,

$$x \equiv 4^{72} \pmod{7}$$
$$x \equiv 4^{6 \cdot 12} \pmod{7}$$
$$x \equiv 1^1 2 \pmod{7}$$
$$x \equiv 1 \pmod{7}$$

Similarly,

$$x \equiv 4^{72} \pmod{13}$$
$$x \equiv 4^{6 \cdot 12} \pmod{13}$$
$$x \equiv 1^6 \pmod{13}$$
$$x \equiv 1 \pmod{13}$$

4.23 Exercise

Find the natural number $k < 117$ such that $2^{117} \equiv k \pmod{117}$. (117 is not a prime).

$$2^{117} \equiv k \pmod{117}$$
$$2^{13 \cdot 3^2} \equiv k \pmod{13 \cdot 3^2}$$

By the Chinese Remainder Theorem, $2^{117} \equiv 2^3 \equiv 8 \pmod 9$ and $2^{117} \equiv 2^9 \equiv 5 \pmod{13}$.
Now let $M = m_1 m_2 m_3 = 3 \cdot 3 \cdot 13 = 117$.

- $M_1 = \frac{M}{m_1} = \frac{117}{3} = 39y_1 \equiv 1 \pmod 3$
- $M_2 = \frac{M}{m_2} = \frac{117}{3} = 39y_2 \equiv 1 \pmod 3$
- $M_3 = \frac{M}{m_3} = \frac{117}{13} = 9y_3 \equiv 1 \pmod{13}$

Now, we need to find the Multiplication inverse of each;

- $39y_1 \equiv 1 \pmod 3$ thus $39y_1 \equiv 1 \pmod 3, y_1 = 1$
- $39y_2 \equiv 1 \pmod 3$ thus $39y_2 \equiv 1 \pmod 3, y_2 = 1$
- $9y_3 \equiv 1 \pmod{13}$ thus $9y_3 \equiv 1 \pmod{13}, y_3 = 3$

Therefore;

$$k = 8(39) + 8(39) + 5(9 \cdot 3) = 795 \equiv 93 \pmod{117}$$

4.24 Theorem

Let a and b be numbers and let n be a natural number. Then

$$(a+b)^n = \textstyle\sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

4.25 Lemma

If p is prime and i is a natural number less than p, then p divides $\binom{p}{i}$.

Proof. Given p prime and i, a natural number and less than p, we can expand $\binom{p}{i}$;

$$\begin{aligned}
\binom{p}{i} &= \frac{p!}{i!(p-i)!} \\
\binom{p}{i} &= \frac{p(p-1)(p-2)\cdots(p-(i-1))(p-i)!}{i!(p-i)!} \\
\binom{p}{i} &= \frac{p(p-1)(p-2)\cdots(p-(i-1))}{i!} \\
\binom{p}{i} \cdot i! &= p(p-1)(p-2)\cdots(p-(i-1))
\end{aligned}$$

Now, p divides p thus we can express it as the following;

$$\begin{aligned}
p \mid p \implies p \mid p(p-1)(p-2)\cdots(p-(i-1)) \implies p \mid \tbinom{p}{i} \cdot i! \\
\implies p \mid \tbinom{p}{i} \cdot i(i-1)(i-2)\cdots 3 \cdot 2 \cdot 1
\end{aligned}$$

Since i is less than p, p can not divide $i!$. Thus we end up with $p \mid \binom{p}{i}$. Therefore, p must divide $\binom{p}{i}$. □

4.26 Theorem (Fermat's Little Theorem, Version II)

If p is a prime and a is any integer; then $a^p \equiv a \pmod{p}$.

Proof. □

4.27 Question

The numbers 1,5,7 and 11 are all natural numbers less than or equal to 12 that are relatively prime to 12, so $\phi(12) = 4$.

1. What is $\phi(7)$? $\phi(7) = 4$
2. What is $\phi(15)$? $\phi(15) = 8$
3. What is $\phi(21)$? $\phi(21) = 12$
4. What is $\phi(35)$? $\phi(35) = 24$

4.28 Theorem

Let a, b, and n be integers such that $(a, n) = 1$ and $(b, n) = 1$. Then $(ab, n) = 1$.

