Cylotomic Polynomials and their applications

Sunaina Pati, Chennai Mathematical Institute, Chennai

January 18, 2025

Contents

0 Introduction

Just my notes on Cylcotomic polynomials. A lot of references has been used:

- This math stackexchange answer
- MIT lecture notes
- Brett Porter's Cyclotomic polynomials
- Ramprasad Saptarishi's scribed Computational Number theory lecture 23 and 24
- Evan's Orders modulo a prime.

  It is also a more refined and self-contained version of Yan Sheng's blog post, Bart Michels's paper and this aops post.

1 Cylcotomic Polynomials

Definition (primitive n-th roots of unity)**.** For $n \geq 1$, the primitive n-th roots of unity are the $\omega \in \mathbb{C}$ such that $\omega^n = 1$, and $\omega^k \neq 1$ for $1 \leq k < n$. More explicitly, these are given by

$$e^{\frac{2\pi ik}{n}}, 1 \leq k \leq n, (k, n) = 1.$$

Note that there are precisely $\varphi(n)$ many primitive n-th roots of unity.

Definition. The n-th cyclotomic polynomial Φ_n is defined by

$$\Phi_n(X) := \prod_j (X - \omega_j),$$

where the product is taken over all primitive n-th roots of unity ω_j.

Note that the n-th roots of unity are precisely the union of the primitive d-th root of unity for $d \mid n$, so

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

So we also get that

$$\sum_{d|n} \varphi(d) = n.$$

Example 1.1. Here are the first few cyclotomic polynomials:

- $\Phi_1(x) = x - 1$
- $\Phi_2(x) = x + 1$
- $\Phi_3(x) = x^2 + x + 1$
- $\Phi_4(x) = x^2 + 1$

Now, we shall prove some properties about it.

Theorem 1.1. *For $n \geq 1$, $\Phi_n(X)$ has integer coefficients.*

Proof. We induct. For $n = 1$, we have $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Say $\Phi_k(x) \in \mathbb{Z}[x]$ for all $k < n$. Note that

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

where $p_n(x) = \prod_{d|n,d\neq n} \Phi_d(x)$. Then $p_n \in \mathbb{Z}[X]$ by induction. Now, we state a claim.

Claim 1.1. *If*

$$(x^n - 1) = (\textstyle\sum_{i=1}^{m} a_i x^i)(\sum_{j=1}^{l} b_j x^i),$$

where $\sum_{i=1}^{m} a_i x^i \in \mathbf{Z}[\mathbf{x}]$, then $b_j \in \mathbb{Q}, \forall j$.

Proof. Note that since $a_m \cdot b_l = 1 \implies b_l \in \mathbb{Q}$. Similarly we can show all the b_j lie in $\mathbb{Q}$. □

So, by the above claim, we get $\Phi_n(x) \in \mathbb{Q}[x]$. Let α be the smallest positive rational such that $\alpha\Phi_n(x) \in \mathbb{Z}[x]$. Note that α must be an integer. Also, note that gcd of the coeffecients of polynomial $\alpha\Phi_n(x) = \Phi'_n(x)$ will be 1.

Definition (Primitive Polynomial)**.** Call an integer polynomial primitive if gcd of the coefficents is 1.

Lemma 1.1. *Let $p(x), q(x)$ be two primitive polynomials. Then $p(x) \cdot q(x)$ is also primitive.*

Proof. Let $p(x)q(x) = c_l x^l + \cdots + c_0$. Let $p(x) = b_m x^m + \cdots + b_0, q(x) = a_n x^n = \cdots + a_0$. Suppose $\gcd(c_l, \ldots, c_0) > 1$. Then $\exists$ prime p which divides all the c_i. Since $p(x)$ is not primitive, $\exists b_j$ such that $p \nmid b'_j$. So ther must exist a minimal b_j such that $p \nmid b_j$. Then $p|b_0, b_1, \ldots, b_{j-1}$. Consider c_j. Since

$$p|c_j \implies p|b_0 a_j + b_1 a_{j-1} + \ldots b_j a_0 \implies p|b_j a_0 \implies p|a_0.$$

Similarly consider c_{j+1}. Since

$$p|c_{j+1} \implies p|b_0 a_{j+1} + \cdots + b_j a_1 + b_{j+1} a_0 \implies p|a_1.$$

Continuing this process, we get that p divides all the coefficients of $q(x)$, contradicting that it is primitive. □

Note that $\Phi'_n(x)$ and $p_n(x)$ are primitive. But note that

$$\Phi'_n(x) \cdot p_n(x) = \alpha(x^n - 1).$$

By above lemma, we should have $\alpha(x^n - 1)$ to be primitive. Hence $|\alpha|$ is 1. And so $\Phi_n(x) \in \mathbb{Z}[x]$. □

Note that these polynomials are also irreducibles.

