Discrete Logarithms and Rabin’s Probabilistic Primality Test

Bernd Schröder
Introduction
Introduction

1. Indices play the role of “logarithms modulo $m$.”
Introduction

1. Indices play the role of “logarithms modulo $m$.” (So they are a natural next step in our investigation of modular arithmetic.)
Introduction

1. Indices play the role of “logarithms modulo $m$.” (So they are a natural next step in our investigation of modular arithmetic.)

2. We will use indices to determine which numbers are power residues, that is “$n^{th}$ powers modulo $m$.”
Introduction

1. Indices play the role of “logarithms modulo \( m \).” (So they are a natural next step in our investigation of modular arithmetic.)

2. We will use indices to determine which numbers are power residues, that is “\( n^{th} \) powers modulo \( m \).” (Okay, the theorem will only work when there are primitive roots modulo \( m \).)
Introduction

1. Indices play the role of “logarithms modulo $m$.” (So they are a natural next step in our investigation of modular arithmetic.)

2. We will use indices to determine which numbers are power residues, that is “$n^{th}$ powers modulo $m$.” (Okay, the theorem will only work when there are primitive roots modulo $m$.)

3. Note that Miller’s primality test fails to detect a number as being composite when certain power equations are solvable.
Introduction

1. Indices play the role of “logarithms modulo $m$.” (So they are a natural next step in our investigation of modular arithmetic.)

2. We will use indices to determine which numbers are power residues, that is “$n^{\text{th}}$ powers modulo $m$.” (Okay, the theorem will only work when there are primitive roots modulo $m$.)

3. Note that Miller’s primality test fails to detect a number as being composite when certain power equations are solvable. The investigation of power residues will lead us to Rabin’s primality test.
Definition.
**Definition.** Let \(a, m \in \mathbb{N}\) be so that there is a primitive root \(r\) modulo \(m\) and \((a, m) = 1\). The unique integer \(x \in \{1, \ldots, \varphi(m)\}\) so that \(r^x \equiv a \pmod{m}\) is called the **index** or discrete logarithm of \(a\) to the base \(r\) modulo \(m\).
Definition. Let \( a, m \in \mathbb{N} \) be so that there is a primitive root \( r \) modulo \( m \) and \( (a, m) = 1 \). The unique integer \( x \in \{1, \ldots, \phi(m)\} \) so that \( r^x \equiv a \pmod{m} \) is called the **index or discrete logarithm of \( a \) to the base \( r \) modulo \( m \). It is denoted \( \text{ind}_r(a) \), assuming the underlying modulus is fixed.
**Definition.** Let $a, m \in \mathbb{N}$ be so that there is a primitive root $r$ modulo $m$ and $(a, m) = 1$. The unique integer $x \in \{1, \ldots, \varphi(m)\}$ so that $r^x \equiv a \pmod{m}$ is called the **index or discrete logarithm** of $a$ **to the base** $r$ modulo $m$. It is denoted $\text{ind}_r(a)$, assuming the underlying modulus is fixed.

**Example.**
Definition. Let $a, m \in \mathbb{N}$ be so that there is a primitive root $r$ modulo $m$ and $(a, m) = 1$. The unique integer $x \in \{1, \ldots, \varphi(m)\}$ so that $r^x \equiv a \pmod{m}$ is called the index or discrete logarithm of $a$ to the base $r$ modulo $m$. It is denoted $\text{ind}_r(a)$, assuming the underlying modulus is fixed.

Example. 2 is a primitive root modulo 11
**Definition.** Let $a, m \in \mathbb{N}$ be so that there is a primitive root $r$ modulo $m$ and $(a, m) = 1$. The unique integer $x \in \{1, \ldots, \varphi(m)\}$ so that $r^x \equiv a \pmod{m}$ is called the **index or discrete logarithm of $a$ to the base $r$ modulo $m$**. It is denoted $\text{ind}_r(a)$, assuming the underlying modulus is fixed.

**Example.** 2 is a primitive root modulo 11, so we can compute indices to the base 2 in modulo 11 arithmetic.
**Definition.** Let \( a, m \in \mathbb{N} \) be so that there is a primitive root \( r \mod m \) and \((a, m) = 1\). The unique integer \( x \in \{1, \ldots, \phi(m)\} \) so that \( r^x \equiv a \mod m \) is called the **index or discrete logarithm of** \( a \) **to the base** \( r \) **modulo** \( m \). It is denoted \( \text{ind}_r(a) \), assuming the underlying modulus is fixed.

**Example.** 2 is a primitive root modulo 11, so we can compute indices to the base 2 in modulo 11 arithmetic. For example, \( \text{ind}_2(10) = 5 \).
**Definition.** Let $a, m \in \mathbb{N}$ be so that there is a primitive root $r$ modulo $m$ and $(a, m) = 1$. The unique integer $x \in \{1, \ldots, \varphi(m)\}$ so that $r^x \equiv a \pmod{m}$ is called the **index or discrete logarithm of $a$ to the base $r$ modulo $m$**. It is denoted $\text{ind}_r(a)$, assuming the underlying modulus is fixed.

**Example.** 2 is a primitive root modulo 11, so we can compute indices to the base 2 in modulo 11 arithmetic. For example, $\text{ind}_2(10) = 5$. 

Theorem.
Theorem. Let $m \in \mathbb{N}$ be so that $r$ is a primitive root modulo $m$. Let $a, b \in \mathbb{Z}$ be so that $(a, m) = (b, m) = 1$. 

Proof. 

1. $r^{\phi(m)} \equiv 1 \pmod{m}$, so, because no smaller positive power of $r$ is congruent to 1, $\text{ind}_r(1) \equiv 0 \pmod{\phi(m)}$. 

2. $r^{\text{ind}_r(ab)} = r^{\text{ind}_r(a) + \text{ind}_r(b)} \equiv ab \equiv r^{\text{ind}_r(ab)} \pmod{m}$. The claimed equality now follows from an earlier theorem about canceling bases. 

3. $r^{k \text{ind}_r(a)} = (r^{\text{ind}_r(a)})^k \equiv a^k \equiv r^{\text{ind}_r(a^k)} \pmod{m}$. The claimed equality now follows from an earlier theorem about canceling bases.
Theorem. Let $m \in \mathbb{N}$ be so that $r$ is a primitive root modulo $m$. Let $a, b \in \mathbb{Z}$ be so that $(a,m) = (b,m) = 1$. Then

1. $\text{ind}_r(1) \equiv 0 \pmod{\varphi(m)}$. 

Theorem. Let $m \in \mathbb{N}$ be so that $r$ is a primitive root modulo $m$. Let $a, b \in \mathbb{Z}$ be so that $(a, m) = (b, m) = 1$. Then

1. $\text{ind}_r(1) \equiv 0 \pmod{\varphi(m)}$.
2. $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)}$. 

Proof. 1. $r^{\varphi(m)} \equiv 1 \pmod{m}$, so, because no smaller positive power of $r$ is congruent to 1, $\text{ind}_r(1) \equiv 0 \pmod{\varphi(m)}$.

2. $r^{\text{ind}_r(a)} \equiv a \pmod{m}$ and $r^{\text{ind}_r(b)} \equiv b \pmod{m}$, so $r^{\text{ind}_r(ab)} \equiv ab \pmod{m}$. The claimed equality now follows from an earlier theorem about canceling bases.

3. $r^{k \text{ind}_r(a)} \equiv a^k \pmod{m}$, so $\text{ind}_r(a^k) \equiv k \text{ind}_r(a) \pmod{\varphi(m)}$. The claimed equality now follows from an earlier theorem about canceling bases.
Theorem. Let \( m \in \mathbb{N} \) be so that \( r \) is a primitive root modulo \( m \). Let \( a, b \in \mathbb{Z} \) be so that \((a,m) = (b,m) = 1\). Then

1. \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( \text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)} \).
3. For all \( k \in \mathbb{N} \), we have \( \text{ind}_r(a^k) \equiv k \text{ind}_r(a) \pmod{\varphi(m)} \).
Theorem. Let $m \in \mathbb{N}$ be so that $r$ is a primitive root modulo $m$. Let $a, b \in \mathbb{Z}$ be so that $(a, m) = (b, m) = 1$. Then

1. $\text{ind}_r(1) \equiv 0 \pmod{\varphi(m)}$.
2. $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)}$.
3. For all $k \in \mathbb{N}$, we have $\text{ind}_r(a^k) \equiv k\text{ind}_r(a) \pmod{\varphi(m)}$.

Proof.
Theorem. Let \( m \in \mathbb{N} \) be so that \( r \) is a primitive root modulo \( m \). Let \( a, b \in \mathbb{Z} \) be so that \( (a, m) = (b, m) = 1 \). Then

1. \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( \text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)} \).
3. For all \( k \in \mathbb{N} \), we have \( \text{ind}_r(a^k) \equiv k\text{ind}_r(a) \pmod{\varphi(m)} \).

Proof.

1. \( r^{\varphi(m)} \equiv 1 \pmod{m} \)
**Theorem.** Let $m \in \mathbb{N}$ be so that $r$ is a primitive root modulo $m$. Let $a, b \in \mathbb{Z}$ be so that $(a, m) = (b, m) = 1$. Then

1. $\text{ind}_r(1) \equiv 0 \pmod{\varphi(m)}$.
2. $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)}$.
3. For all $k \in \mathbb{N}$, we have $\text{ind}_r(a^k) \equiv k\text{ind}_r(a) \pmod{\varphi(m)}$.

**Proof.**

1. $r^{\varphi(m)} \equiv 1 \pmod{m}$, so, because no smaller positive power of $r$ is congruent to 1, $\text{ind}_r(1) \equiv 0 \pmod{\varphi(m)}$. 
Theorem. Let \( m \in \mathbb{N} \) be so that \( r \) is a primitive root modulo \( m \). Let \( a, b \in \mathbb{Z} \) be so that \( (a, m) = (b, m) = 1 \). Then

1. \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( \text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)} \).
3. For all \( k \in \mathbb{N} \), we have \( \text{ind}_r(a^k) \equiv k \cdot \text{ind}_r(a) \pmod{\varphi(m)} \).

Proof.

1. \( r^{\varphi(m)} \equiv 1 \pmod{m} \), so, because no smaller positive power of \( r \) is congruent to 1, \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).

2. \( r^{\text{ind}_r(a) + \text{ind}_r(b)} \)
Theorem. Let $m \in \mathbb{N}$ be so that $r$ is a primitive root modulo $m$. Let $a, b \in \mathbb{Z}$ be so that $(a, m) = (b, m) = 1$. Then

1. $\text{ind}_r(1) \equiv 0 \pmod{\phi(m)}$.
2. $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\phi(m)}$.
3. For all $k \in \mathbb{N}$, we have $\text{ind}_r(a^k) \equiv k \text{ind}_r(a) \pmod{\phi(m)}$.

Proof.
1. $r^{\phi(m)} \equiv 1 \pmod{m}$, so, because no smaller positive power of $r$ is congruent to 1, $\text{ind}_r(1) \equiv 0 \pmod{\phi(m)}$.
2. $r^{\text{ind}_r(a)+\text{ind}_r(b)} = r^{\text{ind}_r(a)} r^{\text{ind}_r(b)}$
Theorem. Let $m \in \mathbb{N}$ be so that $r$ is a primitive root modulo $m$. Let $a, b \in \mathbb{Z}$ be so that $(a, m) = (b, m) = 1$. Then

1. $\text{ind}_r(1) \equiv 0 \pmod{\varphi(m)}$.
2. $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)}$.
3. For all $k \in \mathbb{N}$, we have $\text{ind}_r(a^k) \equiv k \text{ind}_r(a) \pmod{\varphi(m)}$.

Proof.

1. $r^{\varphi(m)} \equiv 1 \pmod{m}$, so, because no smaller positive power of $r$ is congruent to 1, $\text{ind}_r(1) \equiv 0 \pmod{\varphi(m)}$.
2. $r^{\text{ind}_r(a) + \text{ind}_r(b)} = r^{\text{ind}_r(a)} r^{\text{ind}_r(b)} \equiv ab$
Theorem. Let \( m \in \mathbb{N} \) be so that \( r \) is a primitive root modulo \( m \). Let \( a, b \in \mathbb{Z} \) be so that \((a,m) = (b,m) = 1\). Then

1. \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( \text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)} \).
3. For all \( k \in \mathbb{N} \), we have \( \text{ind}_r(a^k) \equiv k \text{ind}_r(a) \pmod{\varphi(m)} \).

Proof.

1. \( r^{\varphi(m)} \equiv 1 \pmod{m} \), so, because no smaller positive power of \( r \) is congruent to 1, \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( r^{\text{ind}_r(a) + \text{ind}_r(b)} = r^{\text{ind}_r(a)} r^{\text{ind}_r(b)} \equiv ab \equiv r^{\text{ind}_r(ab)} \pmod{m} \).
Theorem. Let \( m \in \mathbb{N} \) be so that \( r \) is a primitive root modulo \( m \). Let \( a, b \in \mathbb{Z} \) be so that \( (a, m) = (b, m) = 1 \). Then

1. \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( \text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)} \).
3. For all \( k \in \mathbb{N} \), we have \( \text{ind}_r(a^k) \equiv k \text{ind}_r(a) \pmod{\varphi(m)} \).

Proof.

1. \( r^{\varphi(m)} \equiv 1 \pmod{m} \), so, because no smaller positive power of \( r \) is congruent to 1, \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( r^{\text{ind}_r(a) + \text{ind}_r(b)} = r^{\text{ind}_r(a)} r^{\text{ind}_r(b)} \equiv ab \equiv r^{\text{ind}_r(ab)} \pmod{m} \). The claimed equality now follows from an earlier theorem about canceling bases.
**Theorem.** Let $m \in \mathbb{N}$ be so that $r$ is a primitive root modulo $m$. Let $a, b \in \mathbb{Z}$ be so that $(a, m) = (b, m) = 1$. Then

1. $\text{ind}_r(1) \equiv 0 \pmod{\varphi(m)}$.
2. $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)}$.
3. For all $k \in \mathbb{N}$, we have $\text{ind}_r(a^k) \equiv k \text{ind}_r(a) \pmod{\varphi(m)}$.

**Proof.**

1. $r^{\varphi(m)} \equiv 1 \pmod{m}$, so, because no smaller positive power of $r$ is congruent to 1, $\text{ind}_r(1) \equiv 0 \pmod{\varphi(m)}$.
2. $r^{\text{ind}_r(a)+\text{ind}_r(b)} \equiv r^{\text{ind}_r(a)}r^{\text{ind}_r(b)} \equiv ab \equiv r^{\text{ind}_r(ab)} \pmod{m}$. The claimed equality now follows from an earlier theorem about canceling bases.

3. $r^{k \text{ind}_r(a)}$
Theorem. Let \( m \in \mathbb{N} \) be so that \( r \) is a primitive root modulo \( m \). Let \( a, b \in \mathbb{Z} \) be so that \((a, m) = (b, m) = 1\). Then

1. \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( \text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)} \).
3. For all \( k \in \mathbb{N} \), we have \( \text{ind}_r(a^k) \equiv k \text{ind}_r(a) \pmod{\varphi(m)} \).

Proof.

1. \( r^{\varphi(m)} \equiv 1 \pmod{m} \), so, because no smaller positive power of \( r \) is congruent to 1, \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( r^{\text{ind}_r(a)+\text{ind}_r(b)} = r^{\text{ind}_r(a)} r^{\text{ind}_r(b)} \equiv ab \equiv r^{\text{ind}_r(ab)} \pmod{m} \). The claimed equality now follows from an earlier theorem about canceling bases.
3. \( r^{k \text{ind}_r(a)} = \left(r^{\text{ind}_r(a)}\right)^k \).
Theorem. Let \( m \in \mathbb{N} \) be so that \( r \) is a primitive root modulo \( m \).

Let \( a, b \in \mathbb{Z} \) be so that \((a, m) = (b, m) = 1\). Then

1. \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( \text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)} \).
3. For all \( k \in \mathbb{N} \), we have \( \text{ind}_r(a^k) \equiv k \text{ind}_r(a) \pmod{\varphi(m)} \).

Proof.

1. \( r^{\varphi(m)} \equiv 1 \pmod{m} \), so, because no smaller positive power of \( r \) is congruent to 1, \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( r^{\text{ind}_r(a)+\text{ind}_r(b)} = r^{\text{ind}_r(a)} r^{\text{ind}_r(b)} \equiv ab \equiv r^{\text{ind}_r(ab)} \pmod{m} \). The claimed equality now follows from an earlier theorem about canceling bases.
3. \( r^{k\text{ind}_r(a)} = (r^{\text{ind}_r(a)})^k \equiv a^k \)
Theorem. Let \( m \in \mathbb{N} \) be so that \( r \) is a primitive root modulo \( m \). Let \( a, b \in \mathbb{Z} \) be so that \((a, m) = (b, m) = 1\). Then

1. \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( \text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)} \).
3. For all \( k \in \mathbb{N} \), we have \( \text{ind}_r(a^k) \equiv k \text{ind}_r(a) \pmod{\varphi(m)} \).

Proof.
1. \( r^{\varphi(m)} \equiv 1 \pmod{m} \), so, because no smaller positive power of \( r \) is congruent to 1, \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( r^{\text{ind}_r(a) + \text{ind}_r(b)} = r^{\text{ind}_r(a)} r^{\text{ind}_r(b)} \equiv ab \equiv r^{\text{ind}_r(ab)} \pmod{m} \). The claimed equality now follows from an earlier theorem about canceling bases.
3. \( r^{k \text{ind}_r(a)} = \left(r^{\text{ind}_r(a)}\right)^k \equiv a^k \equiv r^{\text{ind}_r(a^k)} \pmod{m} \).
**Theorem.** Let \( m \in \mathbb{N} \) be so that \( r \) is a primitive root modulo \( m \).
Let \( a, b \in \mathbb{Z} \) be so that \( (a,m) = (b,m) = 1 \). Then

1. \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( \text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)} \).
3. For all \( k \in \mathbb{N} \), we have \( \text{ind}_r(a^k) \equiv k\text{ind}_r(a) \pmod{\varphi(m)} \).

**Proof.**

1. \( r^{\varphi(m)} \equiv 1 \pmod{m} \), so, because no smaller positive power of \( r \) is congruent to 1, \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( r^{\text{ind}_r(a)+\text{ind}_r(b)} = r^{\text{ind}_r(a)} r^{\text{ind}_r(b)} \equiv ab \equiv r^{\text{ind}_r(ab)} \pmod{m} \). The claimed equality now follows from an earlier theorem about canceling bases.
3. \( r^{k\text{ind}_r(a)} = \left(r^{\text{ind}_r(a)}\right)^k \equiv a^k \equiv r^{\text{ind}_r(a^k)} \pmod{m} \). The claimed equality now follows from an earlier theorem about canceling bases.
Theorem. Let \( m \in \mathbb{N} \) be so that \( r \) is a primitive root modulo \( m \). Let \( a, b \in \mathbb{Z} \) be so that \((a, m) = (b, m) = 1\). Then

1. \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( \text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{\varphi(m)} \).
3. For all \( k \in \mathbb{N} \), we have \( \text{ind}_r(a^k) \equiv k \text{ind}_r(a) \pmod{\varphi(m)} \).

Proof.