Proof. By Theorem 1.43. □

4.29 Theorem

Let a, b, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $(a, n) = 1$, then $(b, n) = 1$.

Proof. Given a, b, and n be integers with $n > 0$, $a \equiv b \pmod{n}$ and $(a, n) = 1$. We can express $a \equiv b \pmod{n} \implies n \mid (a - b) \implies nd = a - b \implies a = nd + b, \exists d \in \mathbf{Z}$. Since $(a, n) = 1$, $b \neq 0$. Also, $(a, n) = 1 = ax + ny, \exists x, y \in \mathbf{Z}$.

Now, we can substitute in $a = nd + b$ for a in $1 = ax + ny$;

$$
\begin{aligned}
1 &= ax + ny \\
1 &= (nd + b)x + ny \\
1 &= ndx + bx + ny \\
1 &= n(dx + y) + bx \\
1 &= nz + bx && \text{Some integer } z = dx + y \\
1 &= (b, n)
\end{aligned}
$$

□

4.30 Theorem

Let a, b, c and n be integers with $n > 0$. If $ac \equiv bc \pmod{n}$ and (c,n) = 1, then $a \equiv b \pmod{n}$.

Proof. By Theorem 1.45. □

4.31 Theorem

Let n be a natural number and let $x_1, x_2, ..., x_{\phi(n)}$ be the distinct natural numbers less than or equal to n that are relatively prime to n. Let a be a non-zero integer relatively prime to n and let i and j be different natural numbers less than or equal to $\phi(n)$. Then $ax_i \not\equiv ax_j \pmod{n}$.

Proof. Let n be a natural number and let $x_1, x_2, ..., x_{\phi(n)}$ be the distinct natural numbers less than or equal to n that are relatively prime to n. Also let a be a non-zero integer relatively prime to n and let i and j be different natural numbers less than or equal to $\phi(n)$.
Now we must show that $ax_i \not\equiv ax_j \pmod{n}$. Suppose, by contradiction, $ax_i \equiv ax_j \pmod{n}$, we can express this as $n \mid a(x_i - x_j)$. Since $(a, n) = 1$, then $n \mid (x_i - x_j)$. By definition, that also signifies that $x_i \equiv x_j \pmod{n}$ which is impossible since we have stated that i and j are different natural numbers. Thus, $x_i \not\equiv x_j \pmod{n}$ which also implies that $ax_i \not\equiv ax_j \pmod{n}$. □

4.32 Theorem (Euler's Theorem)

If a and n are integers with $n > 0$ and $(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Proof. Let a and n be integers with $n > 0$ and $(a, n) = 1$. Also suppose a set of integers $A = \{x_1, x_2, ..., x_{\phi_n}\}$ less than n such that $(n, x_i) = 1, i = 1, 2, 3, ..., n$. Then, we'll need to prove that;

$$\{ax_1 \pmod{n}, ax_2 \pmod{n}, ax_3 \pmod{n}, ..., ax_{\phi_n} \pmod{n}\} = \{x_1, x_2, ..., x_{\phi_n}\}$$

We can observe that each $ax_i \pmod{n}$ is less than n and we know that $(n, x_i) = 1$ and that $(n, a) = 1$, thus, by Theorem 4.28, $(n, ax_i) = 1$. Which then implies that the following is true;

$$\{ax_1 \pmod{n}, ax_2 \pmod{n}, ax_3 \pmod{n}, ..., ax_{\phi_n} \pmod{n}\} = \{x_1, x_2, ..., x_{\phi_n}\}$$

This implies then that;

$$ax_1 \cdot ax_2 \cdot ax_3 \cdots ax_{\phi_n} \equiv x_1 \cdot x_2 \cdot x_3 \cdots x_{\phi_n} \pmod{n}$$
$$a^{\phi(n)}(x_1 \cdot x_2 \cdot x_3 \cdots x_{\phi_n}) \equiv x_1 \cdot x_2 \cdot x_3 \cdots x_{\phi_n} \pmod{n}$$
$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Thus, the Euler Theorem holds. □

4.33 Corollary (Fermat's Little Theorem)

If p is a prime and a is an integer relatively prime to p, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. We can use another form of Fermat's Little Theorem which is $a^p \equiv a \pmod{p}$ with a p prime and an integer a such that $(p, a) = 1$. Now, we can deduce that the $\phi(p) = p-1$ since primes are not divisible by any other number. Thus, we can express Fermat's Little Theorem as $a^{\phi(p)} \equiv a \pmod{p}$. Since $(p, a) = 1$ an by theorem 4.2, we can then conclude that $a^{\phi(p)} \equiv a \pmod{p}$ holds. □

4.34 Exercise

Compute each of the following without the aid of a calculator or computer.