Proposition 1.1. *Let p be a prime and $n \geq 1$. Then*

$$\Phi_{pn}(X) = \begin{cases} \Phi_n(X^p) & p \mid n \\ \frac{\Phi_n(X^p)}{\Phi_n(X)} & p \nmid n. \end{cases}$$

Proof. If $p \mid n$, note that the p-th roots of the primitive n-th roots of unity are the primitive pn-th roots of unity If $p \nmid n$, note that the p-th roots of the primitive n-th roots of unity are the union of the primitive n-th and pn-th roots of unity. □

Proposition 1.2. *Let $n \geq 3$ and $x \in (1, \infty)$. Then*

$$(x-1)^{\varphi(n)} < \Phi_n(x) < (x+1)^{\varphi(n)}.$$

Proof. For any primitive n-th root of unity ω, we have $|\omega| = 1$, so by triangle inequality, we get

$$x - 1 \leq |x - \omega| \leq x + 1.$$

Hence taking products over all ω gives

$$(x-1)^{\varphi(n)} < |\Phi_n(x)| < (x+1)^{\varphi(n)}.$$

Note that $\Phi_n(x) > 0$ for $x > 1$. So done. □

2 Cyclotomic Polynomials for two variables

Now we will see why we are dealing with cyclotomic polynomials.

Definition. Define

$$\Phi_n(a, b) := b^{\varphi(n)} \Phi_n\left(\frac{a}{b}\right).$$

Note that $\Phi_n(a, b)$ is an integer. Moreover,

$$\begin{aligned}
\prod_{d|n} \Phi_n(a, b) &= \prod_{d|n} b^{\varphi(d)} \Phi_d\left(\frac{a}{b}\right) \\
&= \prod_{d|n} b^{\varphi(d)} \cdot \prod_{d|n} \Phi_d\left(\frac{a}{b}\right) \\
&= b^n \left[\left(\frac{a}{b}\right)^n - 1\right] \\
&= a^n - b^n.
\end{aligned}$$

Similarl to previous sections, the following two propositions follow.

Proposition 2.1. *Let p be a prime and $n \geq 1$. Then*

$$\Phi_{pn}(a, b) = \begin{cases} \Phi_n(a^p, b^p) & p \mid n \\ \frac{\Phi_n(a^p, b^p)}{\Phi_n(a, b)} & p \nmid n. \end{cases}$$

Proposition 2.2. *Let $n \geq 3$. Then*

$$(a-b)^{\varphi(n)} < \Phi_n(a, b) < (a+b)^{\varphi(n)}.$$

3 Orders and Cyclotomic Polynomials

Let $p \geq 3$ be a prime such that $p \nmid a, b$. Let $n \geq 1$, and let $k \geq 1$ be minimal such that $p \mid a^k - b^k$. Then note that k is order of a/b modulo p. So $k | p - 1$.

Moreover, note that $\Phi_n(a, b) | a^n - b^n$.

Theorem 3.1. *If p is a prime and $\Phi(a) \equiv 0 \pmod{p} \implies ord_p(a) = n \implies p \equiv 1 \pmod{n}$ or $p | n$.*

Proof. Note that

$$\Phi_n(X)|x^n-1 \implies \Phi_n(a)|a^n-1 \implies p|a^n-1 \implies \mathrm{ord}_p(a)|n.$$

If $\mathrm{ord}_p(a)=n$ then the first case holds. If $\mathrm{ord}_p(a)<n$ then $\exists k<n$ such that $p|x^k-1$ and $\Phi_k(a)=1$. So x^n-1 has a root of multiplicity of atleast 2. So

$$(nx^{n-1}, x^n-1) \neq 1 \text{ in } \mathbb{F}_p \implies p|n.$$

□

4 Any subgroup of a mulitiplicative group of a field is cyclic

Lemma 4.1. *Let G a finite group with n elements. If for every $d \mid n$, $\#\{x \in G \mid x^d=1\} \leq d$, then G is cyclic.*

