Zsigmondy's Theorem

Lola Thompson

Dartmouth College

August 11, 2009

Introduction

Definition

$o(a \bmod p) :=$ the multiplicative order of $a \pmod{p}$.

Recall: The multiplicative order of $a \pmod{p}$ is the smallest integer k such that $a^k \equiv 1 \pmod{p}$.

Example $o(2 \bmod 5) = 4$ since $2^1 \equiv 2 \pmod{5}$, $2^2 \equiv 4 \pmod{5}$, $2^3 \equiv 3 \pmod{5}$ and $2^4 \equiv 1 \pmod{5}$.

Introduction

Theorem (Zsigmondy)

For every pair of positive integers (a, n), except $n = 1$ and (2,6), there exists a prime p such that $n = o(a \bmod p)$.

- Let's see why the exceptional cases might not work:

Introduction

Theorem (Zsigmondy)

For every pair of positive integers (a, n)*, except* $n = 1$ *and (2,6), there exists a prime* p *such that* $n = o(a \bmod p)$*.*

- Let's see why the exceptional cases might not work:
- If $n = 1$, then $1 = o(a \bmod p) \Rightarrow a^1 \equiv 1 \pmod{p}$. But this is only true when $a = 1$.

Introduction

Theorem (Zsigmondy)

For every pair of positive integers (a, n), except $n = 1$ and (2,6), there exists a prime p such that $n = o\ (a \bmod p)$.

- $(2, 6)$ is an exception means that there are no primes p such that $6 = o(2 \bmod p)$, i.e. for any prime p such that $2^6 \equiv 1 (\bmod\ p)$, it must be the case that $2^3 \equiv 1 \pmod{p}$ or $2^2 \equiv 1 \pmod{p}$ also.

Introduction

Theorem (Zsigmondy)

For every pair of positive integers (a, n)*, except* $n = 1$ *and (2,6), there exists a prime* p *such that* $n = o\ (a \bmod p)$*.*

- $(2, 6)$ is an exception means that there are no primes p such that $6 = o(2 \bmod p)$, i.e. for any prime p such that $2^6 \equiv 1 (\bmod\ p)$, it must be the case that $2^3 \equiv 1 \pmod{p}$ or $2^2 \equiv 1 \pmod{p}$ also.
- The fact that $(2, 6)$ is an exception can be proven through elementary means, but we'll get it for free in the process of proving Zsigmondy's Theorem.

Outline

Cyclotomic Polynomials

Definition

We define n^{th} cyclotomic polynomial as follows:

$$\Phi_n(x) = \prod_{\substack{\zeta \;\; primitive \\ n^{th} \;\; root \;\; of \;\; 1}} (x - \zeta).$$

$\Phi_n(x)$ has degree $\varphi(n)$ since there are $\varphi(n)$ primitive n^{th} roots of unity. (Recall: If ζ is primitive then ζ^k is primitive if and only if $(k, n) = 1$)

Some Other Properties:

- Monic

Cyclotomic Polynomials

Definition

We define n^{th} cyclotomic polynomial as follows:

$$\Phi_n(x) = \prod_{\substack{\zeta \ \text{primitive} \\ n^{th} \ \text{root of } 1}} (x - \zeta).$$

$\Phi_n(x)$ has degree $\varphi(n)$ since there are $\varphi(n)$ primitive n^{th} roots of unity. (Recall: If ζ is primitive then ζ^k is primitive if and only if $(k, n) = 1$)

Some Other Properties:

- Monic
- Irreducible

Cyclotomic Polynomials

Definition

We define n^{th} cyclotomic polynomial as follows:

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ primitive} \\ n^{th} \text{ root of } 1}} (x - \zeta).$$

$\Phi_n(x)$ has degree $\varphi(n)$ since there are $\varphi(n)$ primitive n^{th} roots of unity.
(Recall: If ζ is primitive then ζ^k is primitive if and only if $(k, n) = 1$)

Some Other Properties:

- Monic
- Irreducible
- In $\mathbb{Z}[x]$
  (In fact, $\Phi_n(x)$ is the minimal polynomial for ζ over $\mathbb{Q}$)

Cyclotomic Polynomials

Theorem

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

(True since $x^n - 1 = \prod_{\zeta \ n^{th} \ root \ of \ 1} (x - \zeta) = \prod_{d|n} \prod_{\substack{\zeta \ primitive \\ d^{th} \ root \ of \ 1}} (x - \zeta)$).