1. \( r^{\varphi(m)} \equiv 1 \pmod{m} \), so, because no smaller positive power of \( r \) is congruent to 1, \( \text{ind}_r(1) \equiv 0 \pmod{\varphi(m)} \).
2. \( r^{\text{ind}_r(a) + \text{ind}_r(b)} = r^{\text{ind}_r(a)} r^{\text{ind}_r(b)} \equiv ab \equiv r^{\text{ind}_r(ab)} \pmod{m} \). The claimed equality now follows from an earlier theorem about canceling bases.
3. \( r^{k \text{ind}_r(a)} = (r^{\text{ind}_r(a)})^k \equiv a^k \equiv r^{\text{ind}_r(a^k)} \pmod{m} \). The claimed equality now follows from an earlier theorem about canceling bases.
Example.

\[ 3^x \equiv 8 \pmod{11} \]

\[ \text{ind}_2 (3^x) + 5 \text{ind}_2 (x) \equiv 3 \pmod{10} \]

\[ 5 \text{ind}_2 (x) \equiv 1 \pmod{2} \]

\[ x \equiv 2, 8, 10, 7, 6 \pmod{11} \]
Example. Solve $3x^5 \equiv 8 \pmod{11}$. 
Example. Solve $3x^5 \equiv 8 \pmod{11}$.

$$3x^5 \equiv 8 \pmod{11}$$
**Example.** Solve $3x^5 \equiv 8 \pmod{11}$.

$$3x^5 \equiv 8 \pmod{11}$$

$$\text{ind}_2\left(3x^5\right) \equiv \text{ind}_2(8) \pmod{\varphi(11)}$$
Example. Solve $3x^5 \equiv 8 \pmod{11}$.

\[
3x^5 \equiv 8 \pmod{11} \\
\text{ind}_2\left(3x^5\right) \equiv \text{ind}_2(8) \pmod{\varphi(11)} \\
\text{ind}_2(3) + 5\text{ind}_2(x) \equiv 3 \pmod{10}
\]
Example. Solve $3x^5 \equiv 8 \pmod{11}$.

$$3x^5 \equiv 8 \pmod{11}$$

$$\text{ind}_2 \left(3x^5\right) \equiv \text{ind}_2(8) \pmod{\varphi(11)}$$

$$\text{ind}_2(3) + 5\text{ind}_2(x) \equiv 3 \pmod{10}$$

$$8 + 5\text{ind}_2(x)$$
Example. Solve $3x^5 \equiv 8 \pmod{11}$.

\[
3x^5 \equiv 8 \pmod{11}
\]

\[
\text{ind}_2 \left( 3x^5 \right) \equiv \text{ind}_2(8) \pmod{\varphi(11)}
\]

\[
\text{ind}_2(3) + 5\text{ind}_2(x) \equiv 3 \pmod{10}
\]

\[
8 + 5\text{ind}_2(x) \equiv 3 \pmod{10}
\]
Example. Solve $3x^5 \equiv 8 \pmod{11}$.

$$3x^5 \equiv 8 \pmod{11}$$

$$\text{ind}_2 \left(3x^5\right) \equiv \text{ind}_2(8) \pmod{\varphi(11)}$$

$$\text{ind}_2(3) + 5\text{ind}_2(x) \equiv 3 \pmod{10}$$

$$8 + 5\text{ind}_2(x) \equiv 3 \pmod{10}$$

$$5\text{ind}_2(x)$$
Example. Solve $3x^5 \equiv 8 \pmod{11}$.

$$3x^5 \equiv 8 \pmod{11}$$

$$\text{ind}_2(3x^5) \equiv \text{ind}_2(8) \pmod{\varphi(11)}$$

$$\text{ind}_2(3) + 5\text{ind}_2(x) \equiv 3 \pmod{10}$$

$$8 + 5\text{ind}_2(x) \equiv 3 \pmod{10}$$

$$5\text{ind}_2(x) \equiv 5 \pmod{10}$$
Example. Solve $3x^5 \equiv 8 \pmod{11}$.

\[
3x^5 \equiv 8 \pmod{11} \\
\text{ind}_2 \left(3x^5\right) \equiv \text{ind}_2(8) \pmod{\varphi(11)} \\
\text{ind}_2(3) + 5\text{ind}_2(x) \equiv 3 \pmod{10} \\
8 + 5\text{ind}_2(x) \equiv 3 \pmod{10} \\
5\text{ind}_2(x) \equiv 5 \pmod{10} \\
\text{ind}_2(x)
\]
Example. Solve $3x^5 \equiv 8 \pmod{11}$.

\[
3x^5 \equiv 8 \pmod{11}
\]

\[
\text{ind}_2 \left( 3x^5 \right) \equiv \text{ind}_2(8) \pmod{\phi(11)}
\]

\[
\text{ind}_2(3) + 5\text{ind}_2(x) \equiv 3 \pmod{10}
\]

\[
8 + 5\text{ind}_2(x) \equiv 3 \pmod{10}
\]

\[
5\text{ind}_2(x) \equiv 5 \pmod{10}
\]

\[
\text{ind}_2(x) \equiv 1 \pmod{2}
\]
Example. Solve $3x^5 \equiv 8 \pmod{11}$.

\[
3x^5 \equiv 8 \pmod{11}
\]

\[
\text{ind}_2 \left( 3x^5 \right) \equiv \text{ind}_2(8) \pmod{\varphi(11)}
\]

\[
\text{ind}_2(3) + 5\text{ind}_2(x) \equiv 3 \pmod{10}
\]

\[
8 + 5\text{ind}_2(x) \equiv 3 \pmod{10}
\]

\[
5\text{ind}_2(x) \equiv 5 \pmod{10}
\]

\[
\text{ind}_2(x) \equiv 1 \pmod{2}
\]

\[
x \equiv 2, 2^3, 2^5, 2^7, 2^9
\]
Example. Solve $3x^5 \equiv 8 \pmod{11}$.

$$3x^5 \equiv 8 \pmod{11}$$

$$\text{ind}_2 \left( 3x^5 \right) \equiv \text{ind}_2(8) \pmod{\varphi(11)}$$

$$\text{ind}_2(3) + 5\text{ind}_2(x) \equiv 3 \pmod{10}$$

$$8 + 5\text{ind}_2(x) \equiv 3 \pmod{10}$$

$$5\text{ind}_2(x) \equiv 5 \pmod{10}$$

$$\text{ind}_2(x) \equiv 1 \pmod{2}$$

$$x \equiv 2, 2^3, 2^5, 2^7, 2^9 \equiv 2, 8, 10, 7, 6 \pmod{11}$$
Example. Solve $3x^5 \equiv 8 \pmod{11}$.

\[
3x^5 \equiv 8 \pmod{11} \\
\text{ind}_2 \left( 3x^5 \right) \equiv \text{ind}_2(8) \pmod{\varphi(11)} \\
\text{ind}_2(3) + 5\text{ind}_2(x) \equiv 3 \pmod{10} \\
8 + 5\text{ind}_2(x) \equiv 3 \pmod{10} \\
5\text{ind}_2(x) \equiv 5 \pmod{10} \\
\text{ind}_2(x) \equiv 1 \pmod{2} \\
x \equiv 2, 2^3, 2^5, 2^7, 2^9 \equiv 2, 8, 10, 7, 6 \pmod{11}
\]
Definition.
Definition. Let $m, k \in \mathbb{N}$ an let $a \in \mathbb{Z}$ be so that $(a, m) = 1$. Then $a$ is a $k^{th}$ power residue of $m$ iff there is an $x$ so that $x^k \equiv a \pmod{m}$. 
Theorem.
Theorem. Let $m, k \in \mathbb{N}$ and $a \in \mathbb{Z}$ be so that there is a primitive root modulo $m$ and so that $(a, m) = 1$. 
**Theorem.** Let \( m, k \in \mathbb{N} \) and \( a \in \mathbb{Z} \) be so that there is a primitive root modulo \( m \) and so that \((a,m) = 1\). Let \( d := (k, \varphi(m)) \).
Theorem. Let $m, k \in \mathbb{N}$ and $a \in \mathbb{Z}$ be so that there is a primitive root modulo $m$ and so that $(a, m) = 1$. Let $d := (k, \varphi(m))$. Then there is an $x$ with $x^k \equiv a \pmod{m}$ iff $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$. 
Theorem. Let \( m, k \in \mathbb{N} \) and \( a \in \mathbb{Z} \) be so that there is a primitive root modulo \( m \) and so that \( (a, m) = 1 \). Let \( d := (k, \varphi(m)) \). Then there is an \( x \) with \( x^k \equiv a \pmod{m} \) iff \( a^{\varphi(m)/d} \equiv 1 \pmod{m} \).

Moreover, if there are solutions to \( x^k \equiv a \pmod{m} \), then there are exactly \( d \) incongruent solutions modulo \( m \).
Theorem. Let $m, k \in \mathbb{N}$ and $a \in \mathbb{Z}$ be so that there is a primitive root modulo $m$ and so that $(a, m) = 1$. Let $d := (k, \varphi(m))$. Then there is an $x$ with $x^k \equiv a \pmod{m}$ iff $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$. Moreover, if there are solutions to $x^k \equiv a \pmod{m}$, then there are exactly $d$ incongruent solutions modulo $m$.

Proof.
**Theorem.** Let $m, k \in \mathbb{N}$ and $a \in \mathbb{Z}$ be so that there is a primitive root modulo $m$ and so that $(a, m) = 1$. Let $d := (k, \varphi(m))$. Then there is an $x$ with $x^k \equiv a \pmod{m}$ iff $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$.

Moreover, if there are solutions to $x^k \equiv a \pmod{m}$, then there are exactly $d$ incongruent solutions modulo $m$.

**Proof.** $x^k \equiv a \pmod{m}$
**Theorem.** Let \( m, k \in \mathbb{N} \) and \( a \in \mathbb{Z} \) be so that there is a primitive root modulo \( m \) and so that \( (a, m) = 1 \). Let \( d := (k, \varphi(m)) \). Then there is an \( x \) with \( x^k \equiv a \pmod{m} \) iff \( a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m} \). Moreover, if there are solutions to \( x^k \equiv a \pmod{m} \), then there are exactly \( d \) incongruent solutions modulo \( m \).

**Proof.** \( x^k \equiv a \pmod{m} \) is equivalent to

\[
k\operatorname{ind}_r(x) \equiv \operatorname{ind}_r(a) \pmod{\varphi(m)}
\]
Theorem. Let \( m, k \in \mathbb{N} \) and \( a \in \mathbb{Z} \) be so that there is a primitive root modulo \( m \) and so that \( (a,m) = 1 \). Let \( d := (k, \varphi(m)) \). Then there is an \( x \) with \( x^k \equiv a \pmod{m} \) iff \( a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m} \). Moreover, if there are solutions to \( x^k \equiv a \pmod{m} \), then there are exactly \( d \) incongruent solutions modulo \( m \).

Proof. \( x^k \equiv a \pmod{m} \) is equivalent to

\[
kind_r(x) \equiv \text{ind}_r(a) \pmod{\varphi(m)}
\]

and this linear congruence (for the “variable” \( \text{ind}_r(x) \)) has solutions iff \( d = (k, \varphi(m)) \) divides \( \text{ind}_r(a) \).
**Theorem.** Let $m, k \in \mathbb{N}$ and $a \in \mathbb{Z}$ be so that there is a primitive root modulo $m$ and so that $(a, m) = 1$. Let $d := (k, \varphi(m))$. Then there is an $x$ with $x^k \equiv a \pmod{m}$ iff $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$. Moreover, if there are solutions to $x^k \equiv a \pmod{m}$, then there are exactly $d$ incongruent solutions modulo $m$.

**Proof.** $x^k \equiv a \pmod{m}$ is equivalent to

$$k \text{ind}_r(x) \equiv \text{ind}_r(a) \pmod{\varphi(m)}$$

and this linear congruence (for the “variable” $\text{ind}_r(x)$) has solutions iff $d = (k, \varphi(m))$ divides $\text{ind}_r(a)$. Moreover, in this case there are $d$ incongruent solutions (indices) modulo $\varphi(m)$. 
**Theorem.** Let $m, k \in \mathbb{N}$ and $a \in \mathbb{Z}$ be so that there is a primitive root modulo $m$ and so that $(a, m) = 1$. Let $d := (k, \varphi(m))$. Then there is an $x$ with $x^k \equiv a \pmod{m}$ iff $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$. Moreover, if there are solutions to $x^k \equiv a \pmod{m}$, then there are exactly $d$ incongruent solutions modulo $m$.

**Proof.** $x^k \equiv a \pmod{m}$ is equivalent to

$$k \text{ind}_r(x) \equiv \text{ind}_r(a) \pmod{\varphi(m)}$$

and this linear congruence (for the “variable” $\text{ind}_r(x)$) has solutions iff $d = (k, \varphi(m))$ divides $\text{ind}_r(a)$. Moreover, in this case there are $d$ incongruent solutions (indices) modulo $\varphi(m)$, which translate into $d$ incongruent solutions $x$ modulo $m$. 
**Theorem.** Let $m, k \in \mathbb{N}$ and $a \in \mathbb{Z}$ be so that there is a primitive root modulo $m$ and so that $(a, m) = 1$. Let $d := (k, \varphi(m))$. Then there is an $x$ with $x^k \equiv a \pmod{m}$ iff $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$. Moreover, if there are solutions to $x^k \equiv a \pmod{m}$, then there are exactly $d$ incongruent solutions modulo $m$.

**Proof.** $x^k \equiv a \pmod{m}$ is equivalent to

$$k \text{ind}_r(x) \equiv \text{ind}_r(a) \pmod{\varphi(m)}$$

and this linear congruence (for the “variable” $\text{ind}_r(x)$) has solutions iff $d = (k, \varphi(m))$ divides $\text{ind}_r(a)$. Moreover, in this case there are $d$ incongruent solutions (indices) modulo $\varphi(m)$, which translate into $d$ incongruent solutions $x$ modulo $m$.

Now note that $d | \text{ind}_r(a)$
**Theorem.** Let $m, k \in \mathbb{N}$ and $a \in \mathbb{Z}$ be so that there is a primitive root modulo $m$ and so that $(a, m) = 1$. Let $d := (k, \varphi(m))$. Then there is an $x$ with $x^k \equiv a \pmod{m}$ iff $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$. Moreover, if there are solutions to $x^k \equiv a \pmod{m}$, then there are exactly $d$ incongruent solutions modulo $m$.

**Proof.** $x^k \equiv a \pmod{m}$ is equivalent to

$$k \text{ind}_r(x) \equiv \text{ind}_r(a) \pmod{\varphi(m)}$$

and this linear congruence (for the “variable” $\text{ind}_r(x)$) has solutions iff $d = (k, \varphi(m))$ divides $\text{ind}_r(a)$. Moreover, in this case there are $d$ incongruent solutions (indices) modulo $\varphi(m)$, which translate into $d$ incongruent solutions $x$ modulo $m$.

Now note that $d | \text{ind}_r(a)$ iff $\frac{\varphi(m)}{d} \text{ind}_r(a) \equiv 0 \pmod{\varphi(m)}$. 

Bernd Schröder

Louisiana Tech University, College of Engineering and Science

Discrete Logarithms and Rabin’s Probabilistic Primality Test
Theorem. Let \( m, k \in \mathbb{N} \) and \( a \in \mathbb{Z} \) be so that there is a primitive root modulo \( m \) and so that \( (a, m) = 1 \). Let \( d := (k, \varphi(m)) \). Then there is an \( x \) with \( x^k \equiv a \pmod{m} \) iff \( a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m} \).

Moreover, if there are solutions to \( x^k \equiv a \pmod{m} \), then there are exactly \( d \) incongruent solutions modulo \( m \).

Proof. \( x^k \equiv a \pmod{m} \) is equivalent to

\[
k \text{ind}_r(x) \equiv \text{ind}_r(a) \pmod{\varphi(m)}
\]

and this linear congruence (for the “variable” \( \text{ind}_r(x) \)) has solutions iff \( d = (k, \varphi(m)) \) divides \( \text{ind}_r(a) \). Moreover, in this case there are \( d \) incongruent solutions (indices) modulo \( \varphi(m) \), which translate into \( d \) incongruent solutions \( x \) modulo \( m \).

Now note that \( d|\text{ind}_r(a) \) iff \( \frac{\varphi(m)}{d} \text{ind}_r(a) \equiv 0 \pmod{\varphi(m)} \) iff

\[
a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}.
\]
Theorem. Let $m, k \in \mathbb{N}$ and $a \in \mathbb{Z}$ be so that there is a primitive root modulo $m$ and so that $(a, m) = 1$. Let $d := (k, \varphi(m))$. Then there is an $x$ with $x^k \equiv a \pmod{m}$ iff $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$. Moreover, if there are solutions to $x^k \equiv a \pmod{m}$, then there are exactly $d$ incongruent solutions modulo $m$.

Proof. $x^k \equiv a \pmod{m}$ is equivalent to

$$k \text{ind}_r(x) \equiv \text{ind}_r(a) \pmod{\varphi(m)}$$

and this linear congruence (for the “variable” $\text{ind}_r(x)$) has solutions iff $d = (k, \varphi(m))$ divides $\text{ind}_r(a)$. Moreover, in this case there are $d$ incongruent solutions (indices) modulo $\varphi(m)$, which translate into $d$ incongruent solutions $x$ modulo $m$. Now note that $d | \text{ind}_r(a)$ iff $\frac{\varphi(m)}{d} \text{ind}_r(a) \equiv 0 \pmod{\varphi(m)}$ iff $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$.
Example.

\[ x^3 \equiv 4 \pmod{9}, \text{ if possible.} \]

Proof.

\[ 4^\phi(9) (3, \phi(9)) = 4^6 (3, 6) = 4^2 \equiv 7 \pmod{9}, \] so there is no solution.
Example. Solve \( x^3 \equiv 4 \pmod{9} \), if possible.
Example. Solve \( x^3 \equiv 4 \pmod{9} \), if possible.

Proof.
Example. Solve $x^3 \equiv 4 \pmod{9}$, if possible.

Proof. $4 \equiv \frac{\varphi(9)}{(3, \varphi(9))}$
Example. Solve $x^3 \equiv 4 \pmod{9}$, if possible.

Proof. $4^\frac{\varphi(9)}{(3,\varphi(9))} = 4^\frac{6}{(3,6)}$
Example. Solve \( x^3 \equiv 4 \pmod{9} \), if possible.

Proof. \( 4^{\phi(9) \over (3, \phi(9))} = 4^{6 \over (3,6)} = 4^2 \)
Example. Solve $x^3 \equiv 4 \pmod{9}$, if possible.

Proof. $4^\left(\frac{\phi(9)}{\gcd(3,\phi(9))}\right) = 4^{\frac{6}{\gcd(3,6)}} = 4^2 \equiv 7 \pmod{9}$
Example. Solve $x^3 \equiv 4 \pmod{9}$, if possible.

Proof. $4^{\frac{\varphi(9)}{(3,\varphi(9))}} = 4^{\frac{6}{(3,6)}} = 4^2 \equiv 7 \pmod{9}$, so there is no solution.
**Example.** *Solve* \( x^3 \equiv 4 \pmod{9} \), *if possible.*

**Proof.** \( 4^{\frac{\varphi(9)}{(3,\varphi(9))}} = 4^{\frac{6}{(3,6)}} = 4^2 \equiv 7 \pmod{9} \), so there is no solution.
Lemma.
Lemma. Let $e, q, p \in \mathbb{N}$ be so that $p$ is an odd prime. Then the number of pairwise incongruent solutions of $x^q \equiv 1 \pmod{p^e}$ is $(q, p^{e-1}(p-1))$. 
**Lemma.** Let $e,q,p \in \mathbb{N}$ be so that $p$ is an odd prime. Then the number of pairwise incongruent solutions of $x^q \equiv 1 \pmod{p^e}$ is $\left( q, p^{e-1} (p-1) \right)$.

**Proof.**
Lemma. Let $e, q, p \in \mathbb{N}$ be so that $p$ is an odd prime. Then the number of pairwise incongruent solutions of $x^q \equiv 1 \pmod{p^e}$ is $(q, p^{e-1}(p-1))$.

Proof. Because $p^e$ is a prime power, there is a primitive root $r$ modulo $p^e$. 
Lemma. Let $e, q, p \in \mathbb{N}$ be so that $p$ is an odd prime. Then the number of pairwise incongruent solutions of $x^q \equiv 1 \pmod{p^e}$ is $(q, p^{e-1}(p - 1))$.

Proof. Because $p^e$ is a prime power, there is a primitive root $r$ modulo $p^e$. Hence we can apply the preceding theorem with $a = 1$. 
Lemma. Let $e, q, p \in \mathbb{N}$ be so that $p$ is an odd prime. Then the number of pairwise incongruent solutions of $x^q \equiv 1 \pmod{p^e}$ is $(q, p^{e-1}(p-1))$.

Proof. Because $p^e$ is a prime power, there is a primitive root $r$ modulo $p^e$. Hence we can apply the preceding theorem with $a = 1$. Because any power of 1 is 1, the condition in the theorem is satisfied and the congruence has a solution.
Lemma. Let $e, q, p \in \mathbb{N}$ be so that $p$ is an odd prime. Then the number of pairwise incongruent solutions of $x^q \equiv 1 \pmod{p^e}$ is $(q, p^{e-1}(p - 1))$.

Proof. Because $p^e$ is a prime power, there is a primitive root $r$ modulo $p^e$. Hence we can apply the preceding theorem with $a = 1$. Because any power of 1 is 1, the condition in the theorem is satisfied and the congruence has a solution. Because there are solutions to the congruence $x^q \equiv 1 \pmod{p^e}$
Lemma. Let $e, q, p \in \mathbb{N}$ be so that $p$ is an odd prime. Then the number of pairwise incongruent solutions of $x^q \equiv 1 \pmod{p^e}$ is $(q, p^{e-1}(p - 1))$.

Proof. Because $p^e$ is a prime power, there is a primitive root $r$ modulo $p^e$. Hence we can apply the preceding theorem with $a = 1$. Because any power of 1 is 1, the condition in the theorem is satisfied and the congruence has a solution. Because there are solutions to the congruence $x^q \equiv 1 \pmod{p^e}$, again by the previous theorem, there are $(q, \varphi(p^e)) = (q, p^{e-1}(p - 1))$ pairwise incongruent solutions.
Lemma. Let $e, q, p \in \mathbb{N}$ be so that $p$ is an odd prime. Then the number of pairwise incongruent solutions of $x^q \equiv 1 \pmod{p^e}$ is $(q, p^{e-1}(p - 1))$.

Proof. Because $p^e$ is a prime power, there is a primitive root $r$ modulo $p^e$. Hence we can apply the preceding theorem with $a = 1$. Because any power of 1 is 1, the condition in the theorem is satisfied and the congruence has a solution. Because there are solutions to the congruence $x^q \equiv 1 \pmod{p^e}$, again by the previous theorem, there are $(q, \varphi(p^e)) = (q, p^{e-1}(p - 1))$ pairwise incongruent solutions. ■
Lemma.

Let \( p, N, k, t, s, u \in \mathbb{N} \) be so that \( p \) is an odd prime with \( p - 1 = 2s \cdot t \) and \( t \) odd and so that \( N = 2k \cdot u \) with \( u \) odd.

Then the number of pairwise incongruent solutions of \( x \equiv -1 \pmod{p} \) is \( 2^k \cdot (t, u) \) when \( 0 \leq k \leq s - 1 \) and it is zero otherwise.

Proof. Let \( r \) be a primitive root modulo \( p \). Then \( x \equiv -1 \pmod{p} \) is equivalent to 

\[ N \cdot \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p - 1}{2} = 2^k \cdot u \pmod{\phi(p)} \]

This congruence has a solution iff \( (2^k \cdot u, 2^s \cdot t) = 2^k \cdot \min(k, s)(u, t) \) divides \( 2^{s - 1} \cdot t \).

Hence we only have solutions when \( 0 \leq k \leq s - 1 \).

In this case, we have \( (2^k \cdot u, 2^s \cdot t) = 2^k \cdot (u, t) \) incongruent solutions modulo \( p \).
Lemma. Let $p, N, k, t, s, u \in \mathbb{N}$ be so that

Let $p, N, k, t, s, u \in \mathbb{N}$ be so that
Lemma. Let $p, N, k, t, s, u \in \mathbb{N}$ be so that $p$ is an odd prime with $p - 1 = 2^s t$ and $t$ odd
Lemma. Let \( p, N, k, t, s, u \in \mathbb{N} \) be so that \( p \) is an odd prime with \( p - 1 = 2^s t \) and \( t \) odd and so that \( N = 2^k u \) with \( u \) odd.
Lemma. Let $p, N, k, t, s, u \in \mathbb{N}$ be so that $p$ is an odd prime with $p - 1 = 2^s t$ and $t$ odd and so that $N = 2^k u$ with $u$ odd. Then the number of pairwise incongruent solutions of $x^N \equiv -1 \pmod{p}$ is $2^k (t, u)$ when $0 \leq k \leq s - 1$. 
Lemma. Let $p, N, k, t, s, u \in \mathbb{N}$ be so that $p$ is an odd prime with $p - 1 = 2^s t$ and $t$ odd and so that $N = 2^k u$ with $u$ odd. Then the number of pairwise incongruent solutions of $x^N \equiv -1 \pmod{p}$ is $2^k (t, u)$ when $0 \leq k \leq s - 1$ and it is zero otherwise.
Lemma. Let \( p, N, k, t, s, u \in \mathbb{N} \) be so that \( p \) is an odd prime with \( p - 1 = 2^s t \) and \( t \) odd and so that \( N = 2^k u \) with \( u \) odd. Then the number of pairwise incongruent solutions of \( x^N \equiv -1 \pmod{p} \) is \( 2^k (t, u) \) when \( 0 \leq k \leq s - 1 \) and it is zero otherwise.