Proof. Fix $d \mid n$ and consider the set G_d made up of elements of G with order d. Suppose that $G_d \neq \varnothing$, so there exists $y \in G_d$; it is clear that $\langle y\rangle \subseteq \{x \in G \mid x^d=1\}$. But the subgroup $\langle y\rangle$ has cardinality d, so from the hypothesis we have that $\langle y\rangle = \{x \in G \mid x^d=1\}$. Therefore G_d is the set of generators of the cyclic group $\langle y\rangle$ of order d, so $\#G_d = \phi(d)$.

We have proved that G_d is empty or has cardinality $\phi(d)$, for every $d \mid n$. So we have:

$$\begin{aligned} n &= \#G && (4.1)\\ &= \sum_{d|n} \#G_d && (4.2)\\ &\leq \sum_{d|n} \phi(d) && (4.3)\\ &= n. && (4.4) \end{aligned}$$

Therefore $\#G_d = \phi(d)$ for every $d|n$. In particular $G_n \neq \varnothing$. This proves that G is cyclic. □

If G is a finite subgroup of the multiplicative group of a field, then G satisfies the hypothesis because the polynomial x^d-1 has d roots at most.

5 Roots of unity on Finite fields

Theorem 5.1. *Let $K^{(n)}$ be splitting field of x^n-1. The set of all the roots be $E^{(n)}$. K be field of char p. Then:*

- *if $p \nmid n$ then $E^{(n)}$ is cyclic group of order n.*
- *if $p \mid n \implies n=p^e m, p \nmid m$ then $K^{(n)}=K^{(m)}, E^{(n)}=E^{(m)}$ and root of x^n-1 are m elements each occuring with muliplicity p^e.*

Proof. The second part follows because

$$x^n-1 = x^{mp^e}-1 = (x^m-1)^{p^e}$$

by frobinious map. The first pat is true because of the following: Note that x^n-1 and nx^n have common factor 1. So no repeating root. The set of roots form a multiplicative group as if $\alpha, \beta \in E^{(n)}$ then

$$(\alpha\beta^{-1})^n = \alpha^n\beta^{-n} = 1 \implies \alpha\beta^{-1} \in E^{(n)}.$$

And any subgroup of a mulitiplicative group of a field is cyclic. □

6 Cyclotomic polynomial on finite fields

Theorem 6.1. *Let $K = \mathbb{F}_p$ and $(p, n) = 1, d = ord_n(p)$, p is prime. Then:*

- *$K^{(n)}$ is the spliting field of any irreducible factor of $\Phi_n(x)$*
- *$[K^{(n)} : K] = d$*

Proof. Let ζ be one primitive root of $\Phi_n(x)$. Note that

$$\zeta \in \mathbb{F}_{p^k} \iff \zeta^{p^k} = \zeta \text{ (as all element of the field satisfy } x^{p^k} - x = 0)$$

$$\iff \zeta^{p^k-1} = 1 \iff n | p^k - 1 \iff p^k \equiv 1 \mod n.$$

Note that since $d = \text{ord}_n(p) \implies \zeta \in \mathbb{F}_{p^d}$ but no proper subfield of $\mathbb{F}_{p^d}$. So the minimal polynomial of ζ has degree d. Same for other primitive roots. So the spliting field $K^{(n)} = \mathbb{F}_{p^d}$ and $[K^{(n)} : K] = d$. □

Let ζ be a primitive- n th root of unity. Note that $\zeta \in \mathbb{F}_p$ when $r = p - 1$ as all the element of $\mathbb{F}_p$ are roots of $x^p - x$, hence all non zero elements are roots of $x^{p-1} - 1$. Let $M(x)$ be the minimal polynomial of ζ. We claim the following:

Theorem 6.2.