The Mobius Function

The Mobius function $\mu(n)$ is an arithmetic function satisfying $\mu(1) = 1$ and $\sum_{d|n} \mu(d) = 0$ for every $n > 1$.

Example: $\sum_{d|2} \mu(d) = \mu(1) + \mu(2) = 0.$

Since $\mu(1) = 1$ then it must be the case that $\mu(2) = -1$.

Example: $\sum_{d|4} \mu(d) = \mu(1) + \mu(2) + \mu(4) = 0.$

Since we know that $\mu(1) + \mu(2) = 0$ then $\mu(4) = 0$.

In general: $\mu(n) = \begin{cases} 0, \; n = m \cdot p^r, r > 1 \\ -1^k, \; n = p_1 p_2 \cdots p_k \end{cases}$

Cyclotomic Polynomials

Theorem (Mobius Inversion Formula)

If $f(n) = \sum_{d|n} g(d)$ *then* $g(n) = \sum_{d|n} f(d) \cdot \mu(n/d)$.

Since $x^n - 1 = \prod_{d|n} \Phi_d(x)$ then $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$

(take log of both sides, apply Mobius inversion, then undo the logs).

Example:

$\Phi_2(x) = (x^1 - 1)^{\mu(2/1)} \cdot (x^2 - 1)^{\mu(2/2)} = (x-1)^{-1} \cdot (x^2 - 1) = x + 1.$

Cyclotomic Polynomials

Some Examples:

$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = x + 1$$
$$\Phi_3(x) = x^2 + x + 1$$
$$\Phi_4(x) = x^2 + 1$$
$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$
$$\Phi_6(x) = x^2 - x + 1$$
$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\Phi_8(x) = x^4 + 1$$

In general, $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

For $k \geq 1, \Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$. So $\Phi_{p^k}(x)$ has the same number of nonzero terms as $\Phi_p(x)$.

Values of Cyclotomic Polynomials

Theorem

Suppose $n > 1$. Then:

(1) $\Phi_n(0) = 1$

(2) $\Phi_n(1) = \begin{cases} p, & n = p^m, m > 0 \\ 1, & \textit{otherwise} \end{cases}$

To prove (2): Evaluate $\frac{x^n-1}{x-1}$ at $x = 1$ in 2 different ways to find $n = \prod_{\substack{d|n \\ d>1}} \Phi_d(1)$. We know that $\Phi_p(x) = x^{p-1} + \cdots + x + 1$, so $\Phi_p(1) = p$.

Moreover, $\Phi_{p^k}(1) = p$. By unique factorization, $n = p_1^{e_1} \cdots p_g^{e_g}$. Since there are e_i divisors of n that are powers of p_i for each prime p_i dividing n then, from our formula above, $\Phi_d(1) = 1$ when d is composite.

Values of Cyclotomic Polynomials

Theorem

Suppose $n > 1$. Then:

(3) If $a > 1$ then $(a-1)^{\varphi(n)} < \Phi_n(a) < (a+1)^{\varphi(n)}$.
(4) If $a \geq 3$ and $p \mid n$ is a prime factor, then $\Phi_n(a) > p$.

Proof of (3)

If $a > 1$ then geometry implies that $a - 1 <| a - \zeta |< a + 1$ for every point $\zeta \neq 1$ on the unit circle. The inequalities stated above follow from the fact that $| \Phi_n(a) |= \prod | a - \zeta |$.

Proof of (4)

Since $\varphi(n) \geq p - 1$ then when $a \geq 3$, we have $\Phi_n(a) > 2^{\varphi(n)} \geq 2^{p-1}$ (by (3)). But $2^{p-1} \geq p$ since $p \geq 2$.

Key Lemma

Lemma

Suppose that $n > 2$ and $a > 1$ are integers and $\Phi_n(a)$ is prime. If $\Phi_n(a) \mid n$ then $n = 6$ and $a = 2$.

Proof

- Let $p = \Phi_n(a)$, where $p \mid n$.

Key Lemma

Lemma

Suppose that $n > 2$ and $a > 1$ are integers and $\Phi_n(a)$ is prime. If $\Phi_n(a) \mid n$ then $n = 6$ and $a = 2$.

Proof

- Let $p = \Phi_n(a)$, where $p \mid n$.
- If $a \geq 3$ then $\Phi_n(a) > p$ by (4), which is obviously false.

Key Lemma

Lemma

Suppose that $n > 2$ and $a > 1$ are integers and $\Phi_n(a)$ is prime. If $\Phi_n(a) \mid n$ then $n = 6$ and $a = 2$.