Proof.
Lemma. Let \( p, N, k, t, s, u \in \mathbb{N} \) be so that \( p \) is an odd prime with \( p - 1 = 2^s t \) and \( t \) odd and so that \( N = 2^k u \) with \( u \) odd. Then the number of pairwise incongruent solutions of \( x^N \equiv -1 \pmod{p} \) is \( 2^k (t, u) \) when \( 0 \leq k \leq s - 1 \) and it is zero otherwise.

Proof. Let \( r \) be a primitive root modulo \( p \).
Lemma. Let $p,N,k,t,s,u \in \mathbb{N}$ be so that $p$ is an odd prime with $p - 1 = 2^s t$ and $t$ odd and so that $N = 2^k u$ with $u$ odd. Then the number of pairwise incongruent solutions of $x^N \equiv -1 \pmod{p}$ is $2^k (t,u)$ when $0 \leq k \leq s - 1$ and it is zero otherwise.

Proof. Let $r$ be a primitive root modulo $p$. Then $x^N \equiv -1 \pmod{p}$
Lemma. Let $p, N, k, t, s, u \in \mathbb{N}$ be so that $p$ is an odd prime with $p - 1 = 2^s t$ and $t$ odd and so that $N = 2^k u$ with $u$ odd. Then the number of pairwise incongruent solutions of $x^N \equiv -1 \pmod{p}$ is $2^k (t, u)$ when $0 \leq k \leq s - 1$ and it is zero otherwise.

Proof. Let $r$ be a primitive root modulo $p$. Then $x^N \equiv -1 \pmod{p}$ is equivalent to

$$N \text{ind}_r(x) \equiv \text{ind}_r(-1)$$
Lemma. Let \( p, N, k, t, s, u \in \mathbb{N} \) be so that \( p \) is an odd prime with \( p - 1 = 2^s t \) and \( t \) odd and so that \( N = 2^k u \) with \( u \) odd. Then the number of pairwise incongruent solutions of \( x^N \equiv -1 \pmod{p} \) is \( 2^k (t, u) \) when \( 0 \leq k \leq s - 1 \) and it is zero otherwise.

Proof. Let \( r \) be a primitive root modulo \( p \). Then \( x^N \equiv -1 \pmod{p} \) is equivalent to

\[
N \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p - 1}{2}
\]
Lemma. Let $p, N, k, t, s, u \in \mathbb{N}$ be so that $p$ is an odd prime with $p - 1 = 2^s t$ and $t$ odd and so that $N = 2^k u$ with $u$ odd. Then the number of pairwise incongruent solutions of $x^N \equiv -1 \pmod{p}$ is $2^k (t, u)$ when $0 \leq k \leq s - 1$ and it is zero otherwise.

Proof. Let $r$ be a primitive root modulo $p$. Then $x^N \equiv -1 \pmod{p}$ is equivalent to

$$N \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p - 1}{2} \pmod{\varphi(p)}$$
Lemma. Let $p, N, k, t, s, u \in \mathbb{N}$ be so that $p$ is an odd prime with $p - 1 = 2^s t$ and $t$ odd and so that $N = 2^k u$ with $u$ odd. Then the number of pairwise incongruent solutions of $x^N \equiv -1 \pmod{p}$ is $2^k (t, u)$ when $0 \leq k \leq s - 1$ and it is zero otherwise.

Proof. Let $r$ be a primitive root modulo $p$. Then $x^N \equiv -1 \pmod{p}$ is equivalent to

$$N \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p-1}{2} \pmod{\varphi(p)}$$

$$2^k u \text{ind}_r(x)$$
Lemma. Let $p, N, k, t, s, u \in \mathbb{N}$ be so that $p$ is an odd prime with $p - 1 = 2^s t$ and $t$ odd and so that $N = 2^k u$ with $u$ odd. Then the number of pairwise incongruent solutions of $x^N \equiv -1 \pmod{p}$ is $2^k (t, u)$ when $0 \leq k \leq s - 1$ and it is zero otherwise.

Proof. Let $r$ be a primitive root modulo $p$. Then $x^N \equiv -1 \pmod{p}$ is equivalent to

$$N \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p-1}{2} \pmod{\varphi(p)}$$

$$2^k u \text{ind}_r(x) \equiv 2^{s-1} t$$
Lemma. Let $p, N, k, t, s, u \in \mathbb{N}$ be so that $p$ is an odd prime with $p - 1 = 2^s t$ and $t$ odd and so that $N = 2^k u$ with $u$ odd. Then the number of pairwise incongruent solutions of $x^N \equiv -1 \pmod{p}$ is $2^k (t, u)$ when $0 \leq k \leq s - 1$ and it is zero otherwise.

Proof. Let $r$ be a primitive root modulo $p$. Then $x^N \equiv -1 \pmod{p}$ is equivalent to

$$N \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p-1}{2} \pmod{\varphi(p)}$$

$$2^k u \text{ind}_r(x) \equiv 2^{s-1} t \pmod{2^s t}$$
Lemma. Let $p, N, k, t, s, u \in \mathbb{N}$ be so that $p$ is an odd prime with $p - 1 = 2^s t$ and $t$ odd and so that $N = 2^k u$ with $u$ odd. Then the number of pairwise incongruent solutions of $x^N \equiv -1 \pmod{p}$ is $2^k (t, u)$ when $0 \leq k \leq s - 1$ and it is zero otherwise.

Proof. Let $r$ be a primitive root modulo $p$. Then $x^N \equiv -1 \pmod{p}$ is equivalent to

$$N \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p - 1}{2} \pmod{\varphi(p)}$$

$$2^k u \text{ind}_r(x) \equiv 2^{s-1} t \pmod{2^s t}$$

This congruence has a solution iff $(2^k u, 2^s t)$
Lemma. Let \( p, N, k, t, s, u \in \mathbb{N} \) be so that \( p \) is an odd prime with \( p - 1 = 2^s t \) and \( t \) odd and so that \( N = 2^k u \) with \( u \) odd. Then the number of pairwise incongruent solutions of \( x^N \equiv -1 \pmod{p} \) is \( 2^k (t, u) \) when \( 0 \leq k \leq s - 1 \) and it is zero otherwise.

Proof. Let \( r \) be a primitive root modulo \( p \). Then \( x^N \equiv -1 \pmod{p} \) is equivalent to

\[
N \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p - 1}{2} \pmod{\varphi(p)}
\]

\[
2^k u \text{ind}_r(x) \equiv 2^{s-1} t \pmod{2^s t}
\]

This congruence has a solution iff \( (2^k u, 2^s t) = 2^{\min(k, s)} (u, t) \)
Lemma. Let $p, N, k, t, s, u \in \mathbb{N}$ be so that $p$ is an odd prime with $p - 1 = 2^s t$ and $t$ odd and so that $N = 2^k u$ with $u$ odd. Then the number of pairwise incongruent solutions of $x^N \equiv -1 \pmod{p}$ is $2^k (t, u)$ when $0 \leq k \leq s - 1$ and it is zero otherwise.

Proof. Let $r$ be a primitive root modulo $p$. Then $x^N \equiv -1 \pmod{p}$ is equivalent to

$$N \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p-1}{2} \pmod{\varphi(p)}$$

$$2^k u \text{ind}_r(x) \equiv 2^{s-1} t \pmod{2^s t}$$

This congruence has a solution iff $(2^k u, 2^s t) = 2^{\min(k, s)} (u, t)$ divides $2^{s-1} t$. 
Lemma. Let \( p, N, k, t, s, u \in \mathbb{N} \) be so that \( p \) is an odd prime with \( p - 1 = 2^s t \) and \( t \) odd and so that \( N = 2^k u \) with \( u \) odd. Then the number of pairwise incongruent solutions of \( x^N \equiv -1 \pmod{p} \) is \( 2^k (t, u) \) when \( 0 \leq k \leq s - 1 \) and it is zero otherwise.

Proof. Let \( r \) be a primitive root modulo \( p \). Then \( x^N \equiv -1 \pmod{p} \) is equivalent to

\[
N \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p - 1}{2} \pmod{\varphi(p)}
\]
\[
2^k u \text{ind}_r(x) \equiv 2^{s-1} t \pmod{2^s t}
\]

This congruence has a solution iff \((2^k u, 2^s t) = 2^{\min(k, s)} (u, t)\) divides \(2^{s-1} t\). Hence we only have solutions when \( 0 \leq k \leq s - 1 \).
**Lemma.** Let $p, N, k, t, s, u \in \mathbb{N}$ be so that $p$ is an odd prime with $p - 1 = 2^s t$ and $t$ odd and so that $N = 2^k u$ with $u$ odd. Then the number of pairwise incongruent solutions of $x^N \equiv -1 \pmod{p}$ is $2^k (t, u)$ when $0 \leq k \leq s - 1$ and it is zero otherwise.

**Proof.** Let $r$ be a primitive root modulo $p$. Then $x^N \equiv -1 \pmod{p}$ is equivalent to

$$N \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p - 1}{2} \pmod{\varphi(p)}$$

$$2^k u \text{ind}_r(x) \equiv 2^{s-1} t \pmod{2^s t}$$

This congruence has a solution iff $(2^k u, 2^s t) = 2^{\min(k, s)} (u, t)$ divides $2^{s-1} t$. Hence we only have solutions when $0 \leq k \leq s - 1$. In this case, we have $(2^k u, 2^s t)$.
Lemma. Let \( p, N, k, t, s, u \in \mathbb{N} \) be so that \( p \) is an odd prime with \( p - 1 = 2^s t \) and \( t \) odd and so that \( N = 2^k u \) with \( u \) odd. Then the number of pairwise incongruent solutions of \( x^N \equiv -1 \pmod{p} \) is \( 2^k (t,u) \) when \( 0 \leq k \leq s - 1 \) and it is zero otherwise.

Proof. Let \( r \) be a primitive root modulo \( p \). Then \( x^N \equiv -1 \pmod{p} \) is equivalent to
\[
N \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p - 1}{2} \pmod{\varphi(p)}
\]
\[
2^k u \text{ind}_r(x) \equiv 2^{s-1} t \pmod{2^s t}
\]
This congruence has a solution iff \( (2^k u, 2^s t) = 2^\min(k,s) (u, t) \) divides \( 2^{s-1} t \). Hence we only have solutions when \( 0 \leq k \leq s - 1 \). In this case, we have \( (2^k u, 2^s t) = 2^k (u, t) \)
Lemma. Let \( p, N, k, t, s, u \in \mathbb{N} \) be so that \( p \) is an odd prime with \( p - 1 = 2^s t \) and \( t \) odd and so that \( N = 2^k u \) with \( u \) odd. Then the number of pairwise incongruent solutions of \( x^N \equiv -1 \pmod{p} \) is \( 2^k (t, u) \) when \( 0 \leq k \leq s - 1 \) and it is zero otherwise.

Proof. Let \( r \) be a primitive root modulo \( p \). Then \( x^N \equiv -1 \pmod{p} \) is equivalent to

\[
N \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p - 1}{2} \pmod{\varphi(p)}
\]

\[
2^k u \text{ind}_r(x) \equiv 2^{s - 1} t \pmod{2^s t}
\]

This congruence has a solution iff \( (2^k u, 2^s t) = 2^{\min(k, s)} (u, t) \) divides \( 2^{s - 1} t \). Hence we only have solutions when \( 0 \leq k \leq s - 1 \). In this case, we have \( (2^k u, 2^s t) = 2^k (u, t) \) incongruent solutions modulo \( p \).
Lemma. Let $p, N, k, t, s, u \in \mathbb{N}$ be so that $p$ is an odd prime with $p - 1 = 2^s t$ and $t$ odd and so that $N = 2^k u$ with $u$ odd. Then the number of pairwise incongruent solutions of $x^N \equiv -1 \pmod{p}$ is $2^k (t, u)$ when $0 \leq k \leq s - 1$ and it is zero otherwise.

Proof. Let $r$ be a primitive root modulo $p$. Then $x^N \equiv -1 \pmod{p}$ is equivalent to

$$N \text{ind}_r(x) \equiv \text{ind}_r(-1) = \frac{p - 1}{2} \pmod{\varphi(p)}$$

$$2^k u \text{ind}_r(x) \equiv 2^{s-1} t \pmod{2^st}$$

This congruence has a solution iff $(2^k u, 2^st) = 2^{\min(k,s)} (u, t)$ divides $2^{s-1} t$. Hence we only have solutions when $0 \leq k \leq s - 1$. In this case, we have $(2^k u, 2^st) = 2^k (u, t)$ incongruent solutions modulo $p$. $\blacksquare$
Lemma.

Let $n = \prod r_j = 1 p_{e_j}$ and suppose that the congruence $f(x) \equiv 0 \pmod{p_{e_j}}$ has $k_j$ incongruent solutions modulo $p_{e_j}$. Then the congruence $f(x) \equiv 0 \pmod{n}$ has $\prod r_j = 1 k_j$ incongruent solutions modulo $n$. Moreover, every solution of $f(x) \equiv 0 \pmod{n}$ solves all the congruences $f(x) \equiv 0 \pmod{p_{e_j}}$, so every solution modulo $n$ is obtained from the solutions of the congruences modulo $p_{e_j}$.

Proof. Let $y_j$ be a solution of $f(x) \equiv 0 \pmod{p_{e_j}}$. Then, by the Chinese Remainder Theorem, the system of congruences $x \equiv y_j \pmod{p_{e_j}}$ has a unique solution $y$ modulo $n = \prod r_j = 1 p_{e_j}$. But then every $p_{e_j}$ divides $f(y)$, which means that $f(y) \equiv 0 \pmod{n}$. Because we can set up $\prod r_j = 1 k_j$ such congruences, we obtain that $f(x) \equiv 0 \pmod{n}$ has $\prod r_j = 1 k_j$ incongruent solutions modulo $n$. 
Lemma. Let \( n = \prod_{j=1}^{r} p_j^{e_j} \) and suppose that the congruence \( f(x) \equiv 0 \pmod{p_j^{e_j}} \) has \( k_j \) incongruent solutions modulo \( p_j^{e_j} \).
Lemma. Let $n = \prod_{j=1}^{r} p_j^{e_j}$ and suppose that the congruence $f(x) \equiv 0 \pmod{p_j^{e_j}}$ has $k_j$ incongruent solutions modulo $p_j^{e_j}$. Then the congruence $f(x) \equiv 0 \pmod{n}$ has $\prod_{j=1}^{r} k_j$ incongruent solutions modulo $n$. 
**Lemma.** Let $n = \prod_{j=1}^{r} p_j^{e_j}$ and suppose that the congruence $f(x) \equiv 0 \pmod{p_j^{e_j}}$ has $k_j$ incongruent solutions modulo $p_j^{e_j}$. Then the congruence $f(x) \equiv 0 \pmod{n}$ has $\prod_{j=1}^{r} k_j$ incongruent solutions modulo $n$. Moreover, every solution of $f(x) \equiv 0 \pmod{n}$ solves all the congruences $f(x) \equiv 0 \pmod{p_j^{e_j}}$. 
Lemma. Let \( n = \prod_{j=1}^{r} p_j^{e_j} \) and suppose that the congruence \( f(x) \equiv 0 \pmod{p_j^{e_j}} \) has \( k_j \) incongruent solutions modulo \( p_j^{e_j} \). Then the congruence \( f(x) \equiv 0 \pmod{n} \) has \( \prod_{j=1}^{r} k_j \) incongruent solutions modulo \( n \). Moreover, every solution of \( f(x) \equiv 0 \pmod{n} \) solves all the congruences \( f(x) \equiv 0 \pmod{p_j^{e_j}} \), so every solution modulo \( n \) is obtained from the solutions of the congruences modulo \( p_j^{e_j} \).
**Lemma.** Let \( n = \prod_{j=1}^{r} p_j^{e_j} \) and suppose that the congruence \( f(x) \equiv 0 \pmod{p_j^{e_j}} \) has \( k_j \) incongruent solutions modulo \( p_j^{e_j} \). Then the congruence \( f(x) \equiv 0 \pmod{n} \) has \( \prod_{j=1}^{r} k_j \) incongruent solutions modulo \( n \). Moreover, every solution of \( f(x) \equiv 0 \pmod{n} \) solves all the congruences \( f(x) \equiv 0 \pmod{p_j^{e_j}} \), so every solution modulo \( n \) is obtained from the solutions of the congruences modulo \( p_j^{e_j} \).

**Proof.**
Lemma. Let \( n = \prod_{j=1}^{r} p_j^{e_j} \) and suppose that the congruence \( f(x) \equiv 0 \pmod{p_j^{e_j}} \) has \( k_j \) incongruent solutions modulo \( p_j^{e_j} \). Then the congruence \( f(x) \equiv 0 \pmod{n} \) has \( \prod_{j=1}^{r} k_j \) incongruent solutions modulo \( n \). Moreover, every solution of \( f(x) \equiv 0 \pmod{n} \) solves all the congruences \( f(x) \equiv 0 \pmod{p_j^{e_j}} \), so every solution modulo \( n \) is obtained from the solutions of the congruences modulo \( p_j^{e_j} \).

Proof. Let \( y_j \) be a solution of \( f(x) \equiv 0 \pmod{p_j^{e_j}} \).
Lemma. Let \( n = \prod_{j=1}^{r} p_j^{e_j} \) and suppose that the congruence \( f(x) \equiv 0 \pmod{p_j^{e_j}} \) has \( k_j \) incongruent solutions modulo \( p_j^{e_j} \). Then the congruence \( f(x) \equiv 0 \pmod{n} \) has \( \prod_{j=1}^{r} k_j \) incongruent solutions modulo \( n \). Moreover, every solution of \( f(x) \equiv 0 \pmod{n} \) solves all the congruences \( f(x) \equiv 0 \pmod{p_j^{e_j}} \), so every solution modulo \( n \) is obtained from the solutions of the congruences modulo \( p_j^{e_j} \).

Proof. Let \( y_j \) be a solution of \( f(x) \equiv 0 \pmod{p_j^{e_j}} \). Then, by the Chinese Remainder Theorem, the system of congruences \( x \equiv y_j \pmod{p_j^{e_j}} \) has a unique solution \( y \) modulo \( n = \prod_{j=1}^{r} p_j^{e_j} \).
Lemma. Let \( n = \prod_{j=1}^{r} p_j^{e_j} \) and suppose that the congruence \( f(x) \equiv 0 \pmod{p_j^{e_j}} \) has \( k_j \) incongruent solutions modulo \( p_j^{e_j} \). Then the congruence \( f(x) \equiv 0 \pmod{n} \) has \( \prod_{j=1}^{r} k_j \) incongruent solutions modulo \( n \). Moreover, every solution of \( f(x) \equiv 0 \pmod{n} \) solves all the congruences \( f(x) \equiv 0 \pmod{p_j^{e_j}} \), so every solution modulo \( n \) is obtained from the solutions of the congruences modulo \( p_j^{e_j} \).

Proof. Let \( y_j \) be a solution of \( f(x) \equiv 0 \pmod{p_j^{e_j}} \). Then, by the Chinese Remainder Theorem, the system of congruences \( x \equiv y_j \pmod{p_j^{e_j}} \) has a unique solution \( y \) modulo \( n = \prod_{j=1}^{r} p_j^{e_j} \). But then every \( p_j^{e_j} \) divides \( f(y) \), which means that \( f(y) \equiv 0 \pmod{n} \).
Lemma. Let \( n = \prod_{j=1}^{r} p_j^{e_j} \) and suppose that the congruence \( f(x) \equiv 0 \pmod{p_j^{e_j}} \) has \( k_j \) incongruent solutions modulo \( p_j^{e_j} \). Then the congruence \( f(x) \equiv 0 \pmod{n} \) has \( \prod_{j=1}^{r} k_j \) incongruent solutions modulo \( n \). Moreover, every solution of \( f(x) \equiv 0 \pmod{n} \) solves all the congruences \( f(x) \equiv 0 \pmod{p_j^{e_j}} \), so every solution modulo \( n \) is obtained from the solutions of the congruences modulo \( p_j^{e_j} \).

Proof. Let \( y_j \) be a solution of \( f(x) \equiv 0 \pmod{p_j^{e_j}} \). Then, by the Chinese Remainder Theorem, the system of congruences \( x \equiv y_j \pmod{p_j^{e_j}} \) has a unique solution \( y \) modulo \( n = \prod_{j=1}^{r} p_j^{e_j} \). But then every \( p_j^{e_j} \) divides \( f(y) \), which means that \( f(y) \equiv 0 \pmod{n} \). Because we can set up \( \prod_{j=1}^{r} k_j \) such congruences, we obtain that \( f(x) \equiv 0 \pmod{n} \) has \( \prod_{j=1}^{r} k_j \) incongruent solutions modulo \( n \).
Lemma. Let \( n = \prod_{j=1}^{r} p_j^{e_j} \) and suppose that the congruence \( f(x) \equiv 0 \pmod{p_j^{e_j}} \) has \( k_j \) incongruent solutions modulo \( p_j^{e_j} \). Then the congruence \( f(x) \equiv 0 \pmod{n} \) has \( \prod_{j=1}^{r} k_j \) incongruent solutions modulo \( n \). Moreover, every solution of \( f(x) \equiv 0 \pmod{n} \) solves all the congruences \( f(x) \equiv 0 \pmod{p_j^{e_j}} \), so every solution modulo \( n \) is obtained from the solutions of the congruences modulo \( p_j^{e_j} \).