$$deg(M(x)) = ord_r(p).$$

Proof. Let $\deg(M(x)) = d$. Let the polynomial be $a_0 + a_1 x + \cdots + a_d x^d$. Note that

$$M(\zeta) = 0 \implies 0 = (M(\zeta))^p \implies (a_0 + a_1\zeta + \cdots + a_d\zeta^d)^p = a_0^p + a_1^p\zeta^p + \cdots + a_d^p\zeta^{pd} = a_0 + a_1\zeta + a_d\zeta^d = 0.$$

$$M(\zeta) = 0 \implies M(\zeta^p) = 0.$$

Similarly, we get $\zeta^{p^2}, \ldots, \zeta^{p^{d-1}}$ as the roots. So the minimal polynomial has roots precisely; $\zeta, \zeta^p, \zeta^{p^2}, \ldots, \zeta^{p^{d-1}}$ as it is degree d polynomial. So note that $\zeta^{p^d} = \zeta^p$. All elements of $\mathbb{F}_{p^d}$ satisfy the equation $x^{p^d} - x = 0$. ($\mathbb{F}_{p^d}$ is the splitting field of this polynomial.) Thus, in particular, $\zeta^{p^d} = \zeta$. So $d = \text{ord}_r(p)$. □

Remark. This proof was in Professor Ramprasad's scribed notes.

7 On primes dividing Cyclotomic polynomials

Theorem 7.1. *Let $p \nmid n$ and $m|n$. Then $\Phi_n(x)$ and $x^m - 1$ has no common root modulo p.*

Proof. Note that $\Phi_n(x)|x^n - 1$ and $x^m - 1|x^n - 1$. And $x^n - 1$ has double root modulo p iff $(x^n - 1, nx^{n-1}) > 1$. But $p \nmid n$. □

Theorem 7.2. *Let n be a positive integer. There are infinitely many primes congruent to $1 \mod n$.*

Proof. Well, we prove it just like how we prove that there are infinitely many primes. Say there are finite many primes say $p_1, p_2, \ldots, p_k$. Then consider $\Phi_n(knp_1, p_2, \ldots, p_k)$ for big enough k. Note the none $p_i | knp_1, p_2, \ldots, p_k$. So a new prime p divides it. However, note that by theorem 3.1, we get that $p \equiv 1 \mod n$. □

8 Irreducibility of Cyclotomic polynomials

Let ζ be a primitive n^{th} root of unity and let $f(z)$ be its minimal polynomial. Since ζ is also a root of $z^n - 1 = 0$, it follows that $f(z)$ divides $(z^n - 1)$ and by Gauss Lemma $f(z)$ has integer coefficients.

Theorem 8.1. *If p is any prime which does not divide n then ζ^p is a root of $f(z) = 0$.*

Proof. Suppose not. Note that $\Phi_n(\zeta^p) = 0$ and ζ is root of $\Phi_n(x)$. So $f(x)|\Phi_n(x)$. So $\Phi_n(x) = f(x)g(x)$. Note $g(x) \in \mathbb{Z}$. Therefore ζ is a root of $g(z^p) = 0$. Since $f(z)$ is the minimal polynomial of ζ, it follows that $f(z)$ divides $g(z^p)$ so that $g(z^p) = f(z)h(z)$ where $h(z)$ is monic with integer coefficients.Also since $\Phi_n(z)$ is a factor of $(z^n - 1)$ so that we have $z^n - 1 = \Phi_n(z)d(z)$ where $d(z)$ is monic and in $\mathbb{Z}[x]$.

$$z^n - 1 = f(z)g(z)d(z)$$
$$g(z^p) = f(z)h(z)$$

Going mod p,

$$g(z^p) = g(z)^p.$$

So any irreducible factor of $f(z)$ will divide $g(z)^p$ and hence $g(z)$. But n is coprime to p. So no repeated roots. Contradiction. □

$f(z)$ is the minimal polynomial for $\zeta^{p_1 p_2 \cdots p_m}$ where $p_1, p_2, \ldots, p_m$ are any primes not dividing n. It follows that ζ^k where k is coprime to n is also a root of $f(z)$. Thus all the primitive n^{th} roots of unity are roots of $f(z) = 0$. Hence $\Phi_n(z) = f(z)$.