1. $12^{49} \pmod{15}$ with $\phi(15) = 8$
   $12^{7 \cdot 7} \pmod{15}$
   $12^{(8-1) \cdot 7} \pmod{15}$
   $(12^8 12^{-1})^7 \pmod{15}$
   $(12^{-1})^7 \pmod{15}$
   $12^{-8+1} \pmod{15}$
   $12^{-8} 12^1 \pmod{15}$
   $12^1 \pmod{15}$
   $12 \pmod{15}$

2. $139^{112} \pmod{27}$ with $\phi(27) = 18$
   $139^{18(7)+13} \pmod{27}$
   $139^{18(7)} 139^{13} \pmod{27}$
   $139^1 3 \pmod{27}$
   $139^{18-5} \pmod{27}$
   $139^5 \pmod{27}$

4.35 Exercise

Find the last digit in the base 10 representation of the integer 13^{474}.

- $13 \equiv 3 \pmod{10}$
- $13^0 \equiv 3^0 \equiv 1 \pmod{10}$
- $13^2 \equiv 3^2 \equiv 9 \pmod{10}$
- $13^3 \equiv 3^3 \equiv 7 \pmod{10}$
- $13^4 \equiv 3^4 \equiv 1 \pmod{10}$
- Thus we can find the exponent remainder at modulo 4.

- $474 \equiv 2 \pmod 4$
- Thus, $13^2 \equiv 169 \equiv 9 \pmod{10}$

4.36 Theorem

Let p be a prime and let a be an integer such that $1 \leq a < p$. Then there exists a unique natural number b less than p such that $ab \equiv 1 \pmod p$.

Proof. Let p be a prime and let a be an integer such that $1 \leq a < p$. Assume that there exists a unique natural number b and less than p. We can deduce that $1 \leq a < p$ implies that $(a, p) = 1$ since p is prime and a is less than p. Moreover, we can also express $ab \equiv 1 \pmod p$ as $(ab, p) = 1$. Now by Theorem 4.29, for $(ab, p) = 1$ to hold, $(b, p) = 1$ must also hold. In this case we know than b is unique and is less than prime p, thus b can not divide p or p can not divide b. Therefore, $(b, p) = 1$ must be true and thus so is $(ab, p) = 1$. □

4.37 Exercise

Let p be a prime. Show that the natural numbers 1 and $p - 1$ are their own inverses modulo p.

Proof. Let p be a prime number. Let also the set $\{1, 2, 3, ..., (p-1)\}$. We can show that 1 is it's own inverse since 1 holds the identity property of the aforementioned set, $1^{-1} \equiv 1 \pmod p$. Now for $p - 1$, we'll first consider $(p - 1)(p - 1)$,

$$\begin{aligned}
(p-1)^2 &= p^2 - 2p + 1 \\
(p-1)^2 &= p(p-2) + 1 \\
(p-1)^2 \pmod p &= (p(p-2)+1) \pmod p \quad \text{Apply } \pmod p \text{ in both sides} \\
(p-1)^2 &\equiv 1 \pmod p \\
(p-1)(p-1) &\equiv 1 \pmod p \\
(p-1)(p-1) \cdot (p-1)^{-1} &\equiv (p-1)^{-1} \pmod p \\
(p-1) &\equiv (p-1)^{-1} \pmod p
\end{aligned}$$

Thus, the natural numbers 1 and $p - 1$ are their own inverses modulo p. □

4.38 Theorem

Let p be a prime and let a and b be integers such that $1 < a, b < p - 1$ and $ab \equiv 1 \pmod p$. Then $a \neq b$.