Proof

- Let $p = \Phi_n(a)$, where $p \mid n$.
- If $a \geq 3$ then $\Phi_n(a) > p$ by (4), which is obviously false.
- Thus, $a = 2$ and $\Phi_n(2) = p$.

Key Lemma

Lemma

Suppose that $n > 2$ and $a > 1$ are integers and $\Phi_n(a)$ is prime. If $\Phi_n(a) \mid n$ then $n = 6$ and $a = 2$.

Proof

- Let $p = \Phi_n(a)$, where $p \mid n$.
- If $a \geq 3$ then $\Phi_n(a) > p$ by (4), which is obviously false.
- Thus, $a = 2$ and $\Phi_n(2) = p$.
- Since $\Phi_n(2) = p$ then $p \mid (2^n - 1)$ (since $\Phi_n(x)$ always divides $x^n - 1$), i.e. $2^n \equiv 1 (\text{mod } p)$.

Key Lemma

Lemma

Suppose that $n > 2$ and $a > 1$ are integers and $\Phi_n(a)$ is prime. If $\Phi_n(a) \mid n$ then $n = 6$ and $a = 2$.

Proof

- Let $p = \Phi_n(a)$, where $p \mid n$.
- If $a \geq 3$ then $\Phi_n(a) > p$ by (4), which is obviously false.
- Thus, $a = 2$ and $\Phi_n(2) = p$.
- Since $\Phi_n(2) = p$ then $p \mid (2^n - 1)$
  (since $\Phi_n(x)$ always divides $x^n - 1$), i.e. $2^n \equiv 1 (\text{mod } p)$.
- So, p must be odd.

Key Lemma

- So far, we have: $p = \Phi_n(2)$, $p \mid n$, p odd.

Key Lemma

- So far, we have: $p = \Phi_n(2)$, $p \mid n$, p odd.
- Factor $n = p^e \cdot m$ where $p \nmid m$.

Key Lemma

- So far, we have: $p = \Phi_n(2)$, $p \mid n$, p odd.
- Factor $n = p^e \cdot m$ where $p \nmid m$.
- It's a well-known fact from abstract algebra that if n is as above and if α is a root of $\Phi_n(x)$ over F_p then $m = o(\alpha)$.

Key Lemma

- So far, we have: $p = \Phi_n(2)$, $p \mid n$, p odd.
- Factor $n = p^e \cdot m$ where $p \nmid m$.
- It's a well-known fact from abstract algebra that if n is as above and if α is a root of $\Phi_n(x)$ over F_p then $m = o(\alpha)$.
- As a result, since we know that $\Phi_n(2) \equiv 0 (\text{mod } p)$, then $m = o(2 \text{ mod } p)$.

Key Lemma

- So far, we have: $p = \Phi_n(2)$, $p \mid n$, p odd.
- Factor $n = p^e \cdot m$ where $p \nmid m$.
- It's a well-known fact from abstract algebra that if n is as above and if α is a root of $\Phi_n(x)$ over F_p then $m = o(\alpha)$.
- As a result, since we know that $\Phi_n(2) \equiv 0 (\text{mod } p)$, then $m = o(2 \text{ mod } p)$.
- If $e > 1$ then $p = \Phi_n(2) = \Phi_{p^e \cdot m}(2) = \Phi_m(2^{p^e}) = \Phi_{pm}(2^{p^{e-1}})$.

Key Lemma

- So far, we have: $p = \Phi_n(2)$, $p \mid n$, p odd.
- Factor $n = p^e \cdot m$ where $p \nmid m$.
- It's a well-known fact from abstract algebra that if n is as above and if α is a root of $\Phi_n(x)$ over F_p then $m = o(\alpha)$.
- As a result, since we know that $\Phi_n(2) \equiv 0 (\text{mod } p)$, then $m = o(2 \text{ mod } p)$.
- If $e > 1$ then $p = \Phi_n(2) = \Phi_{p^e \cdot m}(2) = \Phi_m(2^{p^e}) = \Phi_{pm}(2^{p^{e-1}})$.
- This contradicts (4), since $2^{p^{e-1}} \geq 2^p > 4$.