Proof.
Lemma. Let \( n = \prod_{j=1}^{r} p_j^{e_j} \) and suppose that the congruence \( f(x) \equiv 0 \pmod{p_j^{e_j}} \) has \( k_j \) incongruent solutions modulo \( p_j^{e_j} \). Then the congruence \( f(x) \equiv 0 \pmod{n} \) has \( \prod_{j=1}^{r} k_j \) incongruent solutions modulo \( n \). Moreover, every solution of \( f(x) \equiv 0 \pmod{n} \) solves all the congruences \( f(x) \equiv 0 \pmod{p_j^{e_j}} \), so every solution modulo \( n \) is obtained from the solutions of the congruences modulo \( p_j^{e_j} \).

Proof. The claim that every solution of \( f(x) \equiv 0 \pmod{n} \) is a solution of all \( f(x) \equiv 0 \pmod{p_j^{e_j}} \) is trivial
**Lemma.** Let \( n = \prod_{j=1}^{r} p_j^{e_j} \) and suppose that the congruence
\[ f(x) \equiv 0 \pmod{p_j^{e_j}} \]
has \( k_j \) incongruent solutions modulo \( p_j^{e_j} \).
Then the congruence \( f(x) \equiv 0 \pmod{n} \) has \( \prod_{j=1}^{r} k_j \) incongruent solutions modulo \( n \). Moreover, every solution of \( f(x) \equiv 0 \pmod{n} \) solves all the congruences \( f(x) \equiv 0 \pmod{p_j^{e_j}} \), so every solution modulo \( n \) is obtained from the solutions of the congruences modulo \( p_j^{e_j} \).

**Proof.** The claim that every solution of \( f(x) \equiv 0 \pmod{n} \) is a solution of all \( f(x) \equiv 0 \pmod{p_j^{e_j}} \) is trivial, but it does show that all solutions of \( f(x) \equiv 0 \pmod{n} \) are obtained as indicated above.
**Lemma.** Let $n = \prod_{j=1}^{r} p_j^{e_j}$ and suppose that the congruence $f(x) \equiv 0 \pmod{p_j^{e_j}}$ has $k_j$ incongruent solutions modulo $p_j^{e_j}$. Then the congruence $f(x) \equiv 0 \pmod{n}$ has $\prod_{j=1}^{r} k_j$ incongruent solutions modulo $n$. Moreover, every solution of $f(x) \equiv 0 \pmod{n}$ solves all the congruences $f(x) \equiv 0 \pmod{p_j^{e_j}}$, so every solution modulo $n$ is obtained from the solutions of the congruences modulo $p_j^{e_j}$.

**Proof.** The claim that every solution of $f(x) \equiv 0 \pmod{n}$ is a solution of all $f(x) \equiv 0 \pmod{p_j^{e_j}}$ is trivial, but it does show that all solutions of $f(x) \equiv 0 \pmod{n}$ are obtained as indicated above. Hence the congruence $f(x) \equiv 0 \pmod{n}$ has exactly $\prod_{j=1}^{r} k_j$ incongruent solutions modulo $n$. 
Lemma. Let \( n = \prod_{j=1}^{r} p_j^{e_j} \) and suppose that the congruence \( f(x) \equiv 0 \pmod{p_j^{e_j}} \) has \( k_j \) incongruent solutions modulo \( p_j^{e_j} \). Then the congruence \( f(x) \equiv 0 \pmod{n} \) has \( \prod_{j=1}^{r} k_j \) incongruent solutions modulo \( n \). Moreover, every solution of \( f(x) \equiv 0 \pmod{n} \) solves all the congruences \( f(x) \equiv 0 \pmod{p_j^{e_j}} \), so every solution modulo \( n \) is obtained from the solutions of the congruences modulo \( p_j^{e_j} \).

Proof. The claim that every solution of \( f(x) \equiv 0 \pmod{n} \) is a solution of all \( f(x) \equiv 0 \pmod{p_j^{e_j}} \) is trivial, but it does show that all solutions of \( f(x) \equiv 0 \pmod{n} \) are obtained as indicated above. Hence the congruence \( f(x) \equiv 0 \pmod{n} \) has exactly \( \prod_{j=1}^{r} k_j \) incongruent solutions modulo \( n \).
Miller’s Test

1. Suppose \( b^{n-1} \equiv 1 \) for \( (b, n) = 1 \).

2. Recall that, if \( n \) is prime, then \( b^n - 1 \equiv \pm 1 \pmod{n} \).

3. If \( n \) is an odd integer and \( n-1 = 2^s t \) with \( t \) odd, then we say that \( n \) passes Miller’s test for the base \( b \) iff \( b^t \equiv 1 \pmod{n} \) or \( b^{2j} \equiv -1 \pmod{n} \) for some \( j \in \{0, \ldots, s-1\} \).
Miller’s Test

1. Suppose $b^{n-1} \equiv 1$ for $(b, n) = 1$. 
Miller’s Test

1. Suppose $b^{n-1} \equiv 1$ for $(b, n) = 1$.
2. Recall that, if $n$ is prime, then $b^{n-1} \equiv \pm 1 \pmod{n}$.
Miller’s Test

1. Suppose $b^{n-1} \equiv 1$ for $(b, n) = 1$.
2. Recall that, if $n$ is prime, then $b^{n-1} \equiv \pm 1 \pmod{n}$.
3. If $n$ is an odd integer and $n - 1 = 2^st$ with $t$ odd, then we say that $n$ passes Miller’s test for the base $b$ iff $b^t \equiv 1 \pmod{n}$ or $b^{2jt} \equiv -1 \pmod{n}$ for some $j \in \{0, \ldots, s - 1\}$. 
Theorem.
Theorem. If $n$ is an odd composite integer, then $n$ passes Miller’s test for at most $\frac{n-1}{4}$ bases $b \in \{1, \ldots, n-1\}$. 
Theorem. *If* \( n \) *is an odd composite integer*, then \( n \) *passes Miller’s test for at most* \( \frac{n-1}{4} \) *bases* \( b \in \{1, \ldots, n-1\} \).

Proof.
Theorem. If $n$ is an odd composite integer, then $n$ passes Miller’s test for at most $\frac{n-1}{4}$ bases $b \in \{1,\ldots,n-1\}$.

Proof. So let $n = \prod_{j=1}^{r} p_j^{e_j}$ be a composite number that passes Miller’s test for a base $b$. 
Theorem. If $n$ is an odd composite integer, then $n$ passes Miller’s test for at most $\frac{n-1}{4}$ bases $b \in \{1,\ldots,n-1\}$.

Proof. So let $n = \prod_{j=1}^{r} p_j^{e_j}$ be a composite number that passes Miller’s test for a base $b$. This means that
**Theorem.** If \( n \) is an odd composite integer, then \( n \) passes Miller’s test for at most \( \frac{n-1}{4} \) bases \( b \in \{1, \ldots, n-1\} \).

**Proof.** So let \( n = \prod_{j=1}^{r} p_j^{e_j} \) be a composite number that passes Miller’s test for a base \( b \). This means that

1. \( b^{n-1} \equiv 1 \pmod{n} \)
**Theorem.** If \( n \) is an odd composite integer, then \( n \) passes Miller’s test for at most \( \frac{n-1}{4} \) bases \( b \in \{1, \ldots, n-1\} \).

**Proof.** So let \( n = \prod_{j=1}^{r} p_j^{e_j} \) be a composite number that passes Miller’s test for a base \( b \). This means that

1. \( b^{n-1} \equiv 1 \pmod{n} \)
2. \( n - 1 = 2^s t \) for an odd number \( t \) and \( s \geq 1 \) and

...
Theorem. If \( n \) is an odd composite integer, then \( n \) passes Miller’s test for at most \( \frac{n-1}{4} \) bases \( b \in \{1, \ldots, n-1\} \).

Proof. So let \( n = \prod_{j=1}^{r} p_j^{e_j} \) be a composite number that passes Miller’s test for a base \( b \). This means that

1. \( b^{n-1} \equiv 1 \pmod{n} \)
2. \( n - 1 = 2^s t \) for an odd number \( t \) and \( s \geq 1 \) and
3. \( b^t \equiv 1 \pmod{n} \)
Theorem. If \( n \) is an odd composite integer, then \( n \) passes Miller’s test for at most \( \frac{n-1}{4} \) bases \( b \in \{1, \ldots, n - 1\} \).

Proof. So let \( n = \prod_{j=1}^{r} p_j^{e_j} \) be a composite number that passes Miller’s test for a base \( b \). This means that

1. \( b^{n-1} \equiv 1 \pmod{n} \)
2. \( n - 1 = 2^s t \) for an odd number \( t \) and \( s \geq 1 \) and
3. \( b^t \equiv 1 \pmod{n} \) or \( b^{2^jt} \equiv -1 \pmod{n} \) for some \( j \in \{0, \ldots, s - 1\} \).
Theorem. If \( n \) is an odd composite integer, then \( n \) passes Miller’s test for at most \( \frac{n-1}{4} \) bases \( b \in \{1, \ldots, n-1\} \).

Proof. So let \( n = \prod_{j=1}^{r} p_j^{e_j} \) be a composite number that passes Miller’s test for a base \( b \). This means that

1. \( b^{n-1} \equiv 1 \pmod{n} \)
2. \( n-1 = 2^s t \) for an odd number \( t \) and \( s \geq 1 \) and
3. \( b^t \equiv 1 \pmod{n} \) or \( b^{2^jt} \equiv -1 \pmod{n} \) for some \( j \in \{0, \ldots, s-1\} \).

By earlier lemma, we know that \( x^{n-1} \equiv 1 \pmod{p_j^{e_j}} \) has \( \left(n-1, p_j^{e_j-1}(p_j-1)\right) \) incongruent solutions.
**Theorem.** If \( n \) is an odd composite integer, then \( n \) passes Miller’s test for at most \( \frac{n-1}{4} \) bases \( b \in \{1, \ldots, n-1\} \).

**Proof.** So let \( n = \prod_{j=1}^{r} p_j^{e_j} \) be a composite number that passes Miller’s test for a base \( b \). This means that

1. \( b^{n-1} \equiv 1 \pmod{n} \)
2. \( n - 1 = 2^s t \) for an odd number \( t \) and \( s \geq 1 \) and
3. \( b^t \equiv 1 \pmod{n} \) or \( b^{2^jt} \equiv -1 \pmod{n} \) for some \( j \in \{0, \ldots, s - 1\} \).

By earlier lemma, we know that \( x^{n-1} \equiv 1 \pmod{p_j^{e_j}} \) has \( \left(n - 1, p_j^{e_j-1}(p_j - 1)\right) \) incongruent solutions. Note that

\[
\left(n - 1, p_j^{e_j-1}(p_j - 1)\right) = (n - 1, p_j - 1).
\]
Theorem. If $n$ is an odd composite integer, then $n$ passes Miller’s test for at most $\frac{n-1}{4}$ bases $b \in \{1, \ldots, n-1\}$.

Proof. So let $n = \prod_{j=1}^{r} p_j^{e_j}$ be a composite number that passes Miller’s test for a base $b$. This means that

1. $b^{n-1} \equiv 1 \pmod{n}$
2. $n - 1 = 2^s t$ for an odd number $t$ and $s \geq 1$ and
3. $b^t \equiv 1 \pmod{n}$ or $b^{2^j t} \equiv -1 \pmod{n}$ for some $j \in \{0, \ldots, s-1\}$.

By earlier lemma, we know that $x^{n-1} \equiv 1 \pmod{p_j^{e_j}}$ has

$$\left(n - 1, p_j^{e_j-1}(p_j - 1)\right)$$

incongruent solutions. Note that

$$\left(n - 1, p_j^{e_j-1}(p_j - 1)\right) = (n - 1, p_j - 1).$$

Hence, by the Chinese Remainder Theorem, $x^{n-1} \equiv 1 \pmod{n}$ has exactly

$$\prod_{j=1}^{r} (n - 1, p_j - 1)$$
incongruent solutions.
Theorem. If $n$ is an odd composite integer, then $n$ passes Miller’s test for at most $\frac{n-1}{4}$ bases $b \in \{1, \ldots, n-1\}$.

Proof.
**Theorem.** If $n$ is an odd composite integer, then $n$ passes Miller’s test for at most $\frac{n-1}{4}$ bases $b \in \{1, \ldots, n-1\}$.

**Proof.** We will consider three cases for $n = \prod_{j=1}^{r} p_j^{e_j}$. 
**Theorem.** If $n$ is an odd composite integer, then $n$ passes Miller’s test for at most $\frac{n-1}{4}$ bases $b \in \{1, \ldots, n-1\}$.

**Proof.** We will consider three cases for $n = \prod_{j=1}^{r} p_j^{e_j}$.

1. One $e_k$ is $\geq 2$. 
**Theorem.** If $n$ is an odd composite integer, then $n$ passes Miller’s test for at most $\frac{n-1}{4}$ bases $b \in \{1, \ldots, n-1\}$.

**Proof.** We will consider three cases for $n = \prod_{j=1}^{r} p_j^{e_j}$.

1. One $e_k$ is $\geq 2$.
2. All $e_k$ are equal to 1 and $r \geq 3$. 
**Theorem.** If $n$ is an odd composite integer, then $n$ passes Miller’s test for at most $\frac{n-1}{4}$ bases $b \in \{1, \ldots, n-1\}$.

**Proof.** We will consider three cases for $n = \prod_{j=1}^{r} p_j^{e_j}$.

1. One $e_k$ is $\geq 2$.
2. All $e_k$ are equal to 1 and $r \geq 3$.
3. All $e_k$ are equal to 1 and $r = 2$. 
Proof (case 1).

There is a \( k \) so that 
\[
e^k \geq 2.
\]

\[
\prod_{j=1}^{n-1} (p_j - 1) \leq \prod_{j=1}^{n-1} (\prod_{j \neq k} p_j) p_k - 1 
\leq 2^{9n} p^k - 1 \leq n - 1
\]
where we assume \( n \geq 9 \) in the last step.

Hence there are at most \( n - 1 \) bases \( b \) for which \( n \) is a strong pseudoprime to the base \( b \).
Proof (case 1).
Proof (case 1). There is a $k$ so that $e_k \geq 2$. 
**Proof (case 1).** There is a $k$ so that $e_k \geq 2$.

\[
\prod_{j=1}^{r} (n - 1, p_j - 1)
\]
Proof (case 1). There is a $k$ so that $e_k \geq 2$.

$$\prod_{j=1}^{r} (n-1, p_j-1) \leq \prod_{j=1}^{r} (p_j - 1)$$

where we assume $n \geq 9$ in the last step. Hence there are at most $n - 1$ bases $b$ for which $n$ is a strong pseudoprime to the base $b$. 
**Proof (case 1).** There is a \( k \) so that \( e_k \geq 2 \).

\[
\prod_{j=1}^{r} (n - 1, p_j - 1) \leq \prod_{j=1}^{r} (p_j - 1)
\]

\[
\leq \left( \prod_{j \neq k} p_j \right) \frac{p_k - 1}{p_k^{e_k}} p_k^{e_k}
\]

where we assume \( n \geq 9 \) in the last step.

Hence there are at most \( n - 1 \) bases \( b \) for which \( n \) is a strong pseudoprime to the base \( b \).
Proof (case 1). There is a \( k \) so that \( e_k \geq 2 \).

\[
\prod_{j=1}^{r} (n-1, p_j-1) \leq \prod_{j=1}^{r} (p_j-1)
\]

\[
\leq \left( \prod_{j \neq k} p_j \right) \frac{p_k - 1}{p_k^{e_k}} p_k^{e_k}
\]

\[
\leq \left( \prod_{j \neq k} p_j \right) \frac{2}{9} p_k^{e_k}
\]
Proof (case 1). There is a $k$ so that $e_k \geq 2$.

$$
\prod_{j=1}^{r} (n - 1, p_j - 1) \leq \prod_{j=1}^{r} (p_j - 1)
$$

$$
\leq \left( \prod_{j \neq k} p_j \right) \frac{p_k - 1}{p_k} p_k^{e_k}
$$

$$
\leq \left( \prod_{j \neq k} p_j \right) \frac{2}{9} p_k^{e_k} \leq \frac{2}{9} n
$$
Proof (case 1). There is a $k$ so that $e_k \geq 2$.

$$\prod_{j=1}^{r} (n-1, p_j - 1) \leq \prod_{j=1}^{r} (p_j - 1)$$

$$\leq \left( \prod_{j \neq k} p_j \right) \frac{p_k - 1}{p_k^{e_k}} p_k^{e_k}$$

$$\leq \left( \prod_{j \neq k} p_j \right) \frac{2}{9} p_k^{e_k} \leq \frac{2}{9} n \leq \frac{n - 1}{4}$$
**Proof (case 1).** There is a $k$ so that $e_k \geq 2$.

\[
\prod_{j=1}^{r} (n - 1, p_j - 1) \leq \prod_{j=1}^{r} (p_j - 1)
\]

\[
\leq \left( \prod_{j \neq k} p_j \right) \frac{p_k - 1}{p_k^{e_k}} p_k^{e_k}
\]

\[
\leq \left( \prod_{j \neq k} p_j \right) \frac{2}{9} p_k^{e_k} \leq \frac{2}{9} n \leq \frac{n - 1}{4}
\]

where we assume $n \geq 9$ in the last step.
Proof (case 1). There is a $k$ so that $e_k \geq 2$.

$$\prod_{j=1}^{r} (n-1, p_j - 1) \leq \prod_{j=1}^{r} (p_j - 1)$$

$$\leq \left( \prod_{j \neq k} p_j \right) \frac{p_k - 1}{p_k^{e_k}} p_k^{e_k}$$

$$\leq \left( \prod_{j \neq k} p_j \right) \frac{2}{9} p_k^{e_k} \leq \frac{2}{9} n \leq \frac{n - 1}{4}$$

where we assume $n \geq 9$ in the last step. Hence there are at most $\frac{n-1}{4}$ bases $b$ for which $n$ is a strong pseudoprime to the base $b$. 
Proof (case 2). Let $s_j, t_j \in \mathbb{N}$ be so that $p_j - 1 = 2^{s_j} t_j$ with $t_j$ odd and assume without loss of generality that $s_1 \leq s_2 \leq \cdots \leq s_r$.

Then $(n - 1, p_j - 1) = 2^{\min(s, s_j)} (t, t_j)$.

Now, by earlier lemmas, $x^t \equiv 1 \pmod{p_j}$ has $(t, t_j)$ incongruent solutions and $x^{2^k t} \equiv -1 \pmod{p_j}$ has $2^{k (t, t_j)}$ incongruent solutions for $0 \leq k \leq s_j - 1$ and none otherwise.

Hence (Chinese Remainder Theorem) there are $\prod r_j = 1$ $(t, t_j)$ incongruent solutions of $x^t \equiv 1 \pmod{n}$ and there are $\prod r_j = 1 (2^k (t, t_j))$ incongruent solutions of $x^{2^k t} \equiv -1 \pmod{n}$ for $0 \leq k \leq s_1 - 1$ and none otherwise.

So the number of integers $b$ for which $n$ is a strong pseudoprime to base $b$ is...
Proof (case 2).
Proof (case 2). \( n = \prod_{j=1}^{r} p_j \)
Proof (case 2). $n = \prod_{j=1}^{r} p_j, r \geq 3$. 
Proof (case 2). \( n = \prod_{j=1}^{r} p_j, \ r \geq 3 \). Let \( s_j, t_j \in \mathbb{N} \) be so that 
\[ p_j - 1 = 2^{s_j} t_j \] 
with \( t_j \) odd.
**Proof (case 2).** \( n = \prod_{j=1}^{r} p_j, \ r \geq 3. \) Let \( s_j, t_j \in \mathbb{N} \) be so that 
\( p_j - 1 = 2^{s_j} t_j \) with \( t_j \) odd and assume without loss of generality 
that \( s_1 \leq s_2 \leq \cdots \leq s_r. \)
Proof (case 2). $n = \prod_{j=1}^{r} p_j$, $r \geq 3$. Let $s_j, t_j \in \mathbb{N}$ be so that $p_j - 1 = 2^{s_j} t_j$ with $t_j$ odd and assume without loss of generality that $s_1 \leq s_2 \leq \cdots \leq s_r$. Then $(n - 1, p_j - 1) = 2^{\min(s,s_j)}(t, t_j)$. 

"Index Arithmetic Power Residues Rabin’s Probabilistic Primality Test More Primality Tests"

Bernd Schröder Louisiana Tech University, College of Engineering and Science

Discrete Logarithms and Rabin’s Probabilistic Primality Test
**Proof (case 2).** $n = \prod_{j=1}^{r} p_j$, $r \geq 3$. Let $s_j, t_j \in \mathbb{N}$ be so that $p_j - 1 = 2^{s_j}t_j$ with $t_j$ odd and assume without loss of generality that $s_1 \leq s_2 \leq \cdots \leq s_r$. Then $(n - 1, p_j - 1) = 2^{\min(s,s_j)}(t, t_j)$. Now, by earlier lemmas, $x^t \equiv 1 \pmod{p_j}$ has $(t, t_j)$ incongruent solutions
Proof (case 2). \( n = \prod_{j=1}^{r} p_j, \quad r \geq 3 \). Let \( s_j, t_j \in \mathbb{N} \) be so that
\( p_j - 1 = 2^{s_j} t_j \) with \( t_j \) odd and assume without loss of generality that \( s_1 \leq s_2 \leq \cdots \leq s_r \). Then \( (n - 1, p_j - 1) = 2^{\min(s, s_j)}(t, t_j) \).
Now, by earlier lemmas, \( x^t \equiv 1 \pmod{p_j} \) has \((t, t_j)\) incongruent solutions and \( x^{2^k t} \equiv -1 \pmod{p_j} \) has \( 2^k(t, t_j) \) incongruent solutions for \( 0 \leq k \leq s_j - 1 \) and no solutions otherwise.
**Proof (case 2).** $n = \prod_{j=1}^{r} p_j$, $r \geq 3$. Let $s_j, t_j \in \mathbb{N}$ be so that $p_j - 1 = 2^{s_j} t_j$ with $t_j$ odd and assume without loss of generality that $s_1 \leq s_2 \leq \cdots \leq s_r$. Then $(n - 1, p_j - 1) = 2^{\min(s, s_j)} (t, t_j)$.