9 On coefficients of Cyclotomic polynomials

Theorem 9.1. *The coefficients of cyclotomic polynomials are palindromic for $n \geq 2$*

Proof. This is by induction. For $n = 2$ it is true. Note that

$$\Phi_2\Big(\frac{1}{x}\Big)x^{\phi(2)} = \Phi_2(x).$$

We will be showing that

$$\forall n \geq 2, \Phi_n\Big(\frac{1}{x}\Big)x^{\phi(n)} = \Phi_n(x).$$

However,

$$\Phi_n\Big(\frac{1}{x}\Big)x^{\phi(n)} = \frac{(1/x)^n - 1}{\prod_{d|n, d<n} \Phi_d(\frac{1}{x})}x^{\phi(n)}.$$

By induction hypothesis,

$$= \frac{(1/x)^n - 1}{\prod_{d|n, 1<d<n}(\Phi_d(x))(1/x - 1)x}x^n$$
$$= \frac{1 - x^n}{\prod_{d|n, 1<d<n}(\Phi_d(x))(1/x - 1)x}$$
$$= \frac{1 - x^n}{\prod_{d|n, 1<d<n}(\Phi_d(x))(1 - x)}$$
$$= \Phi_n(x).$$

□

10 Zsigmondy's theorem

Theorem 10.1. *Let $a > b \geq 1$ be coprime integers, and let $n \geq 2$. Then there exists a prime divisor of $a^n - b^n$ that does not divide $a^k - b^k$ for all $1 \leq k < n$, except when:*

- *$n = 2$, and $a + b$ is a power of 2; or*
- *$(a, b, n) = (2, 1, 6)$.*

Example 10.1. Consider $(a, b, n) = (4, 2, 3)$. Then $4^3 - 2^3 = 56, 4^2 - 2^2 = 12, 4^1 - 2^1 = 2$. So one such nice prime would be 7.

Definition. We call such a prime divisor, a **primitive prime divisor** of $a^n - b^n$.

We essentially want to find prime divisors of $a^n - b^n$ which LTE can handle to some extent.

10.1 Lifting the exponent lemma

We state and prove LTE first.

Theorem 10.2. *Let p be a prime, $x, y \in \mathbb{Z}$, and $m \geq 1$, such that $x \equiv y \not\equiv 0 \pmod{p}$.*

- *If $p \geq 3$, then*
$$v_p(x^m - y^m) = v_p(x - y) + v_p(m).$$
- *If $p = 2$, then*
$$v_2(x^m - y^m) = \begin{cases} v_2(x^2 - y^2) + v_2\left(\frac{m}{2}\right) & m \text{ even}, \\ v_2(x - y) & m \text{ odd}. \end{cases}$$

Proof. We will show it for odd primes. For even primes, it is left to the readers. We use induction on $v_p(n)$. We show for $v_p(n) = 0, v_p(n) = 1$ and then use induction.

- We show it for $v_p(n) = 0$. That is show $v_p(x^n - y^n) = v_p(x - y)$, for $v_p(n) = 0$. To show this is true, we will show,
$$v_p\left(\frac{x^n - y^n}{x - y}\right) = v_p(x^{n-1} + yx^{n-2} + y^2x^{n-3} + \cdots + y^{n-1}) = 0.$$
As $x \equiv y \pmod{p}$, so,
$$x^{n-1} + yx^{n-2} + y^2x^{n-3} + \cdots + y^{n-1} \equiv nx^{n-1} \pmod{p}.$$
And $p \nmid nx^{n-1}$
- We show it for $v_p(n) = 1$. That is show $v_p(x^n - y^n) = v_p(x - y) + 1$ To show this is true, we will show,
$$v_p\left(\frac{x^n - y^n}{x - y}\right) = v_p(x^{n-1} + yx^{n-2} + y^2x^{n-3} + \cdots + y^{n-1}) = 1.$$
As $x \equiv y \pmod{p} \implies x = y + pk$, so,
$$x^{n-1} + yx^{n-2} + y^2x^{n-3} + \cdots + y^{n-1} \pmod{p^2}$$
$$\equiv (pk + y)^{n-1} + (pk + y)^{n-2}y + (pk + y)^{n-3}y^2 + \cdots + y^{n-1} \pmod{p^2}$$

$$\equiv (y^{n-1} + pk \cdot (n-1)y^{n-2}) + (y^{n-1} + ypk \cdot (n-2)y^{n-3}) + \cdots + y^{n-1} \pmod{p^2}$$

$$\equiv n \cdot y^{n-1} + pky^{n-2}\frac{(n-1)(n)}{2} \pmod{p^2}$$

Since $(n, p^2) = p$. Let $n' = n/p$.

$$\equiv n' \cdot y^{n-1} + ky^{n-2}\frac{(n-1)(n)}{2} \pmod{p}$$

. We have p odd, so above is equivalent to

$$\equiv n' \cdot y^{n-1}n' \pmod{p}$$

but $p \nmid n', y$. So done!