Key Lemma

- So far, we have: $p = \Phi_n(2),\ p \mid n,\ p$ odd.
- Factor $n = p^e \cdot m$ where $p \nmid m$.
- It's a well-known fact from abstract algebra that if n is as above and if α is a root of $\Phi_n(x)$ over F_p then $m = o(\alpha)$.
- As a result, since we know that $\Phi_n(2) \equiv 0 (\text{mod } p)$, then $m = o(2 \text{ mod } p)$.
- If $e > 1$ then $p = \Phi_n(2) = \Phi_{p^e \cdot m}(2) = \Phi_m(2^{p^e}) = \Phi_{pm}(2^{p^{e-1}})$.
- This contradicts (4), since $2^{p^{e-1}} \geq 2^p > 4$.
- Thus, $n = pm$.

Key Lemma

- At this point, we have deduced: $p = \Phi_n(2)$, $p \mid n$, p odd, $n = pm$ where $p \nmid m$.

Key Lemma

- At this point, we have deduced: $p = \Phi_n(2)$, $p \mid n$, p odd, $n = pm$ where $p \nmid m$.
- We're trying to show that $n = 6$.

Key Lemma

- At this point, we have deduced: $p = \Phi_n(2)$, $p \mid n$, p odd, $n = pm$ where $p \nmid m$.
- We're trying to show that $n = 6$.
- Now, $p = \Phi_{pm}(2) = \frac{\Phi_m(2^p)}{\Phi_m(2)} > \frac{(2^p-1)^{\varphi(m)}}{(2+1)^{\varphi(m)}} \geq \frac{2^p-1}{3}$ (from (3)).

Key Lemma

- At this point, we have deduced: $p = \Phi_n(2),\ p \mid n,\ p$ odd, $n = pm$ where $p \nmid m$.
- We're trying to show that $n = 6$.
- Now, $p = \Phi_{pm}(2) = \frac{\Phi_m(2^p)}{\Phi_m(2)} > \frac{(2^p-1)^{\varphi(m)}}{(2+1)^{\varphi(m)}} \geq \frac{2^p-1}{3}$ (from (3)).
- But then $3p + 1 > 2^p$, which is impossible if $p > 3$.

Key Lemma

- At this point, we have deduced: $p = \Phi_n(2)$, $p \mid n$, p odd, $n = pm$ where $p \nmid m$.
- We're trying to show that $n = 6$.
- Now, $p = \Phi_{pm}(2) = \frac{\Phi_m(2^p)}{\Phi_m(2)} > \frac{(2^p-1)^{\varphi(m)}}{(2+1)^{\varphi(m)}} \geq \frac{2^p-1}{3}$ (from (3)).
- But then $3p + 1 > 2^p$, which is impossible if $p > 3$.
- Therefore, $p = 3$ and $m = o(2 \bmod 3) = 2$, so $n = 2 \cdot 3 = 6$.

Recap and Extensions

We have proven the following Key Lemma:

Lemma

Suppose that $n > 2$ and $a > 1$ are integers and $\Phi_n(a)$ is **prime**. *If $\Phi_n(a) \mid n$ then $n = 6$ and $a = 2$.*

We can extend the Key Lemma to show that if $\Phi_n(a)$ is a **divisor** of n for some $n > 2$ and $a > 1$, then $n = 6$ and $a = 2$.

Good Pairs, Bad Pairs

Definition

Let $a, n \in \mathbb{Z}^+, a > 1$. The pair (a, n) is **good** if $n = o(a \bmod p)$ for some prime p.

Lemma (Good Pairs Condition)

(a, n) is good if and only if there is a prime p such that $p \mid (a^n - 1)$ but $p \nmid (a^{n/q} - 1)$ for every prime factor $q \mid n$.

Example $3^2 - 1$ uses the same primes as $3^1 - 1$, so $(3, 2)$ is bad.

Good Pairs, Bad Pairs

Lemma

$(a, 1)$ is bad when $a = 2$.
$(a, 2)$ is bad when $a = 2^m - 1$ for some $m > 1$.
All other pairs $(a, 2^k)$ are good.

Example $2^2 - 1 = 3, 2^3 - 1 = 7, 2^6 - 1 = 63 = 3^2 \cdot 7$. Thus, $(2, 6)$ is bad.

Zsigmondy's Theorem

Theorem (Zsigmondy)

If $n \geq 2$, the only bad pair (a, n) is $(2, 6)$.

[In other words, there exists a prime p such that $n = o(a \bmod p)$ for every pair (a, n) except (2, 6)]

Proof Outline Suppose (a, n) is bad and $n > 2$. We will translate this into a problem about cyclotomic polynomials and use the Key Lemma to derive a contradiction unless $a = 2$ and $n = 6$.