Now, by earlier lemmas, $x^t \equiv 1 \pmod{p_j}$ has $(t, t_j)$ incongruent solutions and $x^{2^k t} \equiv -1 \pmod{p_j}$ has $2^k (t, t_j)$ incongruent solutions for $0 \leq k \leq s_j - 1$ and no solutions otherwise. Hence (Chinese Remainder Theorem) there are $\prod_{j=1}^{r} (t, t_j)$ incongruent solutions of $x^t \equiv 1 \pmod{n}$.
Proof (case 2). \( n = \prod_{j=1}^{r} p_j, \ r \geq 3. \) Let \( s_j, t_j \in \mathbb{N} \) be so that \( p_j - 1 = 2^{s_j} t_j \) with \( t_j \) odd and assume without loss of generality that \( s_1 \leq s_2 \leq \cdots \leq s_r. \) Then \( (n - 1, p_j - 1) = 2^{\min(s,s_j)}(t, t_j). \) Now, by earlier lemmas, \( x^t \equiv 1 \pmod{p_j} \) has \((t, t_j)\) incongruent solutions and \( x^{2k t} \equiv -1 \pmod{p_j} \) has \( 2^k(t, t_j) \) incongruent solutions for \( 0 \leq k \leq s_j - 1 \) and no solutions otherwise. Hence (Chinese Remainder Theorem) there are \( \prod_{j=1}^{r} (t, t_j) \) incongruent solutions of \( x^t \equiv 1 \pmod{n} \) and there are \( \prod_{j=1}^{r} (2^k(t, t_j)) \) incongruent solutions of \( x^{2k t} \equiv -1 \pmod{n} \) for \( 0 \leq k \leq s_1 - 1 \) and none otherwise.
Proof (case 2). \( n = \prod_{j=1}^{r} p_j, \ r \geq 3 \). Let \( s_j, t_j \in \mathbb{N} \) be so that \( p_j - 1 = 2^{s_j} t_j \) with \( t_j \) odd and assume without loss of generality that \( s_1 \leq s_2 \leq \cdots \leq s_r \). Then \( (n - 1, p_j - 1) = 2^{\min(s,s_j)} (t_j) \). Now, by earlier lemmas, \( x^t \equiv 1 \pmod{p_j} \) has \((t,t_j)\) incongruent solutions and \( x^{2^k t} \equiv -1 \pmod{p_j} \) has \( 2^k (t,t_j) \) incongruent solutions for \( 0 \leq k \leq s_j - 1 \) and no solutions otherwise. Hence (Chinese Remainder Theorem) there are \( \prod_{j=1}^{r} (t,t_j) \) incongruent solutions of \( x^t \equiv 1 \pmod{n} \) and there are \( \prod_{j=1}^{r} (2^k (t,t_j)) \) incongruent solutions of \( x^{2^k t} \equiv -1 \pmod{n} \) for \( 0 \leq k \leq s_1 - 1 \) and none otherwise. So the number of integers \( b \) for which \( n \) is a strong pseudoprime to base \( b \) is
Proof (case 2).
\[
r \prod_{j} = 1^{(t, t_{j})} + s_{1} - 1 \sum_{k=0}^{r \prod_{j} = 1^{(t, t_{j})}} 2^{kr}(t, t_{j}) = r \prod_{j} = 1^{(t, t_{j})}(1 + s_{1} - 1 \sum_{k=0}^{r \prod_{j} = 1^{(t, t_{j})}} 2^{kr}) \leq \prod_{r \prod_{j} = 1^{(t, t_{j})}}^{2}s_{j}t_{j}^{2} \sum_{r \prod_{j} = 1^{(t, t_{j})}}^{s_{j}}(1 + 2^{rs_{1}} - 1 2^{r - 1} 2^{rs_{1}}) \leq \prod_{r \prod_{j} = 1^{(t, t_{j})}}^{(n - 1)}(p_{j} - 1) 2^{rs_{1}}(1 + 2^{rs_{1}} - 1 2^{r - 1} 2^{rs_{1}}) \leq \varphi(n)\left(1 + 2^{rs_{1}} - 1 2^{r - 1} 2^{rs_{1}}\right) \leq \left(n - 1\right)\left(1 + 2^{rs_{1}} - 1 2^{r - 1} 2^{rs_{1}}\right) \leq n - 1\right)\]
Proof (case 2).

\[
\prod_{j=1}^{r}(t, t_j) + \sum_{k=0}^{s_1-1} \prod_{j=1}^{r} \left( 2^k(t, t_j) \right)
\]
Proof (case 2).

\[
\prod_{j=1}^{r} (t, t_j) + \sum_{k=0}^{s_1-1} \prod_{j=1}^{r} \left( 2^k (t, t_j) \right)
\]

\[
= \prod_{j=1}^{r} (t, t_j) \left( 1 + \sum_{k=0}^{s_1-1} 2^{kr} \right)
\]
Proof (case 2).

\[
\prod_{j=1}^{r} (t, t_j) + \sum_{k=0}^{s_1-1} \prod_{j=1}^{r} \left( 2^k (t, t_j) \right)
\]

\[
= \prod_{j=1}^{r} (t, t_j) \left( 1 + \sum_{k=0}^{s_1-1} 2^{kr} \right) = \prod_{j=1}^{r} (t, t_j) \left( 1 + \frac{2^{rs_1} - 1}{2^r - 1} \right)
\]
Proof (case 2).

\[
\prod_{j=1}^{r} (t, t_j) + \sum_{k=0}^{s_1-1} \prod_{j=1}^{r} (2^k (t, t_j)) \\
= \prod_{j=1}^{r} (t, t_j) \left( 1 + \sum_{k=0}^{s_1-1} 2^{kr} \right) = \prod_{j=1}^{r} (t, t_j) \left( 1 + \frac{2^{rs_1} - 1}{2^r - 1} \right) \\
\leq \frac{\prod_{j=1}^{r} 2^{s_j t_j}}{2 \sum_{j=1}^{r} s_j} \left( 1 + \frac{2^{rs_1} - 1}{2^r - 1} \right)
\]
Proof (case 2).

\[
\prod_{j=1}^{r}(t, t_j) + \sum_{k=0}^{s_1-1} \prod_{j=1}^{r} \left(2^k(t, t_j)\right)
\]

\[
= \prod_{j=1}^{r}(t, t_j) \left(1 + \sum_{k=0}^{s_1-1} 2^{kr}\right) = \prod_{j=1}^{r}(t, t_j) \left(1 + \frac{2^{rs_1} - 1}{2^r - 1}\right)
\]

\[
\leq \frac{\prod_{j=1}^{r}2^{s_j}t_j}{2^{\sum_{j=1}^{r}s_j}} \left(1 + \frac{2^{rs_1} - 1}{2^r - 1}\right) \leq \frac{\prod_{j=1}^{r}(p_j - 1)}{2^{rs_1}} \left(1 + \frac{2^{rs_1} - 1}{2^r - 1}\right)
\]
Proof (case 2).

\[ \prod_{j=1}^{r} (t, t_j) + \sum_{k=0}^{s_1-1} \prod_{j=1}^{r} \left( 2^k (t, t_j) \right) \]

\[ = \prod_{j=1}^{r} (t, t_j) \left( 1 + \sum_{k=0}^{s_1-1} 2^{kr} \right) = \prod_{j=1}^{r} (t, t_j) \left( 1 + \frac{2^{rs_1} - 1}{2r - 1} \right) \]

\[ \leq \frac{\prod_{j=1}^{r} 2^{s_j} t_j}{2 \sum_{j=1}^{r} s_j} \left( 1 + \frac{2^{rs_1} - 1}{2r - 1} \right) \leq \frac{\prod_{j=1}^{r} (p_j - 1)}{2^{rs_1}} \left( 1 + \frac{2^{rs_1} - 1}{2r - 1} \right) \]

\[ \leq \varphi(n) \left( \frac{1}{2^{rs_1}} + \frac{2^{rs_1} - 1}{(2r - 1) 2^{rs_1}} \right) \]

Bernd Schröder

Bernd Schröder
Louisiana Tech University, College of Engineering and Science

Discrete Logarithms and Rabin’s Probabilistic Primality Test
Proof (case 2).

\[
\prod_{j=1}^{r} (t, t_j) + \sum_{j=1}^{r} \prod_{k=0}^{s_1-1} \left( 2^k (t, t_j) \right)
\]

\[
= \prod_{j=1}^{r} (t, t_j) \left( 1 + \sum_{k=0}^{s_1-1} 2^{kr} \right) = \prod_{j=1}^{r} (t, t_j) \left( 1 + \frac{2^{rs_1} - 1}{2^r - 1} \right)
\]

\[
\leq \frac{\prod_{j=1}^{r} 2^{s_j} t_j}{2^{\sum_{j=1}^{r} s_j}} \left( 1 + \frac{2^{rs_1} - 1}{2^r - 1} \right) \leq \frac{\prod_{j=1}^{r} (p_j - 1)}{2^{rs_1}} \left( 1 + \frac{2^{rs_1} - 1}{2^r - 1} \right)
\]

\[
\leq \varphi(n) \left( \frac{1}{2^{rs_1}} + \frac{2^{rs_1} - 1}{(2^r - 1) 2^{rs_1}} \right) \leq \varphi(n) \left( \frac{1}{2^{rs_1}} + \frac{1}{2^r - 1} - \frac{1}{(2^r - 1) 2^{rs_1}} \right)
\]
Proof (case 2).

\[
\prod_{j=1}^{r} (t, t_j) + \sum_{k=0}^{s_1-1} \prod_{j=1}^{r} \left( 2^k (t, t_j) \right)
\]

\[
= \prod_{j=1}^{r} (t, t_j) \left( 1 + \sum_{k=0}^{s_1-1} 2^{kr} \right) = \prod_{j=1}^{r} (t, t_j) \left( 1 + \frac{2^{rs_1} - 1}{2^r - 1} \right)
\]

\[
\leq \frac{\prod_{j=1}^{r} 2^{sj} t_j}{2^r \sum_{j=1}^{r} s_j} \left( 1 + \frac{2^{rs_1} - 1}{2^r - 1} \right) \leq \frac{\prod_{j=1}^{r} (p_j - 1)}{2^{rs_1}} \left( 1 + \frac{2^{rs_1} - 1}{2^r - 1} \right)
\]

\[
\leq \varphi(n) \left( \frac{1}{2^{rs_1}} + \frac{2^{rs_1} - 1}{(2^r - 1) 2^{rs_1}} \right) \leq \varphi(n) \left( \frac{1}{2^{rs_1}} + \frac{1}{2^r - 1} - \frac{1}{(2^r - 1) 2^{rs_1}} \right)
\]

\[
\leq (n-1) \left( \frac{1}{2^r - 1} + \frac{2^r - 2}{(2^r - 1) 2^{rs_1}} \right)
\]
Proof (case 2).

\[
\prod_{j=1}^{r}(t, t_j) + \sum_{k=0}^{s_1-1} \prod_{j=1}^{r} \left( 2^k(t, t_j) \right)
\]

\[
= \prod_{j=1}^{r}(t, t_j) \left( 1 + \sum_{k=0}^{s_1-1} 2^{kr} \right) = \prod_{j=1}^{r}(t, t_j) \left( 1 + \frac{2^{rs_1} - 1}{2^r - 1} \right)
\]

\[
\leq \frac{\prod_{j=1}^{r} 2^{s_j} t_j}{2^{\sum_{j=1}^{r} s_j}} \left( 1 + \frac{2^{rs_1} - 1}{2^r - 1} \right) \leq \frac{\prod_{j=1}^{r} (p_j - 1)}{2^{rs_1}} \left( 1 + \frac{2^{rs_1} - 1}{2^r - 1} \right)
\]

\[
\leq \phi(n) \left( \frac{1}{2^{rs_1}} + \frac{2^{rs_1} - 1}{(2^r - 1)2^{rs_1}} \right) \leq \phi(n) \left( \frac{1}{2^{rs_1}} + \frac{1}{2^r - 1} - \frac{1}{(2^r - 1)2^{rs_1}} \right)
\]

\[
\leq (n-1) \left( \frac{1}{2^r - 1} + \frac{2^r - 2}{(2^r - 1)2^{rs_1}} \right) \leq (n-1) \frac{2}{2^r - 1}
\]
Proof (case 2).

\[
\prod_{j=1}^{r}(t, t_j) + \sum_{k=0}^{s_1-1} \prod_{j=1}^{r}(2^k(t, t_j))
\]

\[
= \prod_{j=1}^{r}(t, t_j) \left(1 + \sum_{k=0}^{s_1-1} 2^{kr}\right) = \prod_{j=1}^{r}(t, t_j) \left(1 + \frac{2^{rs_1} - 1}{2^r - 1}\right)
\]

\[
\leq \frac{\prod_{j=1}^{r} 2^{s_j} t_j}{2^n} \left(1 + \frac{2^{rs_1} - 1}{2^r - 1}\right) \leq \frac{\prod_{j=1}^{r} p_j - 1}{2^{rs_1}} \left(1 + \frac{2^{rs_1} - 1}{2^r - 1}\right)
\]

\[
\leq \varphi(n) \left(\frac{1}{2^{rs_1}} + \frac{2^{rs_1} - 1}{(2^r - 1) 2^{rs_1}}\right) \leq \varphi(n) \left(\frac{1}{2^{rs_1}} + \frac{1}{2^r - 1} - \frac{1}{(2^r - 1) 2^{rs_1}}\right)
\]

\[
\leq (n-1) \left(\frac{1}{2^r - 1} + \frac{2^r - 2}{(2^r - 1) 2^{rs_1}}\right) \leq (n-1) \frac{2}{2^r - 1} \leq (n-1) \frac{1}{2^{r-1}}
\]
Proof (case 2).

\[
\prod_{j=1}^{r} (t, t_j) + \sum_{j=1}^{s_1-1} \prod_{k=0}^{r} \left( 2^k (t, t_j) \right)
\]

\[
= \prod_{j=1}^{r} (t, t_j) \left( 1 + \sum_{k=0}^{s_1-1} 2^{kr} \right) = \prod_{j=1}^{r} (t, t_j) \left( 1 + \frac{2^{rs_1} - 1}{2^{r} - 1} \right)
\]

\[
\leq \frac{\prod_{j=1}^{r} 2^{sj} t_j}{2^{\sum_{j=1}^{r} sj}} \left( 1 + \frac{2^{rs_1} - 1}{2^{r} - 1} \right) \leq \frac{\prod_{j=1}^{r} (p_j - 1)}{2^{rs_1}} \left( 1 + \frac{2^{rs_1} - 1}{2^{r} - 1} \right)
\]

\[
\leq \varphi(n) \left( \frac{1}{2^{rs_1}} + \frac{2^{rs_1} - 1}{(2^{r} - 1) 2^{rs_1}} \right) \leq \varphi(n) \left( \frac{1}{2^{rs_1}} + \frac{1}{2^{r} - 1} - \frac{1}{2^{r} - 1} \right)
\]

\[
\leq (n-1) \left( \frac{1}{2^{r} - 1} + \frac{2^r - 2}{(2^{r} - 1) 2^{rs_1}} \right) \leq (n-1) \frac{2}{2^{r} - 1} \leq (n-1) \frac{1}{2^{r-1}}
\]

\[
\leq \frac{n-1}{4}
\]
Proof (case 3).

\[ n = p_1 p_2. \]

Note that \( r \geq 3 \) was only used in the last step of case 2. Hence, with the same argument and notation as in case 2, we obtain that the number of integers \( b \) for which \( n \) is a strong pseudoprime to base \( b \) is at most

\[
\left( \frac{n-1}{2} \right)^2 s_1^2 + s_2 \left( \frac{1}{2} + 2 s_1 - 1 \right) = \left( \frac{n-1}{2} \right)^2 s_2 - s_1 \left( \frac{1}{2} + 3 \cdot 2 s_1 \right) = \left( \frac{n-1}{2} \right)^2 s_2 - s_1 \left( \frac{1}{2} + 3 \cdot 2 s_1 \right) = \left( \frac{n-1}{2} \right)^2 s_2 - s_1 \left( \frac{1}{2} + 3 \cdot 2 s_1 \right) = \left( \frac{n-1}{2} \right)^2 s_2 - s_1 \left( \frac{1}{2} + 3 \cdot 2 s_1 \right)
\]

The term in the parentheses is bounded by \( \frac{1}{2} \), so, for \( s_2 > s_1 \), we obtain an upper bound of \( \frac{1}{4} \left( \frac{n-1}{2} \right)^2 \).
Proof (case 3).
Proof (case 3). $n = p_1 p_2$. 

Note that $r \geq 3$ was only used in the last step of case 2. Hence, with the same argument and notation as in case 2, we obtain that the number of integers $b$ for which $n$ is a strong pseudoprime to base $b$ is at most 

$$\frac{n - 1}{2^{s_2}} \cdot \left(1 + 2^{s_1 - 1} \cdot 2^{s_2 - 1} \cdot 2^{s_3 - 1}ight)$$

The term in the parentheses is bounded by $1$, so, for $s_2 > s_1$, we obtain an upper bound of $\frac{n - 1}{4}$. 

---

Bernd Schröder
Louisiana Tech University, College of Engineering and Science

Discrete Logarithms and Rabin’s Probabilistic Primality Test
**Proof (case 3).** \( n = p_1 p_2 \). Note that \( r \geq 3 \) was only used in the last step of case 2.
Proof (case 3). \( n = p_1 p_2 \). Note that \( r \geq 3 \) was only used in the last step of case 2. Hence, with the same argument and notation as in case 2.
Proof (case 3). $n = p_1 p_2$. Note that $r \geq 3$ was only used in the last step of case 2. Hence, with the same argument and notation as in case 2, we obtain that the number of integers $b$ for which $n$ is a strong pseudoprime to base $b$ is at most

$$(n-1) \frac{1}{2^{s_1+s_2}} \left( 1 + \frac{2^{2s_1} - 1}{2^2 - 1} \right)$$
Proof (case 3). \( n = p_1 p_2 \). Note that \( r \geq 3 \) was only used in the last step of case 2. Hence, with the same argument and notation as in case 2, we obtain that the number of integers \( b \) for which \( n \) is a strong pseudoprime to base \( b \) is at most

\[
(n-1) \frac{1}{2^{s_1+s_2}} \left( 1 + \frac{2^{2s_1} - 1}{2^2 - 1} \right) = (n-1) \frac{1}{2^{2s_1} 2^{s_2-s_1}} \left( 1 + \frac{2^{2s_1} - 1}{3} \right)
\]
Proof (case 3). \( n = p_1p_2 \). Note that \( r \geq 3 \) was only used in the last step of case 2. Hence, with the same argument and notation as in case 2, we obtain that the number of integers \( b \) for which \( n \) is a strong pseudoprime to base \( b \) is at most

\[
(n-1) \frac{1}{2^{s_1+s_2}} \left( 1 + \frac{2^{2s_1} - 1}{2^2 - 1} \right) = (n-1) \frac{1}{2^{2s_1}2^{s_2-s_1}} \left( 1 + \frac{2^{2s_1} - 1}{3} \right) = (n-1) \frac{1}{2^{s_2-s_1}} \left( \frac{1}{2^{2s_1}} + \frac{1}{3} - \frac{1}{3 \cdot 2^{2s_1}} \right)
\]
Proof (case 3). \( n = p_1 p_2 \). Note that \( r \geq 3 \) was only used in the last step of case 2. Hence, with the same argument and notation as in case 2, we obtain that the number of integers \( b \) for which \( n \) is a strong pseudoprime to base \( b \) is at most

\[
(n-1) \frac{1}{2^{s_1+s_2}} \left( 1 + \frac{2^{2s_1} - 1}{2^2 - 1} \right) = (n-1) \frac{1}{2^{2s_1} 2^{s_2-s_1}} \left( 1 + \frac{2^{2s_1} - 1}{3} \right) = (n-1) \frac{1}{2^{s_2-s_1}} \left( \frac{1}{2^{2s_1}} + \frac{1}{3} - \frac{1}{3 \cdot 2^{2s_1}} \right) = (n-1) \frac{1}{2^{s_2-s_1}} \left( \frac{2}{3 \cdot 2^{2s_1}} + \frac{1}{3} \right)
\]
Proof (case 3). \( n = p_1 p_2 \). Note that \( r \geq 3 \) was only used in the last step of case 2. Hence, with the same argument and notation as in case 2, we obtain that the number of integers \( b \) for which \( n \) is a strong pseudoprime to base \( b \) is at most

\[
(n-1) \frac{1}{2^{s_1+s_2}} \left( 1 + \frac{2^{2s_1} - 1}{2^2 - 1} \right) = (n-1) \frac{1}{2^{s_1}2^{s_2-s_1}} \left( 1 + \frac{2^{2s_1} - 1}{3} \right)
\]

\[
= (n-1) \frac{1}{2^{s_2-s_1}} \left( \frac{1}{2^{2s_1}} + \frac{1}{3} - \frac{1}{3 \cdot 2^{2s_1}} \right)
\]

\[
= (n-1) \frac{1}{2^{s_2-s_1}} \left( \frac{2}{3 \cdot 2^{2s_1}} + \frac{1}{3} \right)
\]

\[
= (n-1) \frac{1}{2^{s_2-s_1}} \left( \frac{1}{3 \cdot 2^{2s_1-1}} + \frac{1}{3} \right)
\]
**Proof (case 3).** \( n = p_1 p_2 \). Note that \( r \geq 3 \) was only used in the last step of case 2. Hence, with the same argument and notation as in case 2, we obtain that the number of integers \( b \) for which \( n \) is a strong pseudoprime to base \( b \) is at most

\[
(n-1) \frac{1}{2^{s_1+s_2}} \left(1 + \frac{2^{2s_1} - 1}{2^2 - 1}\right) = (n-1) \frac{1}{2^{2s_1}} \frac{1}{2^{s_2-s_1}} \left(1 + \frac{2^{2s_1} - 1}{3}\right)
\]

\[
= (n-1) \frac{1}{2^{s_2-s_1}} \left(\frac{1}{2^{2s_1}} + \frac{1}{3} - \frac{1}{3 \cdot 2^{2s_1}}\right)
\]

\[
= (n-1) \frac{1}{2^{s_2-s_1}} \left(\frac{2}{3 \cdot 2^{2s_1}} + \frac{1}{3}\right)
\]

\[
= (n-1) \frac{1}{2^{s_2-s_1}} \left(\frac{1}{3 \cdot 2^{2s_1-1}} + \frac{1}{3}\right)
\]