- Let's assume it's true for $v_p = 0, 1, \ldots, j-1$. Now, we will show it's true for $v_p(n) = j$. Then let $n = p^j \cdot c$. Then

$$v_p(x^n - y^n) = v_p(x^{p^j \cdot c} - y^{p^j \cdot c}) = v_p((x^p)^{p^{j-1} \cdot c} - (y^p)^{p^{j-1} \cdot c})$$

$$= v_p(x^p - y^p) + v_p(p^{j-1} \cdot c) = v_p(x-y) + 1 + j - 1 = v_p(x-y) + v_p(n)$$

□

10.2 The $n = 2$ case

Theorem 10.3. *If we have a tuple of the form $(a, b, n) = (a, b, 2), (a, b) = 1$. such that it has no primitive divisor then $a + b$ is perfect power of 2.*

Proof. If $a^2 - b^2$ has no primitive divisor, then if a prime p divides $a^2 - b^2$ then it also divides $a - b$. Moreover, if

$$p|a+b \implies p|a^2 - b^2 \implies p|a+b \implies p = 2 \implies a - b \text{ is a power of 2.}$$

□

So from now we assume that $n \geq 3$.

10.3 LTE on Cylcotomic prolynomials

Theorem 10.4. *Let $p \geq 3$ be a prime such that $p \nmid a, b$. Let $n \geq 1$, and let $k \geq 1$ be minimal such that $p \mid a^k - b^k$. Then*

$$v_p(\Phi_n(a,b)) = \begin{cases} v_p(a^k - b^k) & n = k \\ 1 & n = p^\beta k,\ \beta \geq 1 \\ 0 & \textit{else}. \end{cases}$$

Proof. We begin with cases.
Case 1: Note that if $k = n$ then $p \nmid a^n - b^n$. Hence

$$v_p(a^k - b^k) = v_p(a^n - b^n) \quad = v_p(\Phi_n(a,b)) + \sum_{d|n,\, d \neq n} v_p(\Phi_d(a,b))$$

$$= v_p(\Phi_n(a,b))$$

Note that

$$\sum_{d|n,\, d\neq n} v_p(\Phi_d(a,b)) = 0$$

because of the minimality of k we assumes. If $v_p(\Phi_d(a,b)) > 0$ for some d, then $p|a^d - b^d$. Not possible.

So this proved the first statement.

Case 2: For $n = p^\beta k$ then we get

$$\begin{aligned} v_p(a^k - b^k) + \beta &= v_p(a^{p^\beta k} - b^{p^\beta k}) \\ &= \sum_{d|p^\beta k} v_p(\Phi_d(a,b)) \\ &= \sum_{d|k} v_p(\Phi_d(a,b)) + v_p(\Phi_{pk}(a,b)) + v_p(\Phi_{p^2k}(a,b)) + \cdots + v_p(\Phi_{p^\beta k}(a,b)) \\ &= v_p(a^k - b^k) + v_p(\Phi_{pk}(a,b)) + v_p(\Phi_{p^2k}(a,b)) + \cdots + v_p(\Phi_{p^\beta k}(a,b)) \end{aligned}$$

$$\implies \beta = v_p(\Phi_{pk}(a,b)) + v_p(\Phi_{p^2k}(a,b)) + \cdots + v_p(\Phi_{p^\beta k}(a,b)).$$

So, this implies $v_p(\Phi_{p^jk}(a,b)) = 1$.

Case 3.1: If $k \nmid n$, then $p \nmid a^n - b^n$. So $p \nmid \Phi_n(a,b) \implies v_p(\Phi_n(a,b)) = 0$.