Two More Lemmas

In order to prove Zsigmondy's Theorem, we will need the following two lemmas:

Lemma (1)

If $x^n - 1 = \Phi_n(x) \cdot \omega_n(x)$ *then* $\omega_n(x) = \prod_{\substack{d|n \\ d<n}} \Phi_d(x)$ *and* $(x^d - 1) \mid \omega_n(x)$ *in* $\mathbb{Z}[x]$ *whenever* $d \mid n, d < n$.

Lemma (2)

Suppose that $d \mid n$ *and* $a^d \equiv 1 \pmod{p}$. *If* $d < n$ *then* $p \mid \frac{n}{d}$. *In any case,* $p \mid n$.

Proving Zsigmondy's Theorem

Theorem (Zsigmondy)

If $n \geq 2$, the only bad pair (a, n) is $(2, 6)$.

Proof

- Pick an odd prime factor $p \mid \Phi_n(a)$.

Proving Zsigmondy's Theorem

Theorem (Zsigmondy)

If $n \geq 2$, the only bad pair (a, n) is $(2, 6)$.

Proof

- Pick an odd prime factor $p \mid \Phi_n(a)$.
- Suppose that (a, n) is bad, so that $k = o(a \bmod p)$ is a proper divisor of n.

Proving Zsigmondy's Theorem

Theorem (Zsigmondy)

If $n \geq 2$, the only bad pair (a, n) is $(2, 6)$.

Proof

- Pick an odd prime factor $p \mid \Phi_n(a)$.
- Suppose that (a, n) is bad, so that $k = o(a \bmod p)$ is a proper divisor of n.
- Let $x^n - 1 = \Phi_n(x) \cdot \omega_n(x)$.

Proving Zsigmondy's Theorem

Theorem (Zsigmondy)

If $n \geq 2$, the only bad pair (a, n) is $(2, 6)$.

Proof

- Pick an odd prime factor $p \mid \Phi_n(a)$.
- Suppose that (a, n) is bad, so that $k = o(a \bmod p)$ is a proper divisor of n.
- Let $x^n - 1 = \Phi_n(x) \cdot \omega_n(x)$.
- From Lemma (1), $(a^k - 1) \mid \omega_n(a)$, so $p \mid (a^n - 1)$ also.

Proving Zsigmondy's Theorem

Theorem (Zsigmondy)

If $n \geq 2$, the only bad pair (a, n) is $(2, 6)$.

Proof

- Pick an odd prime factor $p \mid \Phi_n(a)$.
- Suppose that (a, n) is bad, so that $k = o(a \bmod p)$ is a proper divisor of n.
- Let $x^n - 1 = \Phi_n(x) \cdot \omega_n(x)$.
- From Lemma (1), $(a^k - 1) \mid \omega_n(a)$, so $p \mid (a^n - 1)$ also.
- So p^2 is a factor of $\Phi_n(a) \cdot \omega_n(a) = a^n - 1$.

Proving Zsigmondy's Theorem

Theorem (Zsigmondy)

If $n \geq 2$, the only bad pair (a, n) is $(2, 6)$.

Proof

- Pick an odd prime factor $p \mid \Phi_n(a)$.
- Suppose that (a, n) is bad, so that $k = o(a \bmod p)$ is a proper divisor of n.
- Let $x^n - 1 = \Phi_n(x) \cdot \omega_n(x)$.
- From Lemma (1), $(a^k - 1) \mid \omega_n(a)$, so $p \mid (a^n - 1)$ also.
- So p^2 is a factor of $\Phi_n(a) \cdot \omega_n(a) = a^n - 1$.
- By Fermat's little Theorem, $a^{p-1} \equiv 1 (\bmod\ p)$, so $k \mid p - 1$, hence $k < p$.

Proving Zsigmondy's Theorem

- From Lemma (2), we know that if $k \mid n$ and $a^k \equiv 1 (\bmod\ p)$, then if $k < n$, we must have $p \mid \frac{n}{k}$ and $p \mid n$.

Proving Zsigmondy's Theorem

- From Lemma (2), we know that if $k \mid n$ and $a^k \equiv 1 (\text{mod } p)$, then if $k < n$, we must have $p \mid \frac{n}{k}$ and $p \mid n$.
- It follows that p is the only prime factor of $\frac{n}{k}$, so we can write $n = k \cdot p^u$ for some $u \geq 1$.