The term in the parentheses is bounded by \( \frac{1}{2} \)
Proof (case 3). \( n = p_1 p_2 \). Note that \( r \geq 3 \) was only used in the last step of case 2. Hence, with the same argument and notation as in case 2, we obtain that the number of integers \( b \) for which \( n \) is a strong pseudoprime to base \( b \) is at most

\[
(n-1) \frac{1}{2^{s_1+s_2}} \left(1 + \frac{2^{2s_1} - 1}{2^2 - 1}\right)
= (n-1) \frac{1}{2^{s_2-s_1}} \left(1 + \frac{2^{2s_1} - 1}{3}\right)
= (n-1) \frac{1}{2^{s_2-s_1}} \left(\frac{2}{3 \cdot 2^{2s_1}} + \frac{1}{3}\right)
= (n-1) \frac{1}{2^{s_2-s_1}} \left(\frac{1}{3 \cdot 2^{2s_1-1}} + \frac{1}{3}\right)
\]

The term in the parentheses is bounded by \( \frac{1}{2} \), so, for \( s_2 > s_1 \), we obtain an upper bound of \( \frac{1}{4} (n-1) \).
This leaves the case $s_1 = s_2$. In this case we have
$$2^{s_1 t} = n - 1 = p_1 p_2 - 1 = (p_1 - 1) p_2 + (p_2 - 1),$$
which implies $s_1 < s_2$. Therefore $(n - 1, p_j - 1) = 2 s_1 (t_1, t_j)$. Assume without loss of generality that $p_1 > p_2$. Suppose for a contradiction that $(t_1, t_1) = t_1$. Then $(p_1 - 1) | (n - 1)$ and then (modulo $p_1 - 1$) we would have $1 \equiv n = p_1 p_2 \equiv p_2$, which would imply $p_2 \geq p_1$, a contradiction. Hence $(t_1, t_1) < t_1$, which means that $(t_1, t_2) \leq t_1^3$. Hence the number of integers $b$ for which $n$ is a strong pseudoprime to base $b$ is at most
$$(t_1, t_1)(t_2, t_2)(1 + 2 s_1 - 1^3) \leq 1^3 t_1 t_2^2 2 s_1 1^3 2 s_1 (1 + 2 s_1 - 1^3) \leq 1^6 \varphi(n) \leq n - 1.$$
Proof (case 3).
\textbf{Proof (case 3).} This leaves the case \( s_1 = s_2 \).
**Proof (case 3).** This leaves the case $s_1 = s_2$. In this case we have $2^s t$.
Proof (case 3). This leaves the case $s_1 = s_2$. In this case we have $2^s t = n - 1$
Proof (case 3). This leaves the case \( s_1 = s_2 \). In this case we have \( 2^s t = n - 1 = p_1 p_2 - 1 \)
Proof (case 3). This leaves the case $s_1 = s_2$. In this case we have $2^{s_1}t = n - 1 = p_1p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1)$.
**Proof (case 3).** This leaves the case $s_1 = s_2$. In this case we have

$$2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2$$
**Proof (case 3).** This leaves the case $s_1 = s_2$. In this case we have

$$2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2)$$
Proof (case 3). This leaves the case \( s_1 = s_2 \). In this case we have
\[
2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1}(t_1 p_2 + t_2),
\]
which implies \( s_1 < s \).
**Proof (case 3).** This leaves the case \( s_1 = s_2 \). In this case we have \( 2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1}(t_1 p_2 + t_2) \), which implies \( s_1 < s \). Therefore \((n - 1, p_j - 1) = 2^{s_1}(t, t_j)\).
Proof (case 3). This leaves the case $s_1 = s_2$. In this case we have
$2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) =
2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2)$, which implies $s_1 < s$. Therefore $(n - 1, p_j - 1) = 2^{s_1} (t, t_j)$. Assume without loss of generality that $p_1 > p_2$. 

Bernd Schröder

Louisiana Tech University, College of Engineering and Science

Discrete Logarithms and Rabin’s Probabilistic Primality Test
**Proof (case 3).** This leaves the case $s_1 = s_2$. In this case we have

\[ 2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2), \]

which implies $s_1 < s$. Therefore $(n - 1, p_j - 1) = 2^{s_1} (t, t_j)$. Assume without loss of generality that $p_1 > p_2$. Suppose for a contradiction that $(t, t_1) = t_1$. 

---

**Index Arithmetic**

- Power Residues
- Rabin's Probabilistic Primality Test
- More Primality Tests

---

**Bernd Schröder**

Louisiana Tech University, College of Engineering and Science

Discrete Logarithms and Rabin’s Probabilistic Primality Test
Proof (case 3). This leaves the case $s_1 = s_2$. In this case we have
$$2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1) p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2),$$
which implies $s_1 < s$. Therefore $(n - 1, p_j - 1) = 2^{s_1} (t, t_j)$. Assume without loss of generality that $p_1 > p_2$. Suppose for a contradiction that $(t, t_1) = t_1$. Then $(p_1 - 1) | (n - 1)$ and then (modulo $p_1 - 1$) we would have
**Proof (case 3).** This leaves the case $s_1 = s_2$. In this case we have

$$2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2),$$

which implies $s_1 < s$. Therefore $(n - 1, p_j - 1) = 2^{s_1} (t, t_j)$. Assume without loss of generality that $p_1 > p_2$. Suppose for a contradiction that $(t, t_1) = t_1$. Then $(p_1 - 1) | (n - 1)$ and then (modulo $p_1 - 1$) we would have $1 \equiv n$. 


Proof (case 3). This leaves the case $s_1 = s_2$. In this case we have $2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1) p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2)$, which implies $s_1 < s$. Therefore $(n - 1, p_j - 1) = 2^{s_1} (t, t_j)$. Assume without loss of generality that $p_1 > p_2$. Suppose for a contradiction that $(t, t_1) = t_1$. Then $(p_1 - 1) | (n - 1)$ and then (modulo $p_1 - 1$) we would have $1 \equiv n = p_1 p_2$
**Proof (case 3).** This leaves the case $s_1 = s_2$. In this case we have $2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2)$, which implies $s_1 < s$. Therefore $(n - 1, p_j - 1) = 2^{s_1} (t, t_j)$. Assume without loss of generality that $p_1 > p_2$. Suppose for a contradiction that $(t, t_1) = t_1$. Then $(p_1 - 1) | (n - 1)$ and then (modulo $p_1 - 1$) we would have $1 \equiv n = p_1 p_2 \equiv p_2$.
Proof (case 3). This leaves the case $s_1 = s_2$. In this case we have $2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2)$, which implies $s_1 < s$. Therefore $(n - 1, p_j - 1) = 2^{s_1} (t, t_j)$. Assume without loss of generality that $p_1 > p_2$. Suppose for a contradiction that $(t, t_1) = t_1$. Then $(p_1 - 1)| (n - 1)$ and then (modulo $p_1 - 1$) we would have $1 \equiv n = p_1 p_2 \equiv p_2$, which would imply $p_2 \geq p_1$, a contradiction.
**Proof (case 3).** This leaves the case $s_1 = s_2$. In this case we have $2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2)$, which implies $s_1 < s$. Therefore $(n - 1, p_j - 1) = 2^{s_1} (t, t_j)$. Assume without loss of generality that $p_1 > p_2$. Suppose for a contradiction that $(t, t_1) = t_1$. Then $(p_1 - 1) | (n - 1)$ and then (modulo $p_1 - 1$) we would have $1 \equiv n = p_1 p_2 \equiv p_2$, which would imply $p_2 \geq p_1$, a contradiction. Hence $(t, t_1) < t_1$, which means that $(t, t_1) \leq \frac{t_1}{3}$. 
**Proof (case 3).** This leaves the case $s_1 = s_2$. In this case we have $2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2)$, which implies $s_1 < s$. Therefore $(n - 1, p_j - 1) = 2^{s_1} (t, t_j)$. Assume without loss of generality that $p_1 > p_2$. Suppose for a contradiction that $(t, t_1) = t_1$. Then $(p_1 - 1) | (n - 1)$ and then (modulo $p_1 - 1$) we would have $1 \equiv n = p_1 p_2 \equiv p_2$, which would imply $p_2 \geq p_1$, a contradiction. Hence $(t, t_1) < t_1$, which means that $(t, t_1) \leq \frac{t_1}{3}$. Hence the number of integers $b$ for which $n$ is a strong pseudoprime to base $b$ is at most

$$ (t, t_1)(t, t_2) \left(1 + \frac{2^{2s_1} - 1}{3}\right) $$
Proof (case 3). This leaves the case $s_1 = s_2$. In this case we have $2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1}(t_1 p_2 + t_2)$, which implies $s_1 < s$. Therefore $(n - 1, p_j - 1) = 2^{s_1}(t, t_j)$. Assume without loss of generality that $p_1 > p_2$. Suppose for a contradiction that $(t, t_1) = t_1$. Then $(p_1 - 1)|(n - 1)$ and then (modulo $p_1 - 1$) we would have $1 \equiv n = p_1 p_2 \equiv p_2$, which would imply $p_2 \geq p_1$, a contradiction. Hence $(t, t_1) < t_1$, which means that $(t, t_1) \leq \frac{t_1}{3}$. Hence the number of integers $b$ for which $n$ is a strong pseudoprime to base $b$ is at most

$$(t, t_1)(t, t_2) \left(1 + \frac{2^{2s_1} - 1}{3}\right) \leq \frac{1}{3} t_1 t_2 2^{2s_1} \frac{1}{2^{2s_1}} \left(1 + \frac{2^{2s_1} - 1}{3}\right)$$
Proof (case 3). This leaves the case \( s_1 = s_2 \). In this case we have
\[
2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1) p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2),
\]
which implies \( s_1 < s \). Therefore \((n - 1, p_j - 1) = 2^{s_1}(t, t_j)\). Assume without loss of generality that \( p_1 > p_2 \). Suppose for a contradiction that \((t, t_1) = t_1\). Then \((p_1 - 1) | (n - 1)\) and then (modulo \( p_1 - 1 \)) we would have
\[
1 \equiv n = p_1 p_2 \equiv p_2,
\]
which would imply \( p_2 \geq p_1 \), a contradiction. Hence \((t, t_1) < t_1\), which means that \((t, t_1) \leq \frac{t_1}{3}\). Hence the number of integers \( b \) for which \( n \) is a strong pseudoprime to base \( b \) is at most
\[
(t, t_1)(t, t_2) \left(1 + \frac{2^{2s_1} - 1}{3}\right) \leq \frac{1}{3} t_1 t_2 2^{2s_1} \frac{1}{2^{2s_1}} \left(1 + \frac{2^{2s_1} - 1}{3}\right) \leq \frac{1}{3} \varphi(n) \frac{1}{2},
\]
Proof (case 3). This leaves the case $s_1 = s_2$. In this case we have $2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2)$, which implies $s_1 < s$. Therefore $(n - 1, p_j - 1) = 2^{s_1} (t, t_j)$. Assume without loss of generality that $p_1 > p_2$. Suppose for a contradiction that $(t, t_1) = t_1$. Then $(p_1 - 1) | (n - 1)$ and then (modulo $p_1 - 1$) we would have $1 \equiv n = p_1 p_2 \equiv p_2$, which would imply $p_2 \geq p_1$, a contradiction. Hence $(t, t_1) < t_1$, which means that $(t, t_1) \leq \frac{t_1}{3}$. Hence the number of integers $b$ for which $n$ is a strong pseudoprime to base $b$ is at most

$$
(t, t_1)(t, t_2) \left(1 + \frac{2^{2s_1} - 1}{3}\right) \leq \frac{1}{3} t_1 t_2 2^{2s_1} \frac{1}{2^{2s_1}} \left(1 + \frac{2^{2s_1} - 1}{3}\right) \\
\leq \frac{1}{3} \varphi(n) \frac{1}{2} \leq \frac{1}{6} n
$$
**Proof (case 3).** This leaves the case $s_1 = s_2$. In this case we have $2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2)$, which implies $s_1 < s$. Therefore $(n - 1, p_j - 1) = 2^{s_1} (t, t_j)$. Assume without loss of generality that $p_1 > p_2$. Suppose for a contradiction that $(t, t_1) = t_1$. Then $(p_1 - 1) | (n - 1)$ and then (modulo $p_1 - 1$) we would have $1 \equiv n = p_1 p_2 \equiv p_2$, which would imply $p_2 \geq p_1$, a contradiction. Hence $(t, t_1) < t_1$, which means that $(t, t_1) \leq \frac{t_1}{3}$. Hence the number of integers $b$ for which $n$ is a strong pseudoprime to base $b$ is at most

$$(t, t_1)(t, t_2) \left(1 + \frac{2^{2s_1} - 1}{3}\right) \leq \frac{1}{3} t_1 t_2 2^{2s_1} \frac{1}{2^{2s_1}} \left(1 + \frac{2^{2s_1} - 1}{3}\right) \leq \frac{1}{3} \varphi(n) \frac{1}{2} \leq \frac{1}{6} n \leq \frac{n - 1}{4}$$
**Proof (case 3).** This leaves the case \( s_1 = s_2 \). In this case we have \( 2^s t = n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1) = 2^{s_1} t_1 p_2 + 2^{s_1} t_2 = 2^{s_1} (t_1 p_2 + t_2) \), which implies \( s_1 < s \). Therefore \( (n - 1, p_j - 1) = 2^{s_1} (t, t_j) \). Assume without loss of generality that \( p_1 > p_2 \). Suppose for a contradiction that \( (t, t_1) = t_1 \). Then \( (p_1 - 1)|(n - 1) \) and then (modulo \( p_1 - 1 \)) we would have \( 1 \equiv n = p_1 p_2 \equiv p_2 \), which would imply \( p_2 \geq p_1 \), a contradiction. Hence \( (t, t_1) < t_1 \), which means that \( (t, t_1) \leq \frac{t_1}{3} \). Hence the number of integers \( b \) for which \( n \) is a strong pseudoprime to base \( b \) is at most

\[
(t, t_1)(t, t_2) \left( 1 + \frac{2^{2s_1} - 1}{3} \right) \leq \frac{1}{3} t_1 t_2 2^{2s_1} \frac{1}{2^{2s_1}} \left( 1 + \frac{2^{2s_1} - 1}{3} \right) \\
\leq \frac{1}{3} \varphi(n) \frac{1}{2} \leq \frac{1}{6} n \leq \frac{n - 1}{4}
\]
Theorem.
Theorem. Rabin’s Probabilistic Primality Test.
Theorem. Rabin’s Probabilistic Primality Test. Let $n$ be a composite number.
Theorem. Rabin’s Probabilistic Primality Test. Let $n$ be a composite number. Then the probability that $n$ passes Miller’s test with $k$ randomly chosen bases $b_1, \ldots, b_k$ between 1 and $n$ is $\frac{1}{4^k}$. \hfill \blacksquare
Theorem.

Let $n \in \mathbb{N}$ be so that there is an $x \in \mathbb{Z}$ so that $x^{n-1} \equiv 1 \pmod{n}$ and $x^{n-1}q \not\equiv 1 \pmod{n}$ for all prime divisors of $n-1$. Then $n$ is prime.

Proof. Because $x^{n-1} \equiv 1 \pmod{n}$, we know that $\text{ord}_n(x) \mid (n-1)$. Suppose for a contradiction that $\text{ord}_n(x) < n-1$. Then there is a $k > 1$ so that $n-1 = \text{ord}_n(x)^k$. However, this would imply that, for a prime divisor $q$ of $k$, we have $x^{n-1}q = x^{\text{ord}_n(x)^k}q = (x^{\text{ord}_n(x)})^kq \equiv 1 \pmod{n}$, which is a contradiction. Hence $n-1 = \text{ord}_n(x) \leq \phi(n) \leq n-1$, which implies $\phi(n) = n-1$, that is, $n$ is prime.
Theorem. Lucas’ Converse of Fermat’s Little Theorem.

\[ \text{Let } n \in \mathbb{N} \text{ be so that there is an } x \in \mathbb{Z} \text{ so that } x^{n-1} \equiv 1 \pmod{n} \text{ and } x^{n-1} q \not\equiv 1 \pmod{n} \text{ for all prime divisors of } n - 1. \]

Then \( n \) is prime.

Proof. Because \( x^{n-1} \equiv 1 \pmod{n} \), we know that \( \text{ord}_n(x) \mid (n-1) \).

Suppose for a contradiction that \( \text{ord}_n(x) < n - 1 \).

Then there is a \( k > 1 \) so that \( n-1 = \text{ord}_n(x^k) \).

However, this would imply that, for a prime divisor \( q \) of \( k \), we have \( x^{n-1} q = x^{k \text{ord}_n(x)} q \equiv 1 \pmod{n} \), which is a contradiction.

Hence \( n - 1 = \text{ord}_n(x) \leq \phi(n) \leq n - 1 \), which implies \( \phi(n) = n - 1 \), that is, \( n \) is prime.
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let \( n \in \mathbb{N} \) be so that there is an \( x \in \mathbb{Z} \) so that \( x^{n-1} \equiv 1 \pmod{n} \) and \( x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n} \) for all prime divisors of \( n - 1 \).
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let $n \in \mathbb{N}$ be so that there is an $x \in \mathbb{Z}$ so that $x^{n-1} \equiv 1 \pmod{n}$ and $x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$ for all prime divisors of $n - 1$. Then $n$ is prime.
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let $n \in \mathbb{N}$ be so that there is an $x \in \mathbb{Z}$ so that $x^{n-1} \equiv 1 \pmod{n}$ and $x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$ for all prime divisors of $n - 1$. Then $n$ is prime.

Proof.
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let \( n \in \mathbb{N} \) be so that there is an \( x \in \mathbb{Z} \) so that \( x^{n-1} \equiv 1 \) (mod \( n \)) and \( x^{\frac{n-1}{q}} \not\equiv 1 \) (mod \( n \)) for all prime divisors of \( n-1 \). Then \( n \) is prime.

Proof. Because \( x^{n-1} \equiv 1 \) (mod \( n \)), we know that \( \text{ord}_n(x) | (n - 1) \).
**Theorem. Lucas’ Converse of Fermat’s Little Theorem.** Let \( n \in \mathbb{N} \) be so that there is an \( x \in \mathbb{Z} \) so that \( x^{n-1} \equiv 1 \pmod{n} \) and \( x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n} \) for all prime divisors of \( n - 1 \). Then \( n \) is prime.

**Proof.** Because \( x^{n-1} \equiv 1 \pmod{n} \), we know that \( \text{ord}_n(x) | (n - 1) \). Suppose for a contradiction that \( \text{ord}_n(x) < n - 1 \).
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let $n \in \mathbb{N}$ be so that there is an $x \in \mathbb{Z}$ so that $x^{n-1} \equiv 1 \pmod{n}$ and $x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$ for all prime divisors of $n - 1$. Then $n$ is prime.

Proof. Because $x^{n-1} \equiv 1 \pmod{n}$, we know that $\text{ord}_n(x)|(n - 1)$. Suppose for a contradiction that $\text{ord}_n(x) < n - 1$. Then there is a $k > 1$ so that $n - 1 = \text{ord}_n(x)k$. 
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let $n \in \mathbb{N}$ be so that there is an $x \in \mathbb{Z}$ so that $x^{n-1} \equiv 1 \pmod{n}$ and $x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$ for all prime divisors of $n - 1$. Then $n$ is prime.

Proof. Because $x^{n-1} \equiv 1 \pmod{n}$, we know that $\text{ord}_n(x)|(n - 1)$. Suppose for a contradiction that $\text{ord}_n(x) < n - 1$. Then there is a $k > 1$ so that $n - 1 = \text{ord}_n(x)k$. However, this would imply that, for a prime divisor $q$ of $k$, we have

$$x^{\frac{n-1}{q}}$$
Theorem. Lucas’ Converse of Fermat’s Little Theorem. \( \text{Let } n \in \mathbb{N} \text{ be so that there is an } x \in \mathbb{Z} \text{ so that } x^{n-1} \equiv 1 \pmod{n} \text{ and } x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n} \text{ for all prime divisors of } n-1. \text{ Then } n \text{ is prime.} \)

Proof. Because \( x^{n-1} \equiv 1 \pmod{n} \), we know that \( \text{ord}_n(x)|(n-1) \). Suppose for a contradiction that \( \text{ord}_n(x) < n-1 \). Then there is a \( k > 1 \) so that \( n-1 = \text{ord}_n(x)k \). However, this would imply that, for a prime divisor \( q \) of \( k \), we have

\[
\frac{x^{n-1}}{q} = x^{\frac{k\text{ord}_n(x)}{q}}
\]
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let \( n \in \mathbb{N} \) be so that there is an \( x \in \mathbb{Z} \) so that \( x^{n-1} \equiv 1 \pmod{n} \) and \( x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n} \) for all prime divisors of \( n-1 \). Then \( n \) is prime.

Proof. Because \( x^{n-1} \equiv 1 \pmod{n} \), we know that \( \text{ord}_n(x) \mid (n-1) \). Suppose for a contradiction that \( \text{ord}_n(x) < n-1 \). Then there is a \( k > 1 \) so that \( n-1 = \text{ord}_n(x)k \). However, this would imply that, for a prime divisor \( q \) of \( k \), we have

\[
x^{\frac{n-1}{q}} = x^{\frac{k \text{ord}_n(x)}{q}} = \left(x^{\text{ord}_n(x)}\right)^{\frac{k}{q}}
\]
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let $n \in \mathbb{N}$ be so that there is an $x \in \mathbb{Z}$ so that $x^{n-1} \equiv 1 \pmod{n}$ and $x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$ for all prime divisors of $n-1$. Then $n$ is prime.