Proof. Let p be a prime and let a and b be integers such that $1 < a, b < p - 1$ and $ab \equiv 1 \pmod p$. Now lets assume, by contradiction, that $a = b$. Then, $ab \equiv a^2 \equiv 1 \pmod p$. Also, by definition, $a^2 \equiv 1 \pmod p \implies p \mid a^2 - 1$ where $a^2 - 1 = (a + 1)(a - 1)$. Since p is a prime, can divide $a - 1$ or $a + 1$.

However, since we know that $1 < a < p - 1$, which can also be expressed as $1 < a + 1 < p$, this implies that p can not divide a_1. Similarly, since $a < p - 1$, p can not divide $a + 1$ either. This signifies that $p \nmid a^2 = ab, a = b$. Thus $a \neq b$. □

4.39 Exercise

Find all pairs of number a and b in $\{2, 3, ..., 11\}$ *such that* $ab \equiv 1 \pmod{13}$.

$ab \equiv 1 \pmod{13}$ implies that $a^{-1} \equiv b \pmod{13}$. Now with the set of all natural numbers less than 13 $\{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. Let's start to identify pairs a an b where $ab \equiv 1 \pmod{13}$ implies that $a^{-1} \equiv b \pmod{13}$.

- 2 and 7
- 3 and 9
- 5 and 8
- 4 and 10
- 6 and 11

4.40 Theorem

If p is a prime larger than 2, then $2 \cdot 3 \cdot 4 \cdot \cdots \cdot (p - 2) \equiv 1 \pmod{p}$.

Proof. Let there be a prime p larger than 2. Then each integer from 1,...,(p-1) has an inverse modulo p. Now we must show that the inverse is unique.
Let a, b and c be integers where a has no inverse for some distinct b and c modulo p;

$$\begin{aligned} ab &\equiv ac \pmod{p} \\ ab - ac &\equiv 0 \pmod{p} \\ a(b - c) &\equiv 0 \pmod{p} \end{aligned}$$

Therefore, $p \mid a(b - c)$. However, p does not divide a or b-c, which is a contraction. Thus, 1,...,(p-1) has unique inverse modulo p.
If a is it's own inverse then;

$$\begin{aligned} a^2 &\equiv 1 \pmod{p} \\ a^2 - 1 &\equiv 0 \pmod{p} \\ (a + 1)(a - 1) &\equiv 0 \pmod{p} \end{aligned}$$

Thus, $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p} \implies a \equiv p - 1 \pmod{p}$. Hence, we can conclude that the inverse of 1 and p-1 is a itself.
Thus, for each integer $a \in \{2, ..., (p - 2)\}$ there exist a $b \in \{2, ..., (p - 2)\}$ such that $ab \equiv 1 \pmod{p}$ which will get $2 \cdot 3 \cdot 4 \cdot \cdots \cdot (p - 2) \equiv 1 \pmod{p}$. □

4.41 Theorem (Wilson's Theorem)

If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. By Theorem, 4.40, suppose p is a prime larger than 2, then $2 \cdot 3 \cdot 4 \cdots \cdot (p-2) \equiv 1 \pmod{p}$. Now, let's multiply (p-1) in both sides;

$$\begin{aligned} 2 \cdot 3 \cdot 4 \cdots \cdot (p-2) &\equiv 1 \pmod{p} \\ 2 \cdot 3 \cdot 4 \cdots \cdot (p-2) \cdot (p-1) &\equiv (p-1) \pmod{p} \\ 2 \cdot 3 \cdot 4 \cdots \cdot (p-2) \cdot (p-1) &\equiv -1 \pmod{p} \\ (p-1)! &\equiv -1 \pmod{p} \end{aligned}$$

Thus, if p is a prime, then $(p-1)! \equiv -1 \pmod{p}$. □

4.42 Theorem (Converse of Wilson's Theorem)

If n is a natural number such that

$$(n-1)! \equiv -1 \pmod{n},$$

then n is prime.

Proof. Given that n is a natural number such that $(n-1)! \equiv -1 \pmod{n}$. By contradiction let's assume that n is composite. Therefore, it's possible divisions are $1, 2, ..., n-1$ which also implies that the $gcd((n-1)!, n) > 1$. If that's the case then we can not have $(n-1)! \equiv -1 \pmod{n}$. Therefore, n must be prime. □

4.43 Blank Paper Exercise

- Integer to the high power modulo n
- Fermat's Little Theorem
- Binomial Theorem
- Euler's Theorem
- Wilson's Theorem
- Proof 4.24 and 4.26 were extremely difficult and I wasn't able to get.