Case 3.2: If $k \mid n$, then $n = p^\beta mk$ for some $p \nmid m$ (so $\beta = v_p(\frac{n}{k})$). We have dealt with the case $m = 1$. If $m > 1$ then $\Phi_n(a,b)$ is a factor of

$$\frac{\prod_{d|n} \Phi_d(a,b)}{\prod_{d|p^\beta k} \Phi_d(a,b)} = \frac{a^n - b^n}{a^{p^\beta k} - b^{p^\beta k}}.$$

But note that LTE gives $v_p(a^n - b^n) = v_p(a^{p^\beta k} - b^{p^\beta k})$, so p does not divide $\Phi_n(a,b)$. So done. □

Theorem 10.5 (For $p = 2$)**.** *Let a, b be odd, and $n \geq 1$. Then*

$$v_2(\Phi_n(a,b)) = \begin{cases} v_2(a-b) & n = 1 \\ v_2(a+b) & n = 2 \\ 1 & n = 2^\beta,\ \beta \geq 2 \\ 0 & \textit{else}. \end{cases}$$

Left to the readers!

10.4 Final Proof

Suppose that $a^n - b^n$ has no primitive prime divisors.

If $\Phi_n(a,b) > 1$. Let p be a prime factor of $\Phi_n(a,b)$. Then $p \mid a^n - b^n$, so there exists a minimal $1 \leq k < n$ such that $p \mid a^k - b^k$. (since we assumed that $a^n - b^n$ has no primitive prime divisor.

Case 1: If $p \geq 3$, since $n < k$ and $p|\Phi_n(a,b)$. We get that $v_p(\Phi_n(a,b)) = 1$. So n is of the forms $p^\beta k$.We also know that $k|n$ and $k|p-1 \implies k < p$. So note that p is the largest prime factor of n. Suppose $q \neq p$ divides $\Phi_n(a,b)$. By similar reasoning, we get that q is the largest primefactor of n. Contradiction as we got p to be the largest prime factor.

Hence $\Phi_n(a,b)$ is p.

Case 2: If $p = 2$ then $n \geq 3$ is a power of 2, so $4 \mid n$ implies (as $n \geq 3$). So

$$\Phi_n(a,b) = a^{n/2} + b^{n/2} \equiv 2 \pmod 4.$$

So $v_p(\Phi_n(a,b)) = 1$.

So we get

$$p \geq \Phi_n(a,b) \geq (a-b)^{\varphi(n)} \geq (a-b)^{p-1}.$$

If $a - b \geq 2$, then $p = 2$ and $n = 2$.

If $a - b = 1$, write $n = p^\beta k$.

Case 1:If $\beta \geq 2$ then

$$\begin{aligned} p \geq \Phi_n(a,b) &= \Phi_{pk}(a^{p^{\beta-1}}, b^{p^{\beta-1}}) \\ &\geq (a^{p^{\beta-1}} - b^{p^{\beta-1}})^{\varphi(pk)} \\ &\geq a^p - b^p = (b+1)^p - b^p \\ &= pb^{p-1} + \cdots + 1 \end{aligned}$$

Not possible.

Case 2: $\beta = 1$, so $n = pk$. Note $p \nmid k$. Infact $k < p$.

$$\begin{aligned} p \geq \Phi_n(a,b) &= \frac{\Phi_k(a^p, b^p)}{\Phi_k(a,b)} \\ &\geq \left(\frac{a^p - b^p}{a+b}\right)^{\varphi(k)} \\ &\geq \frac{(a^p - b^p)^{\varphi(k)}}{a+b} \\ &\geq \frac{2^p - 1}{3}. \end{aligned}$$

Here, equality can only hold when $p = 3$ and $b = 1$ (so $a = 2$). Also, since $k < p$, we have $k \in 1, 2$, so $n \in$
$3, 6$. But $2^3 - 1^3$ has 7 as a primitive divisor. Note that $2^6 - 1^6$ has no primitive divisors. Hence we get the exception case.
This concludes the proof of Zsigmondy's theorem.

10.5 Sum version of Zsigmondy

The sum version follows from above

Theorem 10.6. *Let $a, b \in \mathbb{N}$ such that $(a,b) = 1$ and $n \in \mathbb{N}$, $n > 1$. There exists a prime divisor of $a^n + b^n$ that does not divide $a^k + b^k$, $\forall k \in \{1, \ldots, n-1\}$, except $1^3 + 2^3$.*

Proof. We use zsigmondy on $2n$. We know there exist primitive prime divisor p of $a^{2n} - b^{2n}$. Note $p | a^n + b^n$ as $p \nmid a^n - b^n$. Moreover, $p \nmid a^k + b^k$ $\forall k < n$ as then $p | a^{2k} - b^{2k}$. □