Proof. Because $x^{n-1} \equiv 1 \pmod{n}$, we know that $\text{ord}_n(x)| (n-1)$. Suppose for a contradiction that $\text{ord}_n(x) < n-1$. Then there is a $k > 1$ so that $n-1 = \text{ord}_n(x)k$. However, this would imply that, for a prime divisor $q$ of $k$, we have

$$x^{\frac{n-1}{q}} = x^{\frac{k\text{ord}_n(x)}{q}} = \left(x^{\text{ord}_n(x)}\right)^{\frac{k}{q}} \equiv 1 \pmod{n}$$
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let $n \in \mathbb{N}$ be so that there is an $x \in \mathbb{Z}$ so that $x^{n-1} \equiv 1 \pmod{n}$ and $x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$ for all prime divisors of $n-1$. Then $n$ is prime.

Proof. Because $x^{n-1} \equiv 1 \pmod{n}$, we know that $\text{ord}_n(x)|(n - 1)$. Suppose for a contradiction that $\text{ord}_n(x) < n - 1$. Then there is a $k > 1$ so that $n - 1 = \text{ord}_n(x)k$. However, this would imply that, for a prime divisor $q$ of $k$, we have

$$x^{\frac{n-1}{q}} = x^{\frac{k\text{ord}_n(x)}{q}} = \left(x^{\text{ord}_n(x)}\right)^{\frac{k}{q}} \equiv 1 \pmod{n},$$

which is a contradiction.
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let \( n \in \mathbb{N} \) be so that there is an \( x \in \mathbb{Z} \) so that \( x^{n-1} \equiv 1 \pmod{n} \) and \( x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n} \) for all prime divisors of \( n - 1 \). Then \( n \) is prime.

Proof. Because \( x^{n-1} \equiv 1 \pmod{n} \), we know that \( \text{ord}_n(x) \mid (n - 1) \). Suppose for a contradiction that \( \text{ord}_n(x) < n - 1 \). Then there is a \( k > 1 \) so that \( n - 1 = \text{ord}_n(x)k \). However, this would imply that, for a prime divisor \( q \) of \( k \), we have

\[
    x^{\frac{n-1}{q}} = x^{\frac{k\text{ord}_n(x)}{q}} = \left(x^{\text{ord}_n(x)}\right)^{\frac{k}{q}} \equiv 1 \pmod{n},
\]

which is a contradiction. Hence \( n - 1 = \text{ord}_n(x) \).
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let $n \in \mathbb{N}$ be so that there is an $x \in \mathbb{Z}$ so that $x^{n-1} \equiv 1 \pmod{n}$ and $x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$ for all prime divisors of $n - 1$. Then $n$ is prime.

Proof. Because $x^{n-1} \equiv 1 \pmod{n}$, we know that $\text{ord}_n(x)|(n-1)$. Suppose for a contradiction that $\text{ord}_n(x) < n - 1$. Then there is a $k > 1$ so that $n - 1 = \text{ord}_n(x)k$. However, this would imply that, for a prime divisor $q$ of $k$, we have

$$x^{\frac{n-1}{q}} = x^{\frac{k\text{ord}_n(x)}{q}} = \left(x^{\text{ord}_n(x)}\right)^{\frac{k}{q}} \equiv 1 \pmod{n},$$

which is a contradiction. Hence

$n - 1 = \text{ord}_n(x) \leq \phi(n)$
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let $n \in \mathbb{N}$ be so that there is an $x \in \mathbb{Z}$ so that $x^{n-1} \equiv 1 \pmod{n}$ and $x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$ for all prime divisors of $n - 1$. Then $n$ is prime.

Proof. Because $x^{n-1} \equiv 1 \pmod{n}$, we know that $\text{ord}_n(x)|(n - 1)$. Suppose for a contradiction that $\text{ord}_n(x) < n - 1$. Then there is a $k > 1$ so that $n - 1 = \text{ord}_n(x)k$. However, this would imply that, for a prime divisor $q$ of $k$, we have

$$x^{\frac{n-1}{q}} = x^{\frac{k\text{ord}_n(x)}{q}} = \left(x^{\text{ord}_n(x)}\right)^{\frac{k}{q}} \equiv 1 \pmod{n},$$

which is a contradiction. Hence $n - 1 = \text{ord}_n(x) \leq \varphi(n) \leq n - 1$. 
**Theorem. Lucas’ Converse of Fermat’s Little Theorem.** Let \( n \in \mathbb{N} \) be so that there is an \( x \in \mathbb{Z} \) so that \( x^{n-1} \equiv 1 \pmod{n} \) and \( x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n} \) for all prime divisors of \( n - 1 \). Then \( n \) is prime.

**Proof.** Because \( x^{n-1} \equiv 1 \pmod{n} \), we know that \( \text{ord}_n(x) \mid (n - 1) \). Suppose for a contradiction that \( \text{ord}_n(x) < n - 1 \). Then there is a \( k > 1 \) so that \( n - 1 = \text{ord}_n(x)k \). However, this would imply that, for a prime divisor \( q \) of \( k \), we have

\[
x^{\frac{n-1}{q}} = x^{\frac{k\text{ord}_n(x)}{q}} = \left(x^{\text{ord}_n(x)}\right)^{\frac{k}{q}} \equiv 1 \pmod{n},
\]

which is a contradiction. Hence \( n - 1 = \text{ord}_n(x) \leq \varphi(n) \leq n - 1 \), which implies \( \varphi(n) = n - 1 \).
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let $n \in \mathbb{N}$ be so that there is an $x \in \mathbb{Z}$ so that $x^{n-1} \equiv 1 \pmod{n}$ and $x^{n-1}/q \not\equiv 1 \pmod{n}$ for all prime divisors of $n - 1$. Then $n$ is prime.

Proof. Because $x^{n-1} \equiv 1 \pmod{n}$, we know that $\text{ord}_n(x) \mid (n - 1)$. Suppose for a contradiction that $\text{ord}_n(x) < n - 1$. Then there is a $k > 1$ so that $n - 1 = \text{ord}_n(x)k$. However, this would imply that, for a prime divisor $q$ of $k$, we have

$$x^{n-1}/q = x^{k \text{ord}_n(x)/q} = (x^{\text{ord}_n(x)})^{k/q} \equiv 1 \pmod{n},$$

which is a contradiction. Hence $n - 1 = \text{ord}_n(x) \leq \varphi(n) \leq n - 1$, which implies $\varphi(n) = n - 1$, that is, $n$ is prime.
Theorem. Lucas’ Converse of Fermat’s Little Theorem. Let $n \in \mathbb{N}$ be so that there is an $x \in \mathbb{Z}$ so that $x^{n-1} \equiv 1 \pmod{n}$ and $x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$ for all prime divisors of $n-1$. Then $n$ is prime.

Proof. Because $x^{n-1} \equiv 1 \pmod{n}$, we know that $\text{ord}_n(x) | (n-1)$. Suppose for a contradiction that $\text{ord}_n(x) < n-1$. Then there is a $k > 1$ so that $n - 1 = \text{ord}_n(x)k$. However, this would imply that, for a prime divisor $q$ of $k$, we have

$$x^{\frac{n-1}{q}} = x^{\frac{k\text{ord}_n(x)}{q}} = (x^{\text{ord}_n(x)})^k \equiv 1 \pmod{n},$$

which is a contradiction. Hence $n - 1 = \text{ord}_n(x) \leq \varphi(n) \leq n - 1$, which implies $\varphi(n) = n - 1$, that is, $n$ is prime.
Corollary.
Corollary. Let \( n, x \in \mathbb{N} \) be so that \( n \) is odd and
\[
x^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad \text{and} \quad x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}
\]
for all odd prime divisors of \( n - 1 \). Then \( n \) is prime.
Corollary. Let $n, x \in \mathbb{N}$ be so that $n$ is odd and
\[ x^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad \text{and} \quad x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n} \quad \text{for all odd prime divisors of } n - 1. \text{ Then } n \text{ is prime.} \]

Proof.
Corollary. Let $n, x \in \mathbb{N}$ be so that $n$ is odd and
$$x^{\frac{n-1}{2}} \equiv -1 \pmod{n} \text{ and } x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n} \text{ for all odd prime divisors of } n - 1.$$ Then $n$ is prime.

Proof. $x^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ implies that $x^{n-1} \equiv 1 \pmod{n}$. 
Corollary. Let $n, x \in \mathbb{N}$ be so that $n$ is odd and
\[ x^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad \text{and} \quad x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n} \quad \text{for all odd prime divisors} \quad q \quad \text{of} \quad n - 1. \quad \text{Then} \quad n \quad \text{is prime.}
\]

Proof. $x^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ implies that $x^{n-1} \equiv 1 \pmod{n}$. Now we can apply Lucas’ result.
Corollary. Let \( n, x \in \mathbb{N} \) be so that \( n \) is odd and 
\[
x^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad \text{and} \quad x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}
\]
for all odd prime divisors of \( n - 1 \). Then \( n \) is prime.

Proof. \( x^{\frac{n-1}{2}} \equiv -1 \pmod{n} \) implies that \( x^{n-1} \equiv 1 \pmod{n} \). Now we can apply Lucas’ result."
Theorem.
**Theorem.** When sufficient information is available, it can be checked in $O\left((\log_2(n))^4\right)$ bit operations if a given number $n$ is prime.
**Theorem.** When sufficient information is available, it can be checked in $O \left( (\log_2(n))^4 \right)$ bit operations if a given number $n$ is prime.

**Explanation.**
Theorem. When sufficient information is available, it can be checked in $O \left( (\log_2(n))^4 \right)$ bit operations if a given number $n$ is prime.

Explanation. Basically, if we can factor $n - 1$, then the number of steps is the number of steps it takes to verify the condition in the preceding corollary.
**Theorem.** When sufficient information is available, it can be checked in $O \left( (\log_2(n))^4 \right)$ bit operations if a given number $n$ is prime.

**Explanation.** Basically, if we can factor $n - 1$, then the number of steps is the number of steps it takes to verify the condition in the preceding corollary.
Theorem. When sufficient information is available, it can be checked in $O\left((\log_2(n))^4\right)$ bit operations if a given number $n$ is prime.

Explanation. Basically, if we can factor $n - 1$, then the number of steps is the number of steps it takes to verify the condition in the preceding corollary.

The next test also relies on some ability to factor $n - 1$. 
Pocklington's Primality Test.

Let $n \in \mathbb{N}$ be so that $n - 1 = FR$, with $(F, R) = 1$ and $F > R$.

If there is an integer $a$ so that $a^n - 1 \equiv 1 \pmod{n}$ and $(a^{n - q - 1}, n) = 1$ for all prime divisors $q$ of $F$,

then $n$ is prime.

Proof.

Suppose for a contradiction that there is a prime divisor $1 < p \leq \sqrt{n}$ of $n$.

The congruence $a^n - 1 \equiv 1 \pmod{n}$ implies that $\text{ord}_p(a) | n - 1$.

Let $t$ be so that $n - 1 = t \text{ord}_p(a)$.

Now let $q$ be a prime factor of $F$ and let $e$ be the exponent of $q$ in the prime factorization of $F$.

Suppose for a contradiction that $q | t$.

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

But this means that $p | (a^{n - q - 1}, n) = 1$, a contradiction.

Hence $q \nmid t$ and therefore $q^e | \text{ord}_p(a)$.

Because $q$ was an arbitrary prime factor of $F$, we conclude $F | \text{ord}_p(a)$.

From $\text{ord}_p(a) | p - 1$, we conclude $F | p - 1$ and hence $F < p$.

This is a contradiction, because we infer $n < F^2 < p^2 \leq n$.
Theorem. Pocklington’s Primality Test.

Let $n \in \mathbb{N}$ be so that $n - 1 = FR$, with $(F, R) = 1$ and $F > R$.

If there is an integer $a$ so that $a^{n-1} \equiv 1 \pmod{n}$ and $(a^{n-1} q^{-1}, n) = 1$ for all prime divisors $q$ of $F$,

then $n$ is prime.

Proof. Suppose for a contradiction that there is a prime divisor $1 < p \leq \sqrt{n}$ of $n$.

The congruence $a^{n-1} \equiv 1 \pmod{n}$ implies that $\text{ord}_p(a) | n - 1$.

Let $t$ be so that $n - 1 = t \text{ord}_p(a)$.

Now let $q$ be a prime factor of $F$ and let $e$ be the exponent of $q$ in the prime factorization of $F$.

Suppose for a contradiction that $q | t$.

Then $a^{n-1} q^{-1} = a^{tq^{-1}} \equiv 1 \pmod{p}$.

But this means that $p | (a^{n-1} q^{-1}, n) = 1$, a contradiction.

Hence $q \nmid t$ and therefore $q^e | \text{ord}_p(a)$.

Because $q$ was an arbitrary prime factor of $F$,

we conclude $F | \text{ord}_p(a)$.

From $\text{ord}_p(a) | p - 1$, we conclude $F | p - 1$ and hence $F < p$.

This is a contradiction, because we infer $n < F^2 < p^2 \leq n$. 

Bernd Schröder

Louisiana Tech University, College of Engineering and Science
Theorem. Pocklington’s Primality Test. Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \((F, R) = 1\) and \( F > R \).
Theorem. Pocklington’s Primality Test. Let \( n \in \mathbb{N} \) be so that \( n-1 = FR \), with \( (F,R) = 1 \) and \( F > R \). If there is an integer \( a \) so that \( a^{n-1} \equiv 1 \pmod{n} \) and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \).
**Theorem. Pocklington’s Primality Test.** Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \( (F, R) = 1 \) and \( F > R \). If there is an integer \( a \) so that \( a^{n-1} \equiv 1 \pmod{n} \) and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.
Theorem. Pocklington’s Primality Test. Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \( (F, R) = 1 \) and \( F > R \). If there is an integer \( a \) so that \( a^{n-1} \equiv 1 \pmod{n} \) and \( (a^{n-1}/q - 1, n) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.

Proof.
Theorem. Pocklington’s Primality Test. Let $n \in \mathbb{N}$ be so that $n - 1 = FR$, with $(F, R) = 1$ and $F > R$. If there is an integer $a$ so that $a^{n-1} \equiv 1 \pmod{n}$ and $\left(a^{\frac{n-1}{q}} - 1, n\right) = 1$ for all prime divisors $q$ of $F$, then $n$ is prime.

Proof. Suppose for a contradiction that there is a prime divisor $1 < p \leq \sqrt{n}$ of $n$. 
**Theorem. Pocklington’s Primality Test.** Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \((F, R) = 1\) and \( F > R \). If there is an integer \( a \) so that \( a^{n-1} \equiv 1 \pmod{n} \) and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.

**Proof.** Suppose for a contradiction that there is a prime divisor \( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \)
Theorem. Pocklington’s Primality Test. Let $n \in \mathbb{N}$ be so that $n - 1 = FR$, with $(F, R) = 1$ and $F > R$. If there is an integer $a$ so that $a^{n-1} \equiv 1 \pmod{n}$ and $\left( a^{\frac{n-1}{q}} - 1, n \right) = 1$ for all prime divisors $q$ of $F$, then $n$ is prime.

Proof. Suppose for a contradiction that there is a prime divisor $1 < p \leq \sqrt{n}$ of $n$. The congruence $a^{n-1} \equiv 1 \pmod{n}$ implies that $\text{ord}_p(a) | n - 1$. 

Bernd Schröder
Louisiana Tech University, College of Engineering and Science
Theorem. Pocklington’s Primality Test. Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \( (F, R) = 1 \) and \( F > R \). If there is an integer \( a \) so that \( a^{n-1} \equiv 1 \pmod{n} \) and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.

Proof. Suppose for a contradiction that there is a prime divisor \( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that \( \text{ord}_p(a) | n - 1 \). Let \( t \) be so that \( n - 1 = t \text{ord}_p(a) \).
Theorem. Pocklington’s Primality Test. Let $n \in \mathbb{N}$ be so that $n - 1 = FR$, with $(F, R) = 1$ and $F > R$. If there is an integer $a$ so that $a^{n-1} \equiv 1 \pmod{n}$ and $(a^{\frac{n-1}{q}} - 1, n) = 1$ for all prime divisors $q$ of $F$, then $n$ is prime.

**Proof.** Suppose for a contradiction that there is a prime divisor $1 < p \leq \sqrt{n}$ of $n$. The congruence $a^{n-1} \equiv 1 \pmod{n}$ implies that $\text{ord}_p(a)|n - 1$. Let $t$ be so that $n - 1 = t \text{ord}_p(a)$. Now let $q$ be a prime factor of $F$ and let $e$ be the exponent of $q$ in the prime factorization of $F$. 
**Theorem. Pocklington’s Primality Test.** Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \( (F, R) = 1 \) and \( F > R \). If there is an integer \( a \) so that 
\[
a^{n-1} \equiv 1 \pmod{n}
\]
and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.

**Proof.** Suppose for a contradiction that there is a prime divisor \( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that \( \text{ord}_p(a)|n - 1 \). Let \( t \) be so that \( n - 1 = t\text{ord}_p(a) \).

Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the prime factorization of \( F \). Suppose for a contradiction that \( q|t \).
Theorem. Pocklington’s Primality Test. Let \( n \in \mathbb{N} \) be so that 
\( n - 1 = FR \), with \((F, R) = 1\) and \( F > R \). If there is an integer \( a \) so that 
\( a^{n-1} \equiv 1 \pmod{n} \) and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \), 
then \( n \) is prime.

Proof. Suppose for a contradiction that there is a prime divisor 
\( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that 
\( \text{ord}_p(a) | n - 1 \). Let \( t \) be so that \( n - 1 = t \text{ord}_p(a) \).
Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the 
prime factorization of \( F \). Suppose for a contradiction that \( q | t \). Then 
\( a^{\frac{n-1}{q}} \)
Theorem. Pocklington’s Primality Test. Let \( n \in \mathbb{N} \) be so that 
\( n - 1 = FR \), with \((F,R) = 1\) and \( F > R \). If there is an integer \( a \) so that
\( a^{n-1} \equiv 1 \pmod{n} \) and \( \left(a^{n-1}/q - 1, n\right) = 1 \) for all prime divisors \( q \) of \( F \),
then \( n \) is prime.

Proof. Suppose for a contradiction that there is a prime divisor 
\( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that 
\( \text{ord}_p(a)|n - 1 \). Let \( t \) be so that \( n - 1 = t\text{ord}_p(a) \).
Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the prime factorization of \( F \). Suppose for a contradiction that \( q|t \). Then 
\[ a^{\frac{n-1}{q}} = a^{\text{ord}_p(a)\frac{t}{q}} \]
Theorem. Pocklington’s Primality Test. Let $n \in \mathbb{N}$ be so that $n - 1 = FR$, with $(F, R) = 1$ and $F > R$. If there is an integer $a$ so that $a^{n-1} \equiv 1 \pmod{n}$ and $\left(a^{\frac{n-1}{q}} - 1, n\right) = 1$ for all prime divisors $q$ of $F$, then $n$ is prime.

Proof. Suppose for a contradiction that there is a prime divisor $1 < p \leq \sqrt{n}$ of $n$. The congruence $a^{n-1} \equiv 1 \pmod{n}$ implies that $\text{ord}_p(a)|n - 1$. Let $t$ be so that $n - 1 = t\text{ord}_p(a)$.

Now let $q$ be a prime factor of $F$ and let $e$ be the exponent of $q$ in the prime factorization of $F$. Suppose for a contradiction that $q|t$. Then $a^{\frac{n-1}{q}} = a^{\text{ord}_p(a)\frac{t}{q}} \equiv 1 \pmod{p}$. 
**Theorem. Pocklington’s Primality Test.** Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \((F, R) = 1\) and \( F > R \). If there is an integer \( a \) so that \( a^{n-1} \equiv 1 \pmod{n} \) and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.

**Proof.** Suppose for a contradiction that there is a prime divisor \( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that \( \text{ord}_p(a) \mid n - 1 \). Let \( t \) be so that \( n - 1 = t \text{ord}_p(a) \).

Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the prime factorization of \( F \). Suppose for a contradiction that \( q \mid t \). Then \( a^{\frac{n-1}{q}} = a^{\text{ord}_p(a) \frac{t}{q}} \equiv 1 \pmod{p} \). But this means that \( p \mid \left( a^{\frac{n-1}{q}} - 1, n \right) \).
Theorem. Pocklington’s Primality Test. Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \((F, R) = 1\) and \( F > R \). If there is an integer \( a \) so that \( a^{n-1} \equiv 1 \pmod{n} \) and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.

Proof. Suppose for a contradiction that there is a prime divisor \( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that \( \text{ord}_p(a) \mid n - 1 \). Let \( t \) be so that \( n - 1 = t \text{ord}_p(a) \).

Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the prime factorization of \( F \). Suppose for a contradiction that \( q \mid t \). Then
\[
\left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \]

But this means that
\[
p \mid \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \]
Theorem. Pocklington’s Primality Test. Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \( (F, R) = 1 \) and \( F > R \). If there is an integer \( a \) so that \( a^{n-1} \equiv 1 \pmod{n} \) and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.

Proof. Suppose for a contradiction that there is a prime divisor \( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that \( \text{ord}_p(a)|n - 1 \). Let \( t \) be so that \( n - 1 = t\text{ord}_p(a) \).

Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the prime factorization of \( F \). Suppose for a contradiction that \( q|t \). Then \( a^{\frac{n-1}{q}} = a^{\text{ord}_p(a) \frac{t}{q}} \equiv 1 \pmod{p} \). But this means that \( p|\left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \), a contradiction.
Theorem. Pocklington’s Primality Test. Let $n \in \mathbb{N}$ be so that $n - 1 = FR$, with $(F, R) = 1$ and $F > R$. If there is an integer $a$ so that $a^{n-1} \equiv 1 \pmod{n}$ and $(a^{\frac{n-1}{q}} - 1, n) = 1$ for all prime divisors $q$ of $F$, then $n$ is prime.

Proof. Suppose for a contradiction that there is a prime divisor $1 < p \leq \sqrt{n}$ of $n$. The congruence $a^{n-1} \equiv 1 \pmod{n}$ implies that $\text{ord}_p(a) | n - 1$. Let $t$ be so that $n - 1 = t \text{ord}_p(a)$.