Supplementary Exercises

4.1.1 Exercise

- a = 2
  - $2^2 \pmod{3} \equiv 1$

- $2^3 \pmod 3 \equiv 2$
- $2^5 \pmod 6 \equiv 1$
- $2^7 \pmod 3 \equiv 2$
- $2^8 \pmod 9 \equiv 1$

- a = 3
  - $3^2 \pmod 5 \equiv 4$
  - $3^3 \pmod 5 \equiv 2$
  - $3^5 \pmod 6 \equiv 1$
  - $3^7 \pmod 5 \equiv 2$
  - $3^8 \pmod 9 \equiv 1$

Conjecture. *When a is a prime 2 or 3 and k=n-1 where n is prime, then* $a^k \equiv 1 \pmod n$.

4.1.2 Theorem

If $(a, n) = 1$*, the period d of the sequence* $a^k \pmod n$ *is given by* $d = ord_n(a)$.

Proof. By Theorem 4.6. □

4.1.3.a Theorem

If $n = a^k$*, the sequence of* $a^k \equiv 1 \pmod n$ *values becomes all zeros after an initial k 1 terms, and these are the only cases in which the period of repetition is one.*

Proof. By definiton, let a and n be natural numbers with $(a, n) = 1$. The smallest natural number k such that $a^k \equiv 1 \pmod n$ is $ord_n(a)$. □

4.1.3.b Theorem

If $n = a^k 1$ *then* $d = k$ *and if* $n = a^k + 1$*, then* $d = 2k$.

Proof. Since $n = a^k 1$ can imply that $a^k \equiv 1 \pmod n$ then if $n = a^k + 1$ implies that $a^k + 2 \equiv 1 \pmod n$, thus $d = 2k$. □

4.1.4 Theorem

If q is prime with (a, q) = 1 and $n = a^r q$ *for some natural number r, define* $ord_n(a) = min k | a^k = 1 mod n$*. Then* $ord_n(a) = ord_q(a)$ *and q = 1 mod (k).*

Proof. By definiton, let a and n be natural numbers with $(a, n) = 1$. The smallest natural number k such that $a^k \equiv 1 \pmod n$ is $ord_n(a)$. Thus if $ord_n(a) = min k | a^k = 1 mod n$ then $ord_n(a) = ord_q(a)$ if and only if q = 1 mod (k). □

4.1.5 Question

That the order will not still signify the smallest value. As there will be instances where $a^k \equiv 0 \pmod{n}$.

4.1.6 Question

That if (a, n) $\neq 1$ then the order will still be less than n and signify the smallest possible value b such that $a^k \equiv b \pmod{n}$.

4.1.7 Question

We are able to define the order function for instances where a and n are not relatively prime.

4.2.1 Lemma

Proof. In the case where n is prime, we can prove this theorem by Lemma 4.25. However, when n is composite we can notice that n always divides n-1$\binom{}{i.}$ □

4.2.2 Lemma

Proof.

0						1						
1					1		1					
2				1		2		1				
3			1		3		3		1			
4		1		4		6		4		1		
5	1		5		10		10		5		1	
6	1	6		15		20		15		6		1

□

4.2.3 Theorem

For all primes p and all $k \geq 0, (a+b)^{p^k} = a^{p^k} + b^{p^k} \pmod{p}$.

Proof. $(a+b)^{p^k}$ will always result to $a^{p^k} + ... + b^{p^k}$. Since everything in between will be a product of a and b of some sort, when we perform modulo p, it will result to 0, since p is then considered for all primes. □

4.2.4 Exercise

- $(a+b)^{17} \equiv a^{17} + b^{17} \pmod{2}$
- $(a+b)^{585} \equiv a^{585} + b^{585} \pmod{2}$
- $(a+b)^{279} \equiv a^{279} + b^{279} \pmod{2}$
- $(a+b)^{3155} \equiv a^{3155} + b^{3155} \pmod{2}$

4.2.7 Theorem

For $n = p^k, (a_1 + \ + a_n)^n = a_1^n + \ + a_m^n$ mod (p). This result is especially useful for $p = 2$.

Proof. By Theorem 4.2.3. □