Proving Zsigmondy's Theorem

- From Lemma (2), we know that if $k \mid n$ and $a^k \equiv 1 \pmod{p}$, then if $k < n$, we must have $p \mid \frac{n}{k}$ and $p \mid n$.
- It follows that p is the only prime factor of $\frac{n}{k}$, so we can write $n = k \cdot p^u$ for some $u \geq 1$.
- We can also use Lemma (2) to show that p is the only prime factor of $\Phi_n(a)$. In other words, $\Phi_n(a) = p^t$ for some $t \geq 1$.

Finishing Up

- We've already shown that p is odd and $p \mid n$ and $\Phi_n(a) = p^t$.

Finishing Up

- We've already shown that p is odd and $p \mid n$ and $\Phi_n(a) = p^t$.
- If $t > 2$ then p^2 divides $\frac{a^n-1}{a^{n/p}-1}$, since $(a^{n/p} - 1) \mid \omega_n(a)$.

Finishing Up

- We've already shown that p is odd and $p \mid n$ and $\Phi_n(a) = p^t$.
- If $t > 2$ then p^2 divides $\frac{a^n-1}{a^{n/p}-1}$, since $(a^{n/p} - 1) \mid \omega_n(a)$.
- We can use the exponent law to derive a contradiction to the statement that $p^2 \mid \frac{a^n-1}{a^{n/p}-1}$. Thus, $\Phi_n(a) = p$.

Finishing Up

- We've already shown that p is odd and $p \mid n$ and $\Phi_n(a) = p^t$.
- If $t > 2$ then p^2 divides $\frac{a^n-1}{a^{n/p}-1}$, since $(a^{n/p} - 1) \mid \omega_n(a)$.
- We can use the exponent law to derive a contradiction to the statement that $p^2 \mid \frac{a^n-1}{a^{n/p}-1}$. Thus, $\Phi_n(a) = p$.
- Now, if $a \geq 3$ then $\Phi_n(a) > p$, which we know is false.

Finishing Up

- We've already shown that p is odd and $p \mid n$ and $\Phi_n(a) = p^t$.
- If $t > 2$ then p^2 divides $\frac{a^n-1}{a^{n/p}-1}$, since $(a^{n/p} - 1) \mid \omega_n(a)$.
- We can use the exponent law to derive a contradiction to the statement that $p^2 \mid \frac{a^n-1}{a^{n/p}-1}$. Thus, $\Phi_n(a) = p$.
- Now, if $a \geq 3$ then $\Phi_n(a) > p$, which we know is false.
- Hence, we must have $a = 2$. By the Key Lemma, $n = 6$.

Finishing Up

- We've already shown that p is odd and $p \mid n$ and $\Phi_n(a) = p^t$.
- If $t > 2$ then p^2 divides $\frac{a^n-1}{a^{n/p}-1}$, since $(a^{n/p} - 1) \mid \omega_n(a)$.
- We can use the exponent law to derive a contradiction to the statement that $p^2 \mid \frac{a^n-1}{a^{n/p}-1}$. Thus, $\Phi_n(a) = p$.
- Now, if $a \geq 3$ then $\Phi_n(a) > p$, which we know is false.
- Hence, we must have $a = 2$. By the Key Lemma, $n = 6$.
- Therefore, $(2, 6)$ is the only bad pair.

Finishing Up

- We've already shown that p is odd and $p \mid n$ and $\Phi_n(a) = p^t$.
- If $t > 2$ then p^2 divides $\frac{a^n-1}{a^{n/p}-1}$, since $(a^{n/p} - 1) \mid \omega_n(a)$.
- We can use the exponent law to derive a contradiction to the statement that $p^2 \mid \frac{a^n-1}{a^{n/p}-1}$. Thus, $\Phi_n(a) = p$.
- Now, if $a \geq 3$ then $\Phi_n(a) > p$, which we know is false.
- Hence, we must have $a = 2$. By the Key Lemma, $n = 6$.
- Therefore, $(2, 6)$ is the only bad pair.
- We've proven Zsigmondy's Theorem!

A Special Case of Zsigmondy's Theorem

A special case of Zsigmondy's Theorem states the problem in terms of Mersenne numbers:

Consider the k^{th} Mersenne number $M_k = 2^k - 1$. Then, each of $M_2, M_3, M_4, \ldots$ has a prime factor that does not occur as a factor of an earlier member of the sequence EXCEPT for M_6.

Acknowledgements

Thanks to Dr. Dan Shapiro, whose expository notes on the subject were invaluable in writing this talk.

Bibliography:

1. *Introduction to the Theory of Numbers* by Harold N. Shapiro

2. *Abstract Algebra* by David S. Dummit and Richard M. Foote