Now let $q$ be a prime factor of $F$ and let $e$ be the exponent of $q$ in the prime factorization of $F$. Suppose for a contradiction that $q | t$. Then $a^{\frac{n-1}{q}} = a^{\text{ord}_p(a) \frac{t}{q}} \equiv 1 \pmod{p}$. But this means that $p | \left(a^{\frac{n-1}{q}} - 1, n\right) = 1$, a contradiction. Hence $q \nmid t$. 
Theorem. **Pocklington’s Primality Test.** Let $n \in \mathbb{N}$ be so that $n - 1 = FR$, with $(F, R) = 1$ and $F > R$. If there is an integer $a$ so that $a^{n-1} \equiv 1 \pmod{n}$ and $\left(a^{\frac{n-1}{q}} - 1, n\right) = 1$ for all prime divisors $q$ of $F$, then $n$ is prime.

**Proof.** Suppose for a contradiction that there is a prime divisor $1 < p \leq \sqrt{n}$ of $n$. The congruence $a^{n-1} \equiv 1 \pmod{n}$ implies that $\text{ord}_p(a)|n - 1$. Let $t$ be so that $n - 1 = t\text{ord}_p(a)$. Now let $q$ be a prime factor of $F$ and let $e$ be the exponent of $q$ in the prime factorization of $F$. Suppose for a contradiction that $q|t$. Then $a^{\frac{n-1}{q}} = a^{\text{ord}_p(a)\frac{t}{q}} \equiv 1 \pmod{p}$. But this means that $p|\left(a^{\frac{n-1}{q}} - 1, n\right) = 1$, a contradiction. Hence $q \nmid t$ and therefore $q^e|\text{ord}_p(a)$. 

Bernd Schröder
Louisiana Tech University, College of Engineering and Science
Discrete Logarithms and Rabin’s Probabilistic Primality Test
Theorem. Pocklington’s Primality Test. Let $n \in \mathbb{N}$ be so that $n - 1 = FR$, with $(F, R) = 1$ and $F > R$. If there is an integer $a$ so that $a^{n-1} \equiv 1 \pmod{n}$ and $\left(a^{\frac{n-1}{q}} - 1, n\right) = 1$ for all prime divisors $q$ of $F$, then $n$ is prime.

Proof. Suppose for a contradiction that there is a prime divisor $1 < p \leq \sqrt{n}$ of $n$. The congruence $a^{n-1} \equiv 1 \pmod{n}$ implies that $\text{ord}_p(a)|n - 1$. Let $t$ be so that $n - 1 = t\text{ord}_p(a)$.

Now let $q$ be a prime factor of $F$ and let $e$ be the exponent of $q$ in the prime factorization of $F$. Suppose for a contradiction that $q|t$. Then $a^{\frac{n-1}{q}} = a^{\text{ord}_p(a) \cdot \frac{t}{q}} \equiv 1 \pmod{p}$. But this means that $p|\left(a^{\frac{n-1}{q}} - 1, n\right) = 1$, a contradiction. Hence $q \nmid t$ and therefore $q^e|\text{ord}_p(a)$. Because $q$ was an arbitrary prime factor of $F$, we conclude $F|\text{ord}_p(a)$. 
Theorem. Pocklington’s Primality Test. Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \((F, R) = 1\) and \( F > R \). If there is an integer \( a \) so that \( a^{n-1} \equiv 1 \pmod{n} \) and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.

Proof. Suppose for a contradiction that there is a prime divisor \( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that \( \text{ord}_p(a) \mid n - 1 \). Let \( t \) be so that \( n - 1 = t \text{ord}_p(a) \).

Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the prime factorization of \( F \). Suppose for a contradiction that \( q \mid t \). Then \( a^{\frac{n-1}{q}} = a^{\text{ord}_p(a) \frac{t}{q}} \equiv 1 \pmod{p} \). But this means that \( p \mid \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \), a contradiction. Hence \( q \nmid t \) and therefore \( q^e \mid \text{ord}_p(a) \). Because \( q \) was an arbitrary prime factor of \( F \), we conclude \( F \mid \text{ord}_p(a) \). From \( \text{ord}_p(a) \mid p - 1 \), we conclude \( F \mid p - 1 \).
Theorem. Pocklington’s Primality Test. Let \( n \in \mathbb{N} \) be so that 
\( n - 1 = FR \), with \( (F, R) = 1 \) and \( F > R \). If there is an integer \( a \) so that 
\( a^{n-1} \equiv 1 \) (mod \( n \)) and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.

Proof. Suppose for a contradiction that there is a prime divisor 
\( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \) (mod \( n \)) implies that 
\( \text{ord}_p(a) | n - 1 \). Let \( t \) be so that \( n - 1 = t \text{ord}_p(a) \).

Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the 
prime factorization of \( F \). Suppose for a contradiction that \( q | t \). Then 
\( a^{\frac{n-1}{q}} = a^{\text{ord}_p(a) \frac{t}{q}} \equiv 1 \) (mod \( p \)). But this means that 
\( p | \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \), a contradiction. Hence \( q \nmid t \) and therefore 
\( q^e | \text{ord}_p(a) \). Because \( q \) was an arbitrary prime factor of \( F \), we conclude 
\( F | \text{ord}_p(a) \). From \( \text{ord}_p(a) | p - 1 \), we conclude \( F | p - 1 \) and hence \( F < p \).
**Theorem. Pocklington’s Primality Test.** Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \( (F, R) = 1 \) and \( F > R \). If there is an integer \( a \) so that \( a^{n-1} \equiv 1 \pmod{n} \) and \( (a^{n-1}/q - 1, n) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.

**Proof.** Suppose for a contradiction that there is a prime divisor \( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that \( \text{ord}_p(a) | n - 1 \). Let \( t \) be so that \( n - 1 = t \text{ord}_p(a) \).

Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the prime factorization of \( F \). Suppose for a contradiction that \( q | t \). Then \( a^{n-1}/q = a^{\text{ord}_p(a) t/q} \equiv 1 \pmod{p} \). But this means that \( p | (a^{n-1}/q - 1, n) = 1 \), a contradiction. Hence \( q \nmid t \) and therefore \( q^e | \text{ord}_p(a) \). Because \( q \) was an arbitrary prime factor of \( F \), we conclude \( F | \text{ord}_p(a) \). From \( \text{ord}_p(a) | p - 1 \), we conclude \( F | p - 1 \) and hence \( F < p \). This is a contradiction, because we infer
Theorem. Pocklington’s Primality Test. Let \( n \in \mathbb{N} \) be so that 
\( n - 1 = FR \), with \((F, R) = 1\) and \( F > R \). If there is an integer \( a \) so that 
\( a^{n-1} \equiv 1 \pmod{n} \) and \( \left(a^{\frac{n-1}{q}} - 1, n\right) = 1 \) for all prime divisors \( q \) of \( F \),
then \( n \) is prime.

Proof. Suppose for a contradiction that there is a prime divisor 
\( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that 
\( \text{ord}_p(a) \mid n - 1 \). Let \( t \) be so that \( n - 1 = t \text{ord}_p(a) \).
Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the prime factorization of \( F \). Suppose for a contradiction that \( q \mid t \). Then 
\( a^{\frac{n-1}{q}} = a^{\text{ord}_p(a) \frac{t}{q}} \equiv 1 \pmod{p} \). But this means that 
\( p \mid \left(a^{\frac{n-1}{q}} - 1, n\right) = 1 \), a contradiction. Hence \( q \nmid t \) and therefore 
\( q^e \mid \text{ord}_p(a) \). Because \( q \) was an arbitrary prime factor of \( F \), we conclude 
\( F \mid \text{ord}_p(a) \). From \( \text{ord}_p(a) \mid p - 1 \), we conclude \( F \mid p - 1 \) and hence \( F < p \).
This is a contradiction, because we infer \( n \)
Theorem. Pocklington’s Primality Test. Let \( n \in \mathbb{N} \) be so that 
\( n - 1 = FR \), with \( (F, R) = 1 \) and \( F > R \). If there is an integer \( a \) so that 
\( a^{n-1} \equiv 1 \pmod{n} \) and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \), 
then \( n \) is prime.

Proof. Suppose for a contradiction that there is a prime divisor 
\( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that 
\( \text{ord}_p(a) | n - 1 \). Let \( t \) be so that \( n - 1 = t \text{ord}_p(a) \).

Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the 
prime factorization of \( F \). Suppose for a contradiction that \( q | t \). Then 
\( a^{\frac{n-1}{q}} = a^{\text{ord}_p(a) \frac{t}{q}} \equiv 1 \pmod{p} \). But this means that 
\( p | \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \), a contradiction. Hence \( q \nmid t \) and therefore 
\( q^e | \text{ord}_p(a) \). Because \( q \) was an arbitrary prime factor of \( F \), we conclude 
\( F | \text{ord}_p(a) \). From \( \text{ord}_p(a) | p - 1 \), we conclude \( F | p - 1 \) and hence \( F < p \).

This is a contradiction, because we infer \( n < F^2 \).
Theorem. Pocklington’s Primality Test. Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \((F, R) = 1\) and \( F > R \). If there is an integer \( a \) so that \( a^{n-1} \equiv 1 \pmod{n} \) and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.

Proof. Suppose for a contradiction that there is a prime divisor \( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that \( \text{ord}_p(a) \mid n - 1 \). Let \( t \) be so that \( n - 1 = t \text{ord}_p(a) \).

Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the prime factorization of \( F \). Suppose for a contradiction that \( q \mid t \). Then \( a^{\frac{n-1}{q}} = a^{\text{ord}_p(a) \frac{t}{q}} \equiv 1 \pmod{p} \). But this means that \( p \mid \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \), a contradiction. Hence \( q \nmid t \) and therefore \( q^e \mid \text{ord}_p(a) \). Because \( q \) was an arbitrary prime factor of \( F \), we conclude \( F \mid \text{ord}_p(a) \).

From \( \text{ord}_p(a) \mid p - 1 \), we conclude \( F \mid p - 1 \) and hence \( F < p \).

This is a contradiction, because we infer \( n < F^2 < p^2 \).
**Theorem. Pocklington’s Primality Test.** Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \( (F, R) = 1 \) and \( F > R \). If there is an integer \( a \) so that \( a^{n-1} \equiv 1 \pmod{n} \) and \( \left(a^{\frac{n-1}{q}} - 1, n\right) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.

**Proof.** Suppose for a contradiction that there is a prime divisor \( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that \( \text{ord}_p(a)|n - 1 \). Let \( t \) be so that \( n - 1 = t \text{ord}_p(a) \).

Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the prime factorization of \( F \). Suppose for a contradiction that \( q|t \). Then \( a^{\frac{n-1}{q}} = a^{\text{ord}_p(a) \frac{t}{q}} \equiv 1 \pmod{p} \). But this means that \( p|\left(a^{\frac{n-1}{q}} - 1, n\right) = 1 \), a contradiction. Hence \( q \nmid t \) and therefore \( q^e|\text{ord}_p(a) \). Because \( q \) was an arbitrary prime factor of \( F \), we conclude \( F|\text{ord}_p(a) \). From \( \text{ord}_p(a)|p - 1 \), we conclude \( F|p - 1 \) and hence \( F < p \).

This is a contradiction, because we infer \( n < F^2 < p^2 \leq n \).
**Theorem. Pocklington’s Primality Test.** Let \( n \in \mathbb{N} \) be so that \( n - 1 = FR \), with \((F, R) = 1\) and \( F > R \). If there is an integer \( a \) so that \( a^{n-1} \equiv 1 \pmod{n} \) and \( \left( a^{\frac{n-1}{q}} - 1, n \right) = 1 \) for all prime divisors \( q \) of \( F \), then \( n \) is prime.

**Proof.** Suppose for a contradiction that there is a prime divisor \( 1 < p \leq \sqrt{n} \) of \( n \). The congruence \( a^{n-1} \equiv 1 \pmod{n} \) implies that \( \text{ord}_p(a)|n - 1 \). Let \( t \) be so that \( n - 1 = t\text{ord}_p(a) \).

Now let \( q \) be a prime factor of \( F \) and let \( e \) be the exponent of \( q \) in the prime factorization of \( F \). Suppose for a contradiction that \( q|t \). Then 
\[
a^{\frac{n-1}{q}} = a^{\text{ord}_p(a) \frac{t}{q}} \equiv 1 \pmod{p}.
\]
But this means that \( p|\left(a^{\frac{n-1}{q}} - 1, n\right) = 1 \), a contradiction. Hence \( q \nmid t \) and therefore \( q^e|\text{ord}_p(a) \). Because \( q \) was an arbitrary prime factor of \( F \), we conclude \( F|\text{ord}_p(a) \). From \( \text{ord}_p(a)|p - 1 \), we conclude \( F|p - 1 \) and hence \( F < p \).

This is a contradiction, because we infer \( n < F^2 < p^2 \leq n \). ■
Theorem.

Let \( n = k 2^m + 1 \), where \( k, m \in \mathbb{N} \) are so that \( k \) is odd and \( k < 2^m \).

If there is an integer \( a \) so that \( a^{n-1}/2 \equiv -1 \pmod{n} \), then \( n \) is prime.

Proof. We will apply Pocklington's primality test. (Note, though, that Proth's test predates Pocklington's.) We let \( F : = 2^m \) and \( R : = k \).

Now consider an integer \( d \) so that \( d \mid n \) and \( d \mid (a^n-1/2-1) \).

Because \( a^{n-1}/2 \equiv -1 \pmod{n} \), we also have \( d \mid (a^n-1/2+1) \).

Hence \( d \mid 2 \).

Because \( n \) is odd, this means that \( d \mid 1 \).

Hence \( (a^{n-1}/2-1, n) = 1 \) and all prime factors of \( F \) are 2.

By Pocklington's test, \( n \) is prime.
Theorem. Proth’s Primality Test.

Let \( n = k2^m + 1 \), where \( k, m \in \mathbb{N} \) are so that \( k \) is odd and \( k < 2^m \).

If there is an integer \( a \) so that \( a^n - 1 \equiv -1 \pmod{n} \), then \( n \) is prime.

Proof. We will apply Pocklington’s primality test. (Note, though, that Proth’s test predates Pocklington’s.)

We let \( F = 2^m \) and \( R = k \).

Now consider an integer \( d \) so that \( d \mid n \) and \( d \mid (a^n - 1 - 1) \).

Because \( a^n - 1 \equiv -1 \pmod{n} \), we also have \( d \mid (a^n - 1 + 1) \).

Hence \( d \mid 2 \).

Because \( n \) is odd, this means that \( d \mid 1 \).

Hence \( (a^n - 1, n) = 1 \) and all prime factors of \( F \) are 2.

By Pocklington’s test, \( n \) is prime.
**Theorem. Proth’s Primality Test.** Let \( n = k2^m + 1 \), where \( k, m \in \mathbb{N} \) are so that \( k \) is odd and \( k < 2^m \).
Theorem. Proth’s Primality Test. \( \text{Let } n = k2^m + 1, \text{ where } k, m \in \mathbb{N} \text{ are so that } k \text{ is odd and } k < 2^m. \text{ If there is an integer } a \text{ so that } a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \)
Theorem. Proth’s Primality Test. Let \( n = k2^m + 1 \), where \( k, m \in \mathbb{N} \) are so that \( k \) is odd and \( k < 2^m \). If there is an integer \( a \) so that \( a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \), then \( n \) is prime.
Theorem. Proth’s Primality Test. Let \( n = k2^m + 1 \), where \( k, m \in \mathbb{N} \) are so that \( k \) is odd and \( k < 2^m \). If there is an integer \( a \) so that \( a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \), then \( n \) is prime.

Proof.
**Theorem. Proth’s Primality Test.** Let \( n = k2^m + 1 \), where \( k, m \in \mathbb{N} \) are so that \( k \) is odd and \( k < 2^m \). If there is an integer \( a \) so that \( a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \), then \( n \) is prime.

**Proof.** We will apply Pocklington’s primality test.
Theorem. Proth’s Primality Test. Let $n = k2^m + 1$, where $k, m \in \mathbb{N}$ are so that $k$ is odd and $k < 2^m$. If there is an integer $a$ so that $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, then $n$ is prime.

Proof. We will apply Pocklington’s primality test. (Note, though, that Proth’s test predates Pocklington’s.)
Theorem. Proth’s Primality Test. Let \( n = k2^m + 1 \), where \( k, m \in \mathbb{N} \) are so that \( k \) is odd and \( k < 2^m \). If there is an integer \( a \) so that \( a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \), then \( n \) is prime.

Proof. We will apply Pocklington’s primality test. (Note, though, that Proth’s test predates Pocklington’s.) We let \( F := 2^m \) and \( R := k \).
Theorem. Proth’s Primality Test. Let \( n = k2^m + 1 \), where \( k, m \in \mathbb{N} \) are so that \( k \) is odd and \( k < 2^m \). If there is an integer \( a \) so that \( a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \), then \( n \) is prime.

Proof. We will apply Pocklington’s primality test. (Note, though, that Proth’s test predates Pocklington’s.) We let \( F := 2^m \) and \( R := k \).
Now consider an integer \( d \) so that \( d|n \) and \( d|\left(a^{\frac{n-1}{2}} - 1\right)\).
Theorem. Proth’s Primality Test. Let \( n = k2^m + 1 \), where \( k, m \in \mathbb{N} \) are so that \( k \) is odd and \( k < 2^m \). If there is an integer \( a \) so that \( a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \), then \( n \) is prime.

Proof. We will apply Pocklington’s primality test. (Note, though, that Proth’s test predates Pocklington’s.) We let \( F := 2^m \) and \( R := k \).

Now consider an integer \( d \) so that \( d|n \) and \( d|\left(a^{\frac{n-1}{2}} - 1\right)\).

Because \( a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \), we also have \( d|\left(a^{\frac{n-1}{2}} + 1\right)\).
Theorem. Proth’s Primality Test. Let $n = k2^m + 1$, where $k, m \in \mathbb{N}$ are so that $k$ is odd and $k < 2^m$. If there is an integer $a$ so that $a^{n-1}/2 \equiv -1 \pmod{n}$, then $n$ is prime.

Proof. We will apply Pocklington’s primality test. (Note, though, that Proth’s test predates Pocklington’s.) We let $F := 2^m$ and $R := k$.
Now consider an integer $d$ so that $d|n$ and $d|\left(a^{n-1}/2 - 1\right)$. Because $a^{n-1}/2 \equiv -1 \pmod{n}$, we also have $d|\left(a^{n-1}/2 + 1\right)$. Hence $d|2$. 

Bernd Schröder

Louisiana Tech University, College of Engineering and Science

Discrete Logarithms and Rabin’s Probabilistic Primality Test
Theorem. Proth’s Primality Test. Let \( n = k2^m + 1 \), where \( k, m \in \mathbb{N} \) are so that \( k \) is odd and \( k < 2^m \). If there is an integer \( a \) so that \( a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \), then \( n \) is prime.

Proof. We will apply Pocklington’s primality test. (Note, though, that Proth’s test predates Pocklington’s.) We let \( F := 2^m \) and \( R := k \).

Now consider an integer \( d \) so that \( d|n \) and \( d|\left(a^{\frac{n-1}{2}} - 1\right)\).

Because \( a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \), we also have \( d|\left(a^{\frac{n-1}{2}} + 1\right)\).

Hence \( d|2 \). Because \( n \) is odd, this means that \( d|1 \).
Theorem. Proth’s Primality Test. Let \( n = k2^m + 1 \), where \( k, m \in \mathbb{N} \) are so that \( k \) is odd and \( k < 2^m \). If there is an integer \( a \) so that \( a^{n-1 \over 2} \equiv -1 \pmod{n} \), then \( n \) is prime.

Proof. We will apply Pocklington’s primality test. (Note, though, that Proth’s test predates Pocklington’s.) We let \( F := 2^m \) and \( R := k \).

Now consider an integer \( d \) so that \( d \mid n \) and \( d \mid \left( a^{n-1 \over 2} - 1 \right) \).

Because \( a^{n-1 \over 2} \equiv -1 \pmod{n} \), we also have \( d \mid \left( a^{n-1 \over 2} + 1 \right) \).

Hence \( d \mid 2 \). Because \( n \) is odd, this means that \( d \mid 1 \). Hence \( \left( a^{n-1 \over 2} - 1, n \right) = 1 \) and all prime factors of \( F \) are 2.
Theorem. Proth’s Primality Test. Let $n = k2^m + 1$, where $k, m \in \mathbb{N}$ are so that $k$ is odd and $k < 2^m$. If there is an integer $a$ so that $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, then $n$ is prime.

Proof. We will apply Pocklington’s primality test. (Note, though, that Proth’s test predates Pocklington’s.) We let $F := 2^m$ and $R := k$.

Now consider an integer $d$ so that $d | n$ and $d | \left( a^{\frac{n-1}{2}} - 1 \right)$.

Because $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, we also have $d | \left( a^{\frac{n-1}{2}} + 1 \right)$.

Hence $d | 2$. Because $n$ is odd, this means that $d | 1$. Hence $\left( a^{\frac{n-1}{2}} - 1, n \right) = 1$ and all prime factors of $F$ are 2. By Pocklington’s test, $n$ is prime.
Theorem. Proth’s Primality Test. Let \( n = k2^m + 1 \), where \( k, m \in \mathbb{N} \) are so that \( k \) is odd and \( k < 2^m \). If there is an integer \( a \) so that \( a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \), then \( n \) is prime.

Proof. We will apply Pocklington’s primality test. (Note, though, that Proth’s test predates Pocklington’s.) We let \( F := 2^m \) and \( R := k \).

Now consider an integer \( d \) so that \( d \mid n \) and \( d \mid \left( a^{\frac{n-1}{2}} - 1 \right) \).

Because \( a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \), we also have \( d \mid \left( a^{\frac{n-1}{2}} + 1 \right) \).

Hence \( d \mid 2 \). Because \( n \) is odd, this means that \( d \mid 1 \). Hence \( \left( a^{\frac{n-1}{2}} - 1, n \right) = 1 \) and all prime factors of \( F \) are 2. By Pocklington’s test, \( n \) is